МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ГРАБОВИЙ ВЛАДИСЛАВ АНДРІЙОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
інформаційних технологій,
канд. техн. наук, доцент
_____О. В. Зелінська
«____»_____ 20__ р.

ЗМЕНШЕННЯ РИЗИКІВ УРАЖЕННЯ ШКІДЛИВИМИ ПРОГРАМАМИ ХМАРНОГО СЕРЕДОВИЩА AMAZON WEB SERVICES

Спеціальність 122 Комп’ютерні науки

Кваліфікаційна (магістерська) робота

Науковий керівник:
С. Д. Штовба, професор кафедри
інформаційних технологій,
д-р. техн. наук, професор
Науковий консультант:
Н. Р. Веселовська, професор
кафедри інформаційних
технологій, д-р. техн. наук,
професор
_____
(підпис)

Оцінка: ___/___/_____
(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця 2024

АНОТАЦІЯ

Грабовий В.А. Зменшення ризиків ураження шкідливими програмами в хмарному середовищі AWS. Спеціальність 122 «Комп’ютерні науки», освітня програма «Комп’ютерні технології обробки даних», Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У кваліфікаційній (магістерській) роботі досліджена проблема зменшення ризиків ураження шкідливими програмами в хмарному середовищі AWS. Проведено аналіз сучасних інструментів кіберзахисту, таких як AWS GuardDuty, AWS Lambda, Amazon Inspector, AWS Backup, а також підходів на основі машинного навчання. Розроблено веб-додаток для управління процесами резервного копіювання, моніторингу загроз і автоматизованого реагування. Робота забезпечує підвищення рівня безпеки даних у хмарних середовищах.

76 с., 0 табл., 15 рис., 2 дод., 36 джерел.

Ключові слова: AWS, кібербезпека, резервне копіювання, машинне навчання, Python, React, веб-додаток.

ABSTRACT

Hrabovyi V.A. Reducing the risks of malware infection in AWS cloud environment. Specialization 122 "Computer Science", educational program "Data Science", Vasyl' Stus Donetsk National University, Vinnytsia, 2024.

The qualification (master's) thesis investigates the problem of reducing the risks of malware infection in the AWS cloud environment. A detailed analysis of modern cybersecurity tools, including AWS GuardDuty, AWS Lambda, Amazon Inspector, AWS Backup, and machine learning-based approaches, was conducted. A web application was developed for managing backup processes, threat monitoring, and automated response. The work enhances data security in cloud environments.

76 p., 0 tab., 15 figures, 2 app., 36 ref.

Keywords: AWS, cybersecurity, backup, machine learning, Python, React, web application.

ЗМІСТ

ВСТУП

Захист хмарного середовища Amazon Web Services (AWS) є однією з найактуальніших проблем у сучасному світі, зважаючи на швидке зростання популярності хмарних технологій. AWS забезпечує компаніям доступ до потужних інструментів для обчислень, зберігання даних та аналізу, що дозволяє оптимізувати бізнес-процеси. Однак із поширенням таких платформ зростає й ризик кібератак, зокрема з боку шкідливого програмного забезпечення, яке може значно впливати на безпеку даних і стабільність бізнес-операцій.

Актуальність теми обумовлена зростаючим числом випадків атак на хмарні середовища. Наприклад, програмне забезпечення-вимагач (ransomware) і атаки на інтерфейси прикладного програмування (API) дедалі частіше використовуються зловмисниками для проникнення в хмарні інфраструктури, викрадення або шифрування даних. У таких умовах забезпечення проактивного захисту стає важливим завданням для організацій, що використовують AWS.

Мета роботи – розробка підходів і технологій для мінімізації ризиків ураження хмарних середовищ AWS шкідливими програмами. Зокрема, важливим є впровадження інструментів автоматизації, штучного інтелекту та машинного навчання, які дозволяють ефективно виявляти та запобігати загрозам.

Об'єкт дослідження – хмарне середовище AWS як платформа для зберігання та обробки даних. Предмет дослідження – методи та засоби захисту даних у хмарних середовищах від шкідливих програм.

Новизна роботи полягає в інтеграції сучасних підходів, таких як автоматизоване резервне копіювання, аналіз поведінкових аномалій та використання моделей машинного навчання для виявлення загроз, що

залишаються непоміченими традиційними інструментами. Також дослідження охоплює експериментальну апробацію запропонованих рішень на реальних даних для оцінки їхньої ефективності.

Практична значущість роботи проявляється у можливості впровадження запропонованих рішень для підвищення рівня безпеки даних у хмарних середовищах, забезпечення безперебійності бізнес-процесів та мінімізації ризиків ураження шкідливими програмами.

Таким чином, у межах роботи передбачено розробку інноваційних підходів до кіберзахисту хмарних сервісів AWS, які дозволять організаціям ефективніше протидіяти сучасним кіберзагрозам, забезпечуючи надійність і стабільність своїх систем.

За результатами роботи опубліковано тези доповіді[36].

РОЗДІЛ 1. ОГЛЯД СТАНУ ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1 Аналіз шкідливих програм в хмарних середовищах як об’єкту дослідження

Шкідливе програмне забезпечення, або малваре, є однією з найнебезпечніших загроз у сфері кібербезпеки, оскільки його вплив може варіюватися від крадіжки даних до повного паралічу бізнес-процесів. Це програми, що мають на меті порушення роботи систем, викрадення інформації або використання ресурсів без дозволу власника. Сучасні малваре можуть діяти у формі вірусів, троянських програм, хробаків, програм-вимагачів та інших шкідливих компонентів, що активно використовуються зловмисниками для досягнення своїх цілей[1].

З розвитком хмарних обчислювальних платформ, таких як Amazon Web Services (AWS), зростає кількість потенційних вразливостей, які можуть бути використані зловмисниками для атаки. Основною перевагою хмарних середовищ є можливість масштабування інфраструктури та зберігання великих обсягів даних у віддалених дата-центрах. Проте ці переваги водночас є критичними точками вразливості, адже централізація даних створює зручні умови для атак. Малваре часто використовує помилки в конфігураціях хмарних сервісів, таких як неправильно налаштовані S3-бакети, для проникнення в інфраструктуру та компрометації даних.

AWS, як одна з найбільших платформ хмарних обчислень, має розгалужену інфраструктуру, яка включає сотні сервісів, таких як обчислювальні платформи (Amazon EC2), сервіси зберігання даних (Amazon S3) та бази даних (Amazon RDS). Ці сервіси активно використовуються як малими компаніями, так і великими корпораціями, що робить AWS

привабливою мішенню для зловмисників. Наприклад, API AWS, що надають доступ до ресурсів, можуть бути вразливими до експлуатації через недостатні заходи безпеки, такі як відсутність обмежень доступу або некоректна авторизація.

Об’єктом дослідження в цій роботі виступає хмарне середовище AWS, яке активно використовується для забезпечення гнучкості та ефективності обробки даних[15]. AWS пропонує користувачам широкий набір інструментів для роботи з великими обсягами даних. Amazon EC2 дозволяє розгортати віртуальні сервери для обробки додатків, адаптуючи ресурси залежно від навантаження, що забезпечує динамічне масштабування. Amazon S3 пропонує можливості безпечного зберігання даних з підтримкою резервного копіювання та архівування. Ці сервіси дозволяють компаніям зберігати інформацію без необхідності фізичних сховищ, що значно зменшує витрати та підвищує операційну ефективність.

Проте, з точки зору кібербезпеки, ці ж сервіси можуть стати каналами для проникнення малваре. Наприклад, програмне забезпечення-вимагач може використовувати слабкі місця в налаштуваннях безпеки Amazon S3 для шифрування даних з метою отримання викупу. Інший приклад – експлуатація помилок у політиках доступу IAM (Identity and Access Management), що може дозволити зловмисникам отримати адміністративний доступ до критичних ресурсів[16].

AWS також пропонує керовані бази даних, такі як Amazon RDS, які дозволяють автоматизувати більшість адміністративних завдань. Але навіть автоматизація може стати потенційною вразливістю, якщо не проводити регулярний моніторинг та аудит безпеки. Наприклад, недостатній контроль над оновленнями баз даних може призвести до того, що уразливості старих версій будуть використані для атак.

Особливо важливим є дослідження методів виявлення та запобігання малваре в хмарних середовищах. Одним із таких методів є використання антивірусного сканування у поєднанні з механізмами штучного інтелекту для аналізу поведінкових аномалій. Наприклад, інтеграція Amazon GuardDuty з іншими інструментами AWS може автоматично виявляти підозрілі дії в реальному часі. Це включає моніторинг логів CloudTrail, який дозволяє відстежувати всі API-запити, а також виявлення нетипових змін у конфігураціях.

Малваре в хмарних середовищах також може діяти через соціальну інженерію, наприклад, фішингові атаки, спрямовані на крадіжку облікових даних. Ці атаки стають дедалі складнішими, і їх виявлення вимагає комплексного підходу, який включає навчання персоналу та впровадження сучасних інструментів, таких як AWS Security Hub. Важливим також є постійний моніторинг уразливостей хмарних середовищ, включаючи аналіз політик доступу, перевірку активності облікових записів та оцінку ризиків, пов’язаних із використанням стороннього програмного забезпечення.

Таким чином, шкідливе програмне забезпечення в хмарних середовищах AWS становить серйозну загрозу для безпеки організацій. Регулярний моніторинг, аудит безпеки та використання сучасних інструментів виявлення малваре є критично важливими для забезпечення надійності інфраструктури. З іншого боку, помилки у конфігураціях, недоліки політик доступу або невчасні оновлення систем можуть значно підвищити ризики компрометації, що робить дослідження цієї теми вкрай актуальним.

1.2 Методи та технології оцінювання ризиків ураження шкідливими програмами в AWS

Оцінка ризиків ураження шкідливими програмами в хмарному середовищі AWS є критично важливою для забезпечення безпеки даних та безперебійної роботи сервісів. Для ефективного виявлення та нейтралізації

загроз використовуються сучасні методи та технології, які поєднують автоматизацію, машинне навчання та глибокий аналіз інцидентів:

- Amazon GuardDuty є інтелектуальною системою моніторингу, яка безперервно аналізує активність у вашому AWS середовищі для виявлення підозрілої поведінки та потенційних загроз. Використовуючи машинне навчання та загрозову розвідку, GuardDuty здатний виявляти аномалії, такі як несанкціонований доступ до ресурсів, спроби ескалації привілеїв або підозрілі API-запити. Важливою перевагою є те, що GuardDuty не потребує встановлення додаткових агентів на інстанції або контейнери, що спрощує його впровадження та знижує операційні витрати. Згідно з офіційною документацією AWS, GuardDuty може аналізувати понад трильйон подій Amazon S3 щодня, що забезпечує високий рівень захисту від потенційних загроз[2].
- Amazon Detective доповнює можливості GuardDuty, надаючи інструменти для глибокого аналізу та розслідування інцидентів безпеки. Використовуючи машинне навчання, статистичний аналіз та теорію графів, Detective автоматично збирає та візуалізує дані з різних джерел AWS, таких як VPC Flow Logs, CloudTrail та DNS-логи. Це дозволяє швидко ідентифікувати першопричини інцидентів, відстежувати взаємозв'язки між ресурсами та користувачами, а також виявляти патерни поведінки, характерні для шкідливих дій. За даними AWS, Detective спрощує процес розслідування, знижуючи час на аналіз інцидентів та підвищуючи ефективність команд безпеки.
- Amazon S3 Malware Scanning є важливим компонентом захисту даних, що зберігаються в Amazon S3. Ця технологія дозволяє автоматично сканувати файли на наявність шкідливого програмного забезпечення під час їх завантаження або модифікації. Інтеграція з іншими сервісами AWS, такими як Lambda та SNS, забезпечує автоматизовану обробку виявлених загроз, наприклад, ізоляцію заражених файлів або сповіщення відповідальних осіб.

Використання багатодвигунного антивірусного сканування підвищує точність виявлення та знижує ризик пропуску нових або невідомих загроз.

Використання штучного інтелекту (ШІ) та машинного навчання (МН) є ключовим елементом сучасних підходів до кібербезпеки. Моделі МН здатні аналізувати великі обсяги даних, виявляти аномалії та прогнозувати потенційні загрози на основі історичних патернів. AWS активно впроваджує ШІ та МН у свої сервіси безпеки, що дозволяє автоматизувати процеси виявлення та реагування на інциденти, знижуючи навантаження на команди безпеки та підвищуючи загальний рівень захисту.

Незважаючи на потужні інструменти та технології, існують певні виклики у забезпеченні безпеки в AWS. Одним із них є складність налаштування та управління політиками безпеки, особливо для організацій без достатнього досвіду або ресурсів. Людський фактор також відіграє значну роль: помилки конфігурації, нехтування процедурами безпеки або недостатнє навчання співробітників можуть призвести до уразливостей. Згідно з дослідженням Gartner, до 2025 року до 99% інцидентів безпеки в хмарних середовищах будуть спричинені помилками клієнтів, а не постачальників послуг[17].

Для подолання цих викликів важливо впроваджувати автоматизацію процесів виявлення та реагування на загрози. Інтеграція сервісів AWS, таких як GuardDuty, Detective та Lambda, дозволяє створювати автоматизовані робочі процеси, які швидко реагують на інциденти, мінімізуючи час впливу та потенційні збитки. Наприклад, при виявленні підозрілої активності GuardDuty може ініціювати Lambda-функцію, яка автоматично ізолює компрометовану інстанцію або змінює відповідні політики доступу.

Таким чином, ефективне оцінювання ризиків ураження шкідливими програмами в AWS вимагає комплексного підходу, що поєднує сучасні інструменти, автоматизацію та постійне вдосконалення процесів безпеки.

Використання таких сервісів, як Amazon GuardDuty, Detective та S3 Malware Scanning, у поєднанні з технологіями штучного інтелекту та машинного навчання, забезпечує високий рівень захисту хмарних середовищ від сучасних кіберзагроз[18].

1.3 Виявлені проблеми та недоліки існуючих підходів

Незважаючи на існування різноманітних інструментів захисту від шкідливих програм у хмарному середовищі AWS, багато дослідників і практиків відзначають низку проблем та недоліків, які знижують ефективність боротьби з малваре. Сучасна динаміка розвитку кіберзагроз потребує адаптивних і вдосконалених підходів до забезпечення безпеки.

Висока складність налаштування та підтримки засобів безпеки: багато компаній, особливо середнього та малого бізнесу, стикаються зі складністю налаштування та управління інструментами безпеки в AWS. Відсутність досвідчених спеціалістів або обмежені ресурси можуть призвести до ненавмисних помилок у конфігураціях, які створюють нові вразливості для атак. Наприклад, неправильне налаштування політик IAM (Identity and Access Management) часто дозволяє надмірні привілеї користувачам, що відкриває шлях для потенційних зловмисників. Згідно з дослідженням MarketsandMarkets, розмір світового ринку аналізу шкідливого програмного забезпечення прогнозовано зросте з 3,0 мільярдів доларів у 2019 році до 11,7 мільярдів доларів до 2024 року зі середньорічним темпом зростання (CAGR) у 31,0%[3]. Це свідчить про зростання потреби у високоефективних інструментах аналізу та захисту.

Обмеження сигнатурних рішень для виявлення шкідливих програм: більшість традиційних антивірусних рішень спираються на сигнатурний підхід, який ефективно працює лише для вже відомих загроз. Проте сучасні кіберзлочинці активно використовують методи обфускації, динамічної модифікації та поліморфізму, щоб уникнути виявлення. Такі

техніки дозволяють створювати нові варіації шкідливого ПЗ, які залишаються непоміченими. У відповідь на ці виклики, сучасні платформи, такі як AWS, починають інтегрувати штучний інтелект і машинне навчання для виявлення аномальної активності, яка не відповідає відомим патернам загроз.

Недостатнє тестування на проникнення та аудит безпеки: багато організацій покладаються на вбудовані засоби захисту AWS, такі як Amazon GuardDuty чи Amazon Inspector, але часто нехтують додатковим тестуванням на проникнення або аудитами. Це створює значні ризики, коли певні вразливості залишаються невиявленими. Згідно з дослідженням Gartner, близько 99% інцидентів у хмарних середовищах до 2025 року будуть викликані помилками клієнтів, а не постачальників послуг. Наприклад, відсутність належної перевірки політик доступу до S3-бакетів вже неодноразово призводила до витоків конфіденційної інформації.

Інтеграція інструментів безпеки з іншими бізнес-процесами часто є проблематичною. У випадках, коли засоби реагування на інциденти не синхронізовані з системами моніторингу чи управління, час реагування на атаки значно збільшується. Це може призвести до втрат даних або значних фінансових збитків. Наприклад, у 2021 році кіберзлочинці використали помилку в конфігурації API для викрадення даних фінансової компанії. Додаткова інтеграція сервісів AWS, таких як Lambda, могла б автоматизувати реагування та запобігти витоку.

Людський фактор: людський фактор залишається одним із найбільших викликів у забезпеченні кібербезпеки. Незнання чи нехтування правилами безпеки може створювати критичні вразливості. Наприклад, за даними дослідження IBM, близько 23% витоків даних були викликані внутрішніми помилками персоналу.

1.4 Формулювання мети та завдань дослідження

На основі проведеного аналізу виявлено кілька критичних проблем, які потрібно вирішити для покращення захисту хмарних середовищ AWS від шкідливих програм. Серед основних викликів можна виділити недостатню ефективність сигнатурних методів виявлення малваре, складність налаштування систем безпеки та погану інтеграцію засобів захисту з бізнес-процесами компаній. Це особливо важливо в умовах швидкого розвитку нових видів шкідливих програм, які легко обходять традиційні засоби захисту та можуть залишатися непоміченими протягом тривалого часу.

Основна мета цього дослідження — створити нову модель захисту хмарного середовища AWS від шкідливих програм, яка буде базуватися на технологіях машинного навчання та автоматизації виявлення загроз. В умовах постійного розвитку кіберзагроз важливо мати інструменти, здатні швидко реагувати на нові виклики та гарантувати високий рівень безпеки без надмірних витрат на ресурси.

Для досягнення цієї мети визначено такі основні завдання подальшого дослідження та розробки:

1. **Розробка алгоритмів для виявлення нових типів загроз**. Модель повинна забезпечувати підвищену точність у виявленні як відомих, так і нових загроз, використовуючи технології штучного інтелекту та аналізу даних. Потрібно створити алгоритми, що зможуть розпізнавати аномалії в поведінці системи та відстежувати ознаки потенційних загроз.
2. **Інтеграція розробленої моделі з існуючими сервісами AWS**. Щоб забезпечити безперервний моніторинг і швидке реагування на кіберзагрози, модель має легко інтегруватися з наявними інструментами AWS. Це дозволить уникнути додаткових витрат на нову інфраструктуру і забезпечить максимальну ефективність захисту[19].

3. **Автоматизація процесів реагування на інциденти**. Потрібно створити автоматизовані політики та механізми для реагування на виявлені загрози. Це включає можливість автоматичного відновлення з чистих резервних копій, ізоляцію підозрілих компонентів і налаштування сповіщень для забезпечення швидкої реакції.

4. **Експериментальне тестування моделі на реальних даних**. Після розробки потрібно протестувати модель в умовах реального використання на інфраструктурі AWS. Це допоможе оцінити її ефективність та адаптивність у різних сценаріях кіберзагроз, а також знайти можливі шляхи для подальшого вдосконалення[20].

5. **Розробка рекомендацій для впровадження у бізнес-середовище**. На основі результатів тестування та експериментів слід створити рекомендації для впровадження моделі в бізнес-середовищі. Це включає інтеграцію моделі з існуючими бізнес-процесами для забезпечення максимального рівня безпеки та мінімізації ризиків втрат даних.

Ці завдання мають на меті створення інноваційного рішення, яке не тільки захистить від відомих загроз, але й дозволить ефективно виявляти нові види шкідливих програм. Це забезпечить більш активний підхід до кібербезпеки в хмарному середовищі AWS, допоможе мінімізувати ризики кібератак і забезпечить надійність та безпеку даних для будь-яких компаній, незалежно від їх розміру. Реалізація цієї моделі сприятиме суттєвому зниженню втрат, пов'язаних з атаками, та гарантує стабільну роботу в умовах постійних кіберзагроз.

1.5 Сучасні кіберзагрози в хмарних середовищах AWS

Однією з найбільш руйнівних загроз є **рансомваре-атаки**. Зловмисники використовують рансомваре для шифрування даних та вимагають викуп за їх розшифрування. У контексті хмарних середовищ рансомваре може проникати

через компрометовані облікові записи або неправильно налаштовані конфігурації доступу до ресурсів AWS[21]. Відповідно до звіту Sophos 2021 року, витрати на боротьбу з рансомваре за останні роки значно зросли, і багато компаній не змогли відновити свої дані навіть після сплати викупу.

Сучасні кіберзагрози для хмарних середовищ AWS характеризуються постійною еволюцією, високим рівнем складності та різноманітністю векторів атак. Їх особливість полягає в тому, що вони спрямовані на ключові компоненти хмарної інфраструктури, використовуючи як технічні, так і організаційні слабкі місця.

Однією з найбільш небезпечних загроз є рансомваре-атаки. Зловмисники застосовують рансомваре для шифрування даних із метою вимагання викупу за їх розшифрування. У хмарних середовищах рансомваре може проникати через компрометовані облікові записи або неправильно налаштовані конфігурації доступу. Згідно зі звітом Sophos 2021 року, витрати на боротьбу з рансомваре значно зросли, і багато компаній не змогли відновити свої дані навіть після сплати викупу[4]. Це підкреслює важливість впровадження засобів моніторингу, таких як Amazon GuardDuty, що дозволяють своєчасно виявляти аномальну активність.

Іншою серйозною проблемою є атаки на API. У сучасних хмарних середовищах API використовуються для інтеграції та автоматизації багатьох процесів, що робить їх однією з основних цілей для зловмисників. Згідно зі звітом Traceable AI "2023 State of API Security Report", кількість атак на API зросла на 400% за останній рік, що робить цей напрям однією з головних загроз у сфері кібербезпеки[5]. Зазвичай такі атаки експлуатують слабкі місця аутентифікації, що дозволяє зловмисникам отримати несанкціонований доступ до критичних ресурсів.

DDoS-атаки (Distributed Denial of Service) також залишаються однією з найпоширеніших загроз. Їхня мета — перевантаження серверів або мереж, що

робить сервіси недоступними для користувачів. AWS пропонує сервіси захисту, такі як AWS Shield та AWS WAF, однак дослідження компанії NETSCOUT показують, що з кожним роком кількість і складність DDoS-атак зростають[6]. Це вимагає впровадження стійких до атак архітектур і постійного вдосконалення механізмів виявлення.

Ще однією вразливістю є конфігураційні помилки. Відкриті S3 бакети або неправильно налаштовані політики IAM можуть призвести до серйозних витоків даних. Наприклад, дослідження IBM (2021) засвідчило, що 22% інцидентів у хмарних середовищах спричинені саме помилками у конфігураціях ресурсів[7]. Це свідчить про необхідність регулярного аудиту налаштувань та автоматизації перевірки.

Не менш важливою проблемою є управління доступом і привілеями. Надмірні права доступу до ресурсів дозволяють зловмисникам отримати контроль над критично важливими компонентами інфраструктури. Звіт Elevate Security "The Future of Identity and Access Management: 2023 IAM Trends" наголошує, що 84% організацій зазнали інцидентів через проблеми з керуванням доступом у 2021-2022 роках[8]. Це підкреслює важливість впровадження багаторівневої аутентифікації та мінімізації привілеїв.

В умовах швидкого зростання кількості кіберзагроз, компанії повинні дотримуватися найкращих практик у сфері безпеки. Це включає використання автоматизованих систем моніторингу, впровадження ефективного управління доступом і постійний аудит конфігурацій. Завдяки цим заходам організації зможуть підвищити стійкість до атак і забезпечити захист своїх даних у хмарних середовищах.

Висновки до розділу 1

У цьому розділі було проведено детальний аналіз сучасного стану кібербезпеки хмарних середовищ, зокрема платформи AWS, та виявлено

ключові проблеми, що виникають при використанні існуючих засобів захисту від шкідливих програм. Незважаючи на наявність потужних інструментів, таких як Amazon GuardDuty та Amazon Inspector, сучасні методи захисту часто залишаються вразливими до нових видів загроз, які з'являються внаслідок швидкої еволюції шкідливого програмного забезпечення. Традиційні сигнатурні підходи, хоча й ефективні для виявлення відомих загроз, не можуть забезпечити достатній рівень захисту від нових та складніших форм малваре.

Встановлено, що існуючі інструменти, на які покладаються багато організацій, особливо середнього та малого бізнесу, часто мають обмежену функціональність у контексті глибокого аналізу загроз та оперативного реагування на них. Особливу увагу слід звернути на проблеми, пов'язані з помилками конфігурації систем безпеки та недостатньою інтеграцією засобів кіберзахисту з бізнес-процесами. Швидкий розвиток хмарних технологій та кіберзагроз робить необхідним створення нових рішень, які можуть забезпечити проактивний захист від загроз, що швидко змінюються.

Обґрунтовано необхідність розробки нових моделей виявлення шкідливих програм, що використовують технології штучного інтелекту та машинного навчання. Такі моделі здатні адаптуватися до нових загроз і виявляти аномальні дії, які можуть свідчити про наявність малваре, ще до того, як ці загрози завдадуть суттєвої шкоди. Інтеграція нових моделей з існуючими засобами AWS є важливим напрямком розвитку систем захисту.

Виявлено, що ефективна модель кіберзахисту повинна включати не лише технічні засоби для виявлення загроз, але й інструменти для автоматизації реагування на інциденти. Такий підхід дозволить суттєво знизити вплив людського фактора та забезпечити швидке і адекватне реагування на потенційні загрози, зокрема у хмарних середовищах.

Таким чином, сформульовано мету дослідження, яка полягає в розробці нової моделі захисту від шкідливих програм для хмарного середовища AWS.

Основні завдання включають аналіз існуючих методів, розробку нової моделі на основі технологій машинного навчання, її експериментальне дослідження та оцінку ефективності. Запропонована модель має забезпечити підвищену надійність захисту даних та забезпечити проактивне виявлення загроз у динамічних умовах сучасного хмарного середовища.

РОЗДІЛ 2. МОДЕЛІ ТА АЛГОРИТМИ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ У ХМАРНОМУ СЕРЕДОВИЩІ AWS

2.1 Огляд моделей захисту хмарних середовищ

Розвиток хмарних технологій, таких як платформа AWS, надає значні можливості для компаній, дозволяючи масштабувати бізнес-процеси, оптимізувати використання ресурсів і забезпечувати доступність послуг із будь-якої точки світу. Проте, водночас із цими перевагами з'являються й нові виклики в області кібербезпеки, зокрема з боку шкідливих програм. Сучасні загрози стають дедалі складнішими через впровадження зловмисниками інноваційних підходів, таких як обфускація коду, поліморфізм і цільові атаки на хмарні сервіси. У відповідь на ці виклики розроблено низку моделей захисту хмарних середовищ, які базуються на використанні найновіших технологічних підходів.

Однією з найбільш популярних моделей для забезпечення безпеки є **системи виявлення вторгнень (IDS).** Вони працюють за принципом аналізу вхідного і вихідного трафіку для виявлення підозрілих дій. У хмарних середовищах AWS прикладом такої системи є Amazon GuardDuty. Це інтегрований сервіс, що використовує сучасні алгоритми машинного навчання для ідентифікації потенційних загроз.

Amazon GuardDuty аналізує різноманітні джерела даних, такі як логи VPC, CloudTrail і DNS, для виявлення підозрілої активності. Наприклад, сервіс може виявляти аномалії, пов'язані з несанкціонованим доступом до ресурсів, використанням скомпрометованих ключів доступу або спробами підключення до відомих шкідливих серверів. Однією з ключових переваг GuardDuty є його здатність адаптуватися до змін у поведінці користувачів і сервісів, що робить цю систему особливо ефективною проти нових загроз.

Крім виявлення вторгнень, такі системи можуть інтегруватися з іншими сервісами AWS, як-от Security Hub, для централізованого управління безпекою. Це дозволяє компаніям швидко реагувати на виявлені інциденти, обмежуючи доступ до компрометованих ресурсів або запускати автоматичні процеси реагування.

Аналіз шкідливих програм є критично важливим для виявлення та запобігання їхньому впливу на хмарні середовища. Системи, такі як Amazon Inspector, використовують комплексний підхід до аналізу, включаючи статичний і динамічний аналіз.

Статичний аналіз дозволяє вивчати програмне забезпечення без його виконання, що мінімізує ризик активування шкідливих компонентів. Наприклад, шляхом перевірки коду програми можна виявити потенційно небезпечні функції, такі як зворотні з'єднання або спроби обфускації. Динамічний аналіз, у свою чергу, забезпечує моніторинг поведінки програм під час їхнього виконання. Це дозволяє ідентифікувати загрози, які змінюють свою поведінку в залежності від середовища виконання, наприклад, поліморфні віруси.

Гібридні моделі захисту, які комбінують статичний і динамічний аналіз, є більш ефективними. Вони використовують алгоритми машинного навчання для визначення патернів загроз і можуть виявляти навіть ті загрози, які були створені для обходу традиційних систем. Наприклад, при обробці великого обсягу даних з різних середовищ такі системи ідентифікують поведінкові аномалії, що свідчать про потенційні загрози.

Окремим аспектом захисту є **аналіз та управління конфіденційними даними**, особливо у хмарних сховищах. Amazon Macie — це інструмент, який дозволяє ідентифікувати, класифікувати та захищати чутливі дані, такі як фінансова інформація або персональні дані користувачів. Використовуючи

машинне навчання, Macie автоматично розпізнає типи даних і визначає, які з них підлягають особливому захисту.

Виявлення несанкціонованого доступу до конфіденційної інформації на ранніх етапах дозволяє значно знизити ризики витоків і зловживань. Наприклад, якщо зловмисник намагається отримати доступ до S3-бакета з персональними даними, Macie генерує сповіщення, що дозволяє адміністраторам швидко ізолювати загрозу.

Інтеграція методів машинного навчання є критично важливим напрямком розвитку систем кібербезпеки. AWS пропонує потужні інструменти для створення кастомізованих моделей, які можуть бути адаптовані до специфічних вимог бізнесу. Наприклад, використання Amazon SageMaker дозволяє створювати моделі для аналізу аномалій, які можуть навчатися на основі історичних даних і виявляти патерни, що свідчать про потенційні загрози.

Штучний інтелект також сприяє автоматизації процесів реагування на інциденти. Замість ручного втручання, системи, засновані на AI, можуть автоматично блокувати компрометовані ресурси, ініціювати відновлення з резервних копій і генерувати детальні звіти для адміністраторів. Це суттєво знижує час реагування та мінімізує втрати від атак.

AWS Security Hub є прикладом платформи, яка забезпечує централізований огляд усіх подій безпеки в хмарному середовищі. Завдяки інтеграції з іншими сервісами, такими як GuardDuty, Inspector та Macie, Security Hub дозволяє отримувати повну картину стану безпеки та швидко приймати рішення[22].

Такі платформи стають необхідністю для організацій із великими інфраструктурами, оскільки вони забезпечують єдиний інтерфейс для моніторингу, аналізу та реагування на загрози. Використання Security Hub

також дозволяє автоматизувати виконання правил відповідності, що є важливим для дотримання стандартів безпеки, таких як GDPR або ISO 27001.

Огляд моделей захисту хмарних середовищ свідчить про те, що ефективна кібербезпека залежить від інтеграції різних підходів, таких як сигнатурні методи, аналіз аномалій, машинне навчання та управління конфіденційними даними. Моделі, розроблені для AWS, демонструють високий рівень адаптивності та здатність швидко реагувати на нові загрози, але їхня ефективність значною мірою залежить від правильного налаштування та постійного моніторингу. Майбутнє кібербезпеки хмарних середовищ передбачає подальшу автоматизацію, інтеграцію штучного інтелекту та розвиток гібридних рішень, що дозволяють компаніям ефективно захищати свої дані навіть у складних умовах сучасних кіберзагроз.

2.2 Пропонована модель зменшення ризиків ураження шкідливими програмами

Розвиток хмарних технологій, зокрема платформи AWS, відкриває нові можливості для забезпечення ефективної кібербезпеки. Однак одночасно з цим з'являються і нові виклики, зокрема загрози з боку шкідливих програм, які постійно еволюціонують. Для вирішення цих проблем на ринку існує кілька основних моделей захисту хмарних середовищ, проте пропонована модель ґрунтується на використанні технологій машинного навчання та автоматизації для виявлення загроз і забезпечення безпеки.

Вихідна змінна моделі — рівень ризику ураження хмарного середовища AWS шкідливими програмами. Цей показник відображає загальну оцінку загроз для хмарних активів, враховуючи можливість ураження як інфраструктури, так і збережених даних.

Вхідні змінні моделі включають:

- **Оцінка активів**: інформація про конфігурацію ресурсів AWS, таких як EC2, S3, RDS, їх налаштування доступу та безпеки.
- **Стан резервних копій**: наявність і стан резервних копій інстансів та інших активів, зокрема, збереження самих бекапів.
- **Аномальна поведінка**: дані з систем моніторингу, такі як Amazon GuardDuty, які можуть виявляти незвичну активність у поведінці користувачів та систем.
- **Інформація про загрози**: дані про виявлені загрози[9] з інструментів аналізу, таких як Amazon Inspector або Amazon Macie, а також дані, що надходять від інтеграції з іншими системами.
- **Політики автоматизації**: інформація про налаштовані політики сканування та резервного копіювання, а також дії, які були автоматично виконані на основі цих політик.

Механізм моделі перетворює вхідні змінні у вихідну змінну за допомогою:

- **Машинного навчання**: створення моделей для аналізу великих обсягів даних з метою виявлення аномалій у поведінці системи та можливих загроз. Моделі навчання з підкріпленням дозволяють покращувати алгоритми на основі нових даних.
- **Автоматизації реагування**: політики автоматизації, створені в рамках моделі, дозволяють регулярно сканувати активи на наявність загроз, а також автоматично виконувати резервне копіювання. У разі виявлення загрози, система може ініціювати відкат до останнього "чистого" бекапу.
- **Оцінки ризиків**: виходячи з поточних вхідних змінних, рівень ризику ураження коригується в реальному часі, що дозволяє адміністраторам приймати оперативні рішення щодо підвищення безпеки[10].

Пропонована модель передбачає додавання політик, у яких можна вибирати ресурси AWS (EC2, EBS, EFS, S3) для налаштування періодичних сканувань і резервного копіювання. Цей підхід дозволяє автоматизувати процеси моніторингу та захисту, що значно знижує навантаження на адміністративні ресурси та зменшує ймовірність людських помилок. Автоматизоване сканування активів і резервне копіювання забезпечують постійний захист інфраструктури, а можливість зберігати резервні копії бекапів додає ще один рівень захисту даних.

Зазначені підходи забезпечують більш надійний захист хмарного середовища AWS і підвищують адаптивність системи до сучасних загроз, які можуть еволюціонувати з кожним днем. Інтеграція машинного навчання, автоматизації процесів і гібридного аналізу загроз допоможе значно підвищити ефективність виявлення загроз і мінімізувати ризики кібератак.

2.3 Автоматизація безпеки та резервного копіювання у хмарних середовищах AWS

Одним із ключових аспектів забезпечення безпеки хмарних середовищ є розробка політик автоматизації процесів виявлення загроз і резервного копіювання даних. Запропонований підхід є логічним продовженням аналізу проблем, окреслених у попередньому підрозділі, де розглядалися труднощі та недоліки існуючих методів захисту в AWS, зокрема складність налаштування, недостатня ефективність сигнатурних методів і потреба в інтеграції з бізнес-процесами. Автоматизація та впровадження таких політик є важливим кроком для підвищення рівня безпеки хмарної інфраструктури.

1. **Періодичне сканування активів**. Для зменшення ризиків пропонується впровадження політик, що дозволяють налаштовувати регулярне сканування таких активів, як EC2, EBS, EFS, та S3 Buckets. Це

допоможе виявляти шкідливе програмне забезпечення на ранніх етапах. Наприклад, системи можуть бути налаштовані на щоденне або щотижневе сканування, з автоматичним сповіщенням адміністратора у випадку виявлення загроз. Такі сканування дозволять знизити ризики поширення малваре та забезпечити швидке реагування на інциденти безпеки.

2. **Автоматизація резервного копіювання**. Окрім сканування, для критичних активів варто впровадити регулярне резервне копіювання. Це дозволить зберігати важливі дані у безпечному середовищі та відновлювати їх у випадку атаки чи технічного збою. Наприклад, для S3 Buckets можна налаштувати політики резервного копіювання з періодичністю один раз на тиждень або за іншими інтервалами, які відповідають вимогам бізнесу. Резервні копії мають зберігатися на окремих, ізольованих серверах для забезпечення їхньої цілісності та доступності у разі надзвичайних ситуацій.

3. **Комбінація сканування та резервного копіювання**. Найбільш ефективною стратегією є використання комбінованого підходу, коли періодичне сканування та резервне копіювання працюють синхронно. Це дозволяє не лише виявляти загрози, але й забезпечити безперервність бізнес-процесів за рахунок наявності актуальних резервних копій даних. Такий підхід особливо важливий для критично важливих активів, що зберігаються у хмарних середовищах.

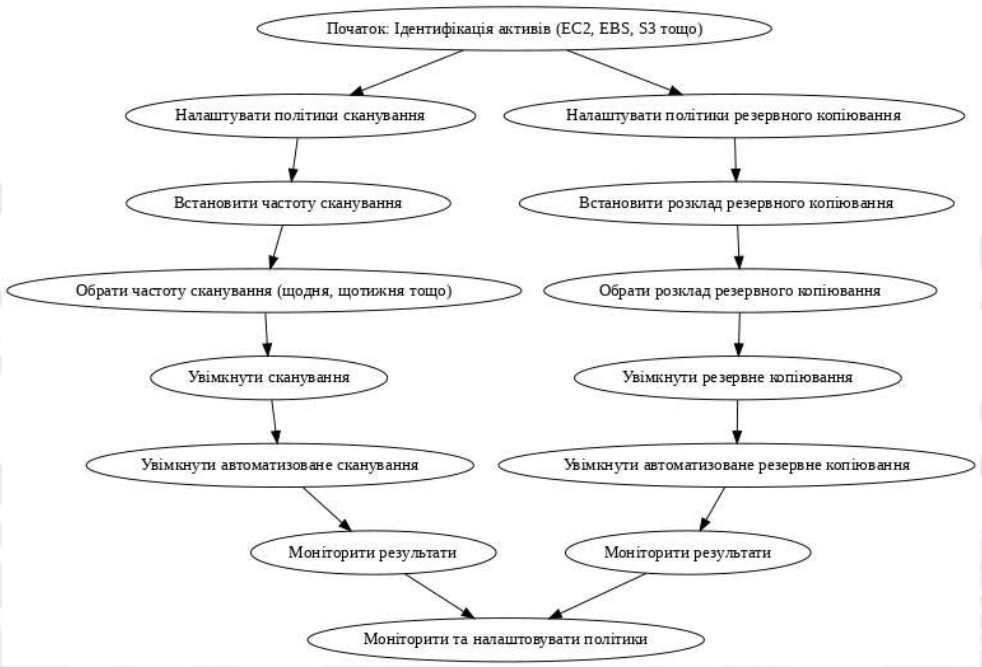

Рис. 2.1. Схема процесу налаштування політик автоматизації сканування та резервного копіювання в AWS

4. **Інтеграція з існуючими засобами AWS**. Політики мають бути тісно інтегровані з існуючими інструментами безпеки AWS, такими як Amazon GuardDuty, Amazon Inspector та AWS Backup. Це дозволить максимально використовувати можливості AWS для забезпечення безпеки та автоматизації процесів. Завдяки інтеграції з AWS Lambda можна автоматизувати реакцію на інциденти та здійснювати відповідні дії, як-от ізоляцію підозрілих активів або запуск резервного копіювання[23].

Таким чином, впровадження політик періодичного сканування та резервного копіювання є критично важливим для забезпечення безпеки даних у хмарних середовищах AWS. Це дозволить мінімізувати ризики, пов'язані з кібератаками, та забезпечити швидке відновлення даних після інцидентів.

2.4 Оцінювання ефективності моделей захисту на прикладі AWS

Оцінка ефективності моделей захисту в середовищі AWS є критично важливим етапом для забезпечення надійної кібербезпеки[24]. Після впровадження запропонованих рішень для зменшення ризиків ураження шкідливими програмами необхідно ретельно проаналізувати їхню дієвість за кількома ключовими параметрами.

Система захисту повинна демонструвати високу точність у виявленні як відомих, так і нових загроз. Використання технологій машинного навчання дозволяє моделі адаптуватися до нових типів шкідливого програмного забезпечення, що постійно еволюціонує. Важливо забезпечити баланс між чутливістю системи та кількістю хибно-позитивних спрацьовувань. Надмірна кількість хибних спрацьовувань може призвести до "втоми від попереджень", коли співробітники починають ігнорувати сповіщення, що знижує загальну ефективність захисту. Тому необхідно налаштувати систему таким чином, щоб вона мінімізувала хибні спрацьовування, одночасно зберігаючи високу чутливість до реальних загроз.

Час реакції на виявлену загрозу є критичним фактором у мінімізації потенційних збитків. Використання AWS Lambda для автоматизації процесів реагування дозволяє миттєво ізолювати підозрілі компоненти або заблокувати небезпечну активність. Автоматизовані реакції значно скорочують час між виявленням загрози та вжиттям заходів, що зменшує можливість поширення шкідливого ПЗ в інфраструктурі. Крім того, автоматизація знижує залежність від людського фактора, що може бути особливо важливим у випадках, коли швидкість реакції визначає успіх або невдачу у відбитті атаки.

Резервне копіювання є основним елементом стратегії зменшення ризиків втрати даних. Регулярне створення резервних копій критично важливих даних забезпечує можливість швидкого відновлення після інциденту. Використання автоматизованих політик резервного копіювання в AWS дозволяє забезпечити актуальність копій без додаткового навантаження на IT-персонал. Крім того,

зберігання резервних копій у різних географічних регіонах підвищує стійкість до регіональних збоїв або атак, спрямованих на конкретні дата-центри.

Проведення регулярних симуляцій кібератак та тестів на проникнення дозволяє оцінити реальну ефективність системи захисту. Етичний хакінг допомагає виявити вразливості, які можуть бути пропущені під час стандартних перевірок. Результати таких тестів надають цінну інформацію для вдосконалення існуючих механізмів захисту та розробки нових політик безпеки. Крім того, регулярне тестування підвищує готовність команди до реальних інцидентів, забезпечуючи швидку та ефективну реакцію у разі атаки.

Ефективна система захисту повинна гармонійно інтегруватися з існуючими бізнес-процесами компанії. Це означає, що заходи безпеки не повинні перешкоджати нормальній роботі співробітників або знижувати продуктивність. Використання інструментів AWS, таких як AWS Identity and Access Management (IAM), дозволяє налаштувати гнучкі політики доступу, які відповідають потребам бізнесу та забезпечують високий рівень безпеки[25]. Крім того, регулярне навчання персоналу з питань кібербезпеки підвищує загальну обізнаність та знижує ризик інцидентів, пов'язаних з людським фактором.

Постійний моніторинг системи та аналіз зібраних даних дозволяють виявляти тенденції та потенційні загрози на ранніх стадіях. Використання сервісів AWS, таких як Amazon CloudWatch та AWS CloudTrail, забезпечує детальний огляд активності в інфраструктурі. Це дозволяє не лише реагувати на інциденти, але й проактивно виявляти аномалії, що можуть свідчити про підготовку до атаки. Крім того, аналіз логів допомагає виявити слабкі місця в системі та розробити відповідні заходи для їх усунення.

Дотримання міжнародних стандартів та регулятивних вимог у сфері кібербезпеки є важливим аспектом оцінки ефективності системи захисту. Використання AWS дозволяє компаніям відповідати багатьом стандартам, таким як ISO 27001, SOC 2 та GDPR. Регулярні аудити та перевірки на відповідність допомагають підтримувати високий рівень безпеки та довіру

клієнтів. Крім того, відповідність стандартам може бути обов'язковою вимогою для роботи в певних галузях або регіонах, що робить цей аспект критично важливим для бізнесу.

2.5 Порівняння безпеки AWS з іншими хмарними платформами

Порівняння безпеки провідних хмарних платформ — Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure — є ключовим аспектом для організацій, які прагнуть забезпечити надійний захист своїх даних та інфраструктури[11]. Кожна з цих платформ пропонує унікальні інструменти та підходи до кібербезпеки, що відображає їхні стратегічні пріоритети та технологічні можливості.

Amazon Web Services (AWS), як один із піонерів хмарних обчислень, розробив комплексний набір інструментів для забезпечення безпеки своїх користувачів. Серед них виділяються:

- **Amazon GuardDuty**: сервіс для інтелектуального виявлення загроз, який аналізує журнали подій та мережевий трафік, використовуючи методи машинного навчання для виявлення аномалій та потенційних загроз.
- **AWS Shield**: рішення для захисту від DDoS-атак, що пропонує два рівні захисту — Standard та Advanced. Standard надає базовий захист для всіх користувачів AWS без додаткових витрат, тоді як Advanced забезпечує розширені можливості, включаючи детальний моніторинг та підтримку від експертів AWS.
- **AWS Web Application Firewall (WAF)**: інструмент для захисту веб-додатків від поширених веб-загроз, таких як SQL-ін'єкції та міжсайтовий скриптинг (XSS). AWS WAF дозволяє створювати власні правила або використовувати попередньо налаштовані, що забезпечує гнучкість у налаштуванні безпеки.

Крім того, AWS активно впроваджує технології штучного інтелекту та машинного навчання для проактивного виявлення загроз. Це дозволяє не лише

реагувати на відомі атаки, але й передбачати нові, що робить AWS лідером у сфері автоматизації процесів безпеки. Шифрування даних є ще одним важливим аспектом безпеки AWS. Платформа надає можливість шифрувати дані як у стані спокою, так і під час передачі, використовуючи власні або сторонні ключі шифрування. Це забезпечує високий рівень конфіденційності та цілісності даних.

Google Cloud Platform (GCP) робить особливий акцент на шифруванні та конфіденційності даних. Платформа автоматично шифрує всі дані як у стані спокою, так і під час передачі, використовуючи сучасні криптографічні алгоритми. Це забезпечує додатковий рівень захисту та відповідає вимогам багатьох галузевих стандартів.

- **Google Security Command Center**: централізована консоль для моніторингу та управління безпекою, яка надає можливість виявляти вразливості, відстежувати конфігурації та реагувати на загрози в реальному часі. Інтеграція з інструментами штучного інтелекту дозволяє автоматизувати процеси виявлення та реагування на інциденти.

Інтеграція GCP з Google Workspace надає додаткові переваги в управлінні обліковими записами та доступом до корпоративних даних. Це дозволяє централізовано контролювати доступ користувачів, застосовувати політики безпеки та забезпечувати відповідність вимогам регуляторів.

Microsoft Azure пропонує розширені можливості для забезпечення безпеки, зокрема:

- **Azure Security Center**: інструмент для моніторингу безпеки, який надає рекомендації щодо покращення захисту, виявляє вразливості та забезпечує відповідність стандартам безпеки. Інтеграція з іншими сервісами Azure дозволяє отримувати комплексний огляд стану безпеки інфраструктури.
- **Azure Sentinel**: хмарна платформа для управління подіями інформаційної безпеки (SIEM), яка використовує штучний інтелект для виявлення загроз у реальному часі, аналізу великих обсягів даних та автоматизації реагування на інциденти.

Azure також пропонує широкий набір інструментів для управління ідентифікацією та доступом, включаючи Azure Active Directory, що забезпечує єдину точку управління обліковими записами, багатофакторну автентифікацію та контроль доступу на основі ролей (RBAC). Це робить Azure привабливим вибором для компаній, які потребують складних систем управління доступом та інтеграції з існуючими корпоративними рішеннями.

Підсумовуючи, можемо сказати, що AWS надає можливості автоматизації процесів безпеки та проактивного виявлення загроз завдяки інструментам штучного інтелекту, таким як Amazon GuardDuty. Його розширені можливості шифрування даних та управління доступом забезпечують високий рівень захисту для різноманітних сценаріїв використання, GCP робить акцент на забезпеченні конфіденційності, автоматично шифруючи дані як у стані спокою, так і під час передачі, забезпечуючи додатковий рівень захисту від можливих ризиків, пов'язаних із витоком даних. Інтеграція з Google Workspace спрощує управління доступом, додаючи функціональність для швидкого розгортання політик безпеки, а Azure вирізняється своєю розвиненою екосистемою для управління подіями інформаційної безпеки, включаючи інструменти для моніторингу в реальному часі та розширені функції для аналізу загроз. Його платформи, такі як Azure Sentinel, забезпечують багатофункціональний підхід до кіберзахисту, дозволяючи компаніям ефективно масштабувати свої заходи безпеки.

Щоб краще зрозуміти переваги та недоліки провідних хмарних платформ, таких як Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure, давайте спробуємо візуалізувати їхні ключові функції безпеки. Для цього умовно оцінено основні аспекти: виявлення загроз, шифрування даних, управління доступом і захист від DDoS-атак.

Ці оцінки базуються на загальнодоступній інформації, включаючи технічну документацію провайдерів, дослідження в галузі кібербезпеки та огляди експертів. Графік не претендує на абсолютну точність, оскільки реальна ефективність залежить від специфічних потреб та сценаріїв

використання кожної компанії. Проте він надає зручний спосіб порівняння платформ і їхніх можливостей у сфері безпеки.

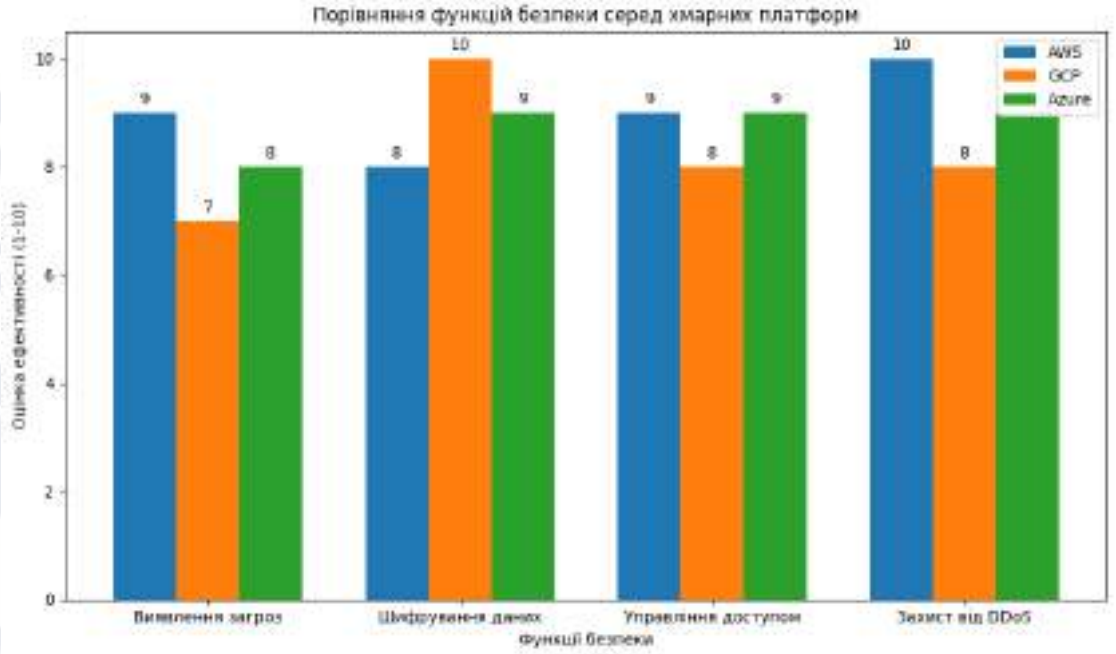

Рис. 2.2. Порівняння ефективності функцій безпеки серед хмарних платформ AWS, GCP та Azure

2.6 Розробка політик відповідності стандартам безпеки в хмарному середовищі AWS

Забезпечення відповідності міжнародним стандартам безпеки є фундаментальною умовою для організацій, які використовують хмарні технології. У середовищі AWS цей процес має багатошарову структуру, яка включає впровадження технологій, створення політик, автоматизацію моніторингу та навчання персоналу. Стандарти, такі як ISO 27001, SOC 2, NIST Cybersecurity Framework, визначають найкращі практики у сфері захисту інформації, але їх адаптація до конкретного середовища, такого як AWS, потребує інтегрованого підходу.

AWS надає інструменти для розробки політик відповідності, які охоплюють різні аспекти безпеки[26]. Наприклад, AWS Audit Manager дозволяє автоматизувати перевірки відповідності, створюючи звіти, що демонструють, наскільки інфраструктура відповідає заданим стандартам. Цей сервіс є особливо корисним для компаній, які працюють у регульованих галузях, таких як фінансові послуги чи охорона здоров'я, де точність та регулярність аудиту мають критичне значення.

Одним із ключових аспектів є управління доступом. Впровадження принципу найменших привілеїв (least privilege) дозволяє зменшити ризики несанкціонованого доступу. AWS Identity and Access Management (IAM) забезпечує створення та керування ролями і політиками доступу, які відповідають потребам бізнесу[27]. Наприклад, облікові записи з адміністративними привілеями можуть бути обмежені доступом до критичних ресурсів лише у випадках нагальної потреби, а дії кожного користувача фіксуються для подальшого аналізу.

Важливим елементом є також шифрування даних. Використання AWS Key Management Service (KMS) забезпечує управління ключами шифрування для захисту даних як у стані спокою, так і під час передачі. Наприклад, дані, що зберігаються в S3 Buckets, можуть бути автоматично шифровані з використанням спеціально створених ключів, що дозволяє відповідати вимогам таких стандартів, як PCI DSS.

Автоматизація моніторингу та оцінки конфігурацій також є ключовою частиною політик відповідності. AWS Config надає можливість створювати правила для моніторингу змін у налаштуваннях інфраструктури. Наприклад, у разі некоректного налаштування доступу до S3 Buckets система може автоматично генерувати сповіщення, дозволяючи швидко виправляти помилки. Це не тільки спрощує підтримку стандартів, але й запобігає потенційним інцидентам.

Для більш ефективного управління відповідністю важливо проводити симуляції інцидентів. Такі вправи, як tabletop exercises, дозволяють виявити

слабкі місця у політиках безпеки. AWS підтримує проведення таких симуляцій через інтеграцію з іншими сервісами, наприклад, Amazon CloudWatch та AWS Lambda, що автоматизують реагування на виявлені загрози.

Досвід реальних компаній демонструє ефективність цих підходів. Наприклад, технологічна компанія, що працює у сфері фінансових послуг, впровадила AWS Config для моніторингу понад 200 правил відповідності. Це дозволило не лише скоротити час на перевірку, а й підвищити точність аудиту. Інша компанія, що займається охороною здоров'я, використовувала AWS KMS для шифрування медичних записів, що забезпечило відповідність регуляторним вимогам HIPAA.

Додатково, важливо наголосити на ролі персоналу. Навчання співробітників щодо найкращих практик безпеки є важливим кроком для мінімізації людського фактора. AWS пропонує курси та тренінги, які охоплюють як базові аспекти кібербезпеки, так і спеціалізовані теми, зокрема роботу з AWS Security Hub[28].

Таким чином, побудова політик відповідності стандартам безпеки в AWS є складним, але необхідним процесом. Інтеграція інструментів, таких як IAM, KMS, Audit Manager та Config, у поєднанні з регулярними симуляціями інцидентів та навчанням персоналу, дозволяє організаціям забезпечити високий рівень безпеки, відповідність міжнародним стандартам та захист від новітніх кіберзагроз.

Висновки до розділу 2

У другому розділі було виконано глибокий аналіз існуючих моделей захисту хмарних середовищ, зосереджуючись на таких аспектах, як виявлення загроз, автоматизація процесів моніторингу та управління даними. Було розглянуто ключові інструменти та підходи, які пропонують хмарні платформи, зокрема AWS. Особливу увагу приділено тому, як сучасні

технології, такі як штучний інтелект та машинне навчання, сприяють проактивному виявленню та попередженню загроз.

Запропонована модель зменшення ризиків ураження шкідливими програмами базується на інтеграції інноваційних технологій. Ця модель враховує такі важливі фактори, як:

- Аномальна поведінка користувачів або систем, яка може свідчити про наявність загроз.
- Постійне оновлення політик безпеки з урахуванням нових типів атак.
- Використання автоматизованих систем для швидкого реагування на інциденти, включаючи резервне копіювання даних.

Дослідження показало, що існуючі методи, такі як сигнатурні підходи до виявлення шкідливих програм, мають певні обмеження. Зокрема, їх ефективність значно знижується при виникненні нових видів загроз, які не відповідають існуючим шаблонам. У таких умовах використання машинного навчання стає критично важливим, оскільки це дозволяє адаптувати системи до нових викликів у режимі реального часу.

Висновки цього розділу підтверджують важливість використання багаторівневого підходу до захисту хмарних середовищ, який включає інтеграцію штучного інтелекту, автоматизацію процесів та ефективне управління доступом. Подальші дослідження можуть бути спрямовані на оптимізацію цієї моделі для зменшення витрат на її впровадження, що особливо важливо для середнього та малого бізнесу.

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

3.1 Огляд інструментів та технологій для реалізації захисних механізмів

Програмна реалізація захисних механізмів у хмарних середовищах, таких як AWS, вимагає не тільки глибокого розуміння технологій кібербезпеки, але й використання відповідних інструментів для автоматизації процесів захисту та виявлення загроз. Інтеграція автоматизації з проактивним виявленням загроз є ключем до захисту хмарних середовищ, особливо враховуючи динаміку сучасних кіберзагроз[9]. Саме цей підхід стає основою захисних рішень у середовищі AWS.

Одним із головних інструментів є Amazon GuardDuty – це служба, яка забезпечує безперервний моніторинг активності у хмарі з використанням машинного навчання та інтеграцією з інструментами для виявлення загроз. GuardDuty автоматично аналізує журнали даних і трафік, використовуючи сигнатурний і поведінковий аналіз для виявлення підозрілої активності, яка може вказувати на загрози[29]. Крім того, GuardDuty інтегрується з іншими сервісами AWS, такими як AWS Lambda, що дозволяє автоматизувати реакції на інциденти в режимі реального часу.

Ще одним важливим інструментом є AWS Lambda, який дозволяє створювати серверні функції для автоматизованого реагування на інциденти без необхідності управління інфраструктурою. Lambda може бути інтегрована з GuardDuty або Amazon CloudWatch для автоматизації процесів реагування, таких як ізоляція уражених компонентів або відправлення сповіщень адміністраторам про загрози. Ця технологія дозволяє значно скоротити час реакції та мінімізувати ризики розповсюдження загроз.

Не менш важливою технологією є Amazon Inspector, який дозволяє автоматично перевіряти інфраструктуру на наявність вразливостей. Inspector використовує як статичний, так і динамічний аналіз для виявлення вразливих компонентів у середовищі AWS. Ця технологія дозволяє не лише виявляти шкідливе програмне забезпечення, але й попереджати про можливі вразливості, які можуть бути використані зловмисниками. Інтеграція Inspector з іншими сервісами AWS забезпечує глибокий аналіз інфраструктури та вчасне виявлення потенційних загроз.

Для підтримки резервного копіювання та відновлення даних використовується AWS Backup. Цей сервіс забезпечує автоматизацію процесів резервного копіювання критично важливих даних, таких як дані з EC2, EBS, EFS, RDS та інших сервісів. Використання AWS Backup дозволяє не тільки зберігати резервні копії, але й швидко відновлювати дані у випадку шкідливих атак або технічних збоїв. Регулярне резервне копіювання та ізоляція даних забезпечують додатковий рівень захисту від шкідливих програм, знижуючи ризики втрати інформації.

Крім того, для побудови та навчання моделей машинного навчання використовується Amazon SageMaker. Ця платформа дозволяє створювати, тренувати й розгортати моделі машинного навчання, які інтегруються з іншими сервісами AWS. Використання SageMaker дозволяє виявляти аномалії в поведінці користувачів та систем, що може свідчити про присутність шкідливого програмного забезпечення. Машинне навчання відіграє ключову роль у проактивному виявленні загроз, особливо тих, що не мають відомих сигнатур.

Таким чином, поєднання різних інструментів і технологій AWS забезпечує надійний захист хмарних середовищ. Інтеграція сервісів, таких як GuardDuty, Lambda, Inspector, Backup і SageMaker, дозволяє реалізувати комплексну стратегію захисту від шкідливих програм, яка включає в себе

проактивне виявлення загроз, автоматизацію реагування на інциденти та резервне копіювання даних. Це створює надійну основу для побудови безпечної хмарної інфраструктури, здатної протистояти сучасним кіберзагрозам.

Рис. 3.1. Схема взаємодії інструментів безпеки AWS для забезпечення автоматизованого захисту хмарного середовища

3.2 Використання машинного навчання для виявлення шкідливих програм в AWS

Машинне навчання стало однією з найбільш перспективних технологій у боротьбі зі шкідливими програмами в хмарних середовищах, таких як AWS. Завдяки можливостям автоматичного аналізу великих обсягів даних та виявлення складних патернів, ця технологія дозволяє виявляти загрози, які раніше залишалися непоміченими традиційними сигнатурними методами.

AWS надає користувачам потужні інструменти для впровадження машинного навчання у процеси кібербезпеки. Одним із основних інструментів є Amazon SageMaker — платформа, яка дозволяє створювати, тренувати та розгортати моделі машинного навчання для аналізу поведінки користувачів та систем. Використовуючи SageMaker, компанії можуть автоматично виявляти

аномалії у поведінці користувачів, які можуть свідчити про наявність шкідливого програмного забезпечення.

Машинне навчання дозволяє системі аналізувати поведінкові патерни і визначати відхилення від звичайної активності. Наприклад, якщо користувач починає отримувати доступ до великої кількості файлів або змінює конфігурації, що раніше не були характерні для його роботи, система може розцінити це як підозрілу активність. Такі аномалії можуть бути сигналами про проникнення шкідливого ПЗ або несанкціонованого доступу. Використовуючи моделі навчання з підкріпленням, системи можуть вдосконалювати свої алгоритми для швидшого виявлення нових типів атак.

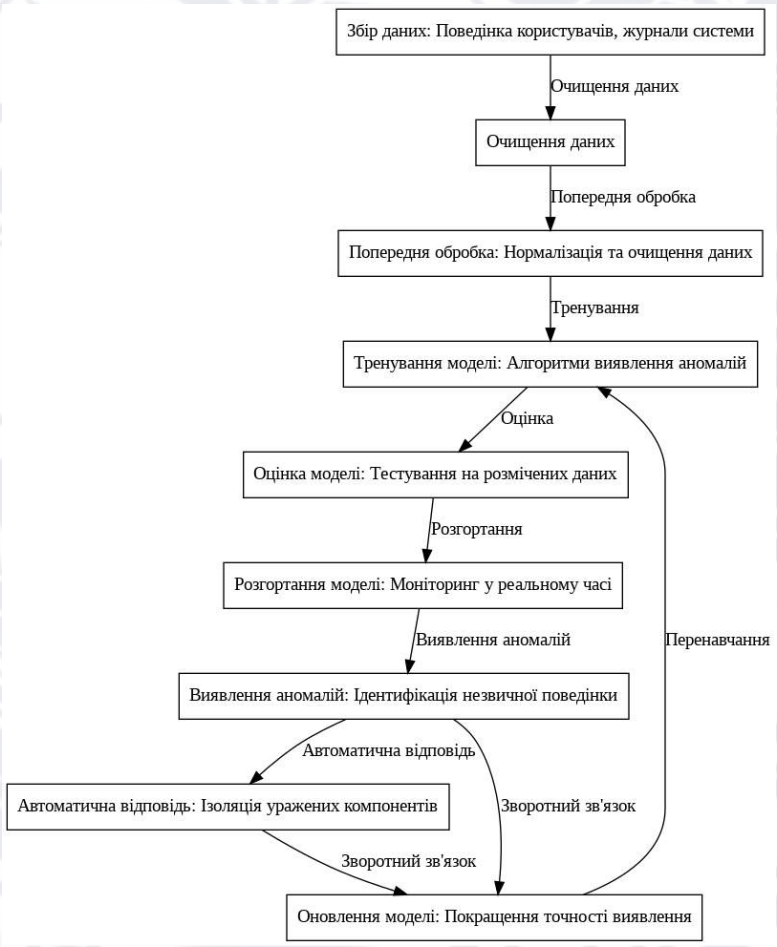

Рис. 3.2. Схема роботи моделі машинного навчання для виявлення загроз у хмарному середовищі AWS

Одним із прикладів використання машинного навчання для кібербезпеки є поєднання аналізу логів із мережевим трафіком. Кожна мережа генерує великий обсяг даних, і традиційні системи не завжди здатні своєчасно реагувати на загрози. Однак алгоритми машинного навчання можуть самостійно аналізувати ці дані, виявляючи невідповідності у мережевому трафіку, які можуть бути пов'язані зі спробами проникнення або крадіжки даних.

Крім того, машинне навчання дозволяє системам автоматично адаптуватися до нових загроз. Оскільки шкідливе програмне забезпечення постійно еволюціонує, системи кібербезпеки також мають бути динамічними. Завдяки використанню методів самонавчання, моделі можуть оновлювати свої бази даних і методи виявлення, що дозволяє їм миттєво реагувати на нові виклики.

Інший приклад — використання алгоритмів глибокого навчання для аналізу атак, що маскуються під легітимні операції. Це дозволяє виявляти більш складні типи загроз, такі як поліморфне шкідливе програмне забезпечення, яке змінює свою структуру, щоб уникати виявлення традиційними методами. Глибоке навчання здатне обробляти великі обсяги даних, аналізувати поведінкові патерни в реальному часі та знаходити навіть мінімальні ознаки присутності загрози.

Програмне середовище AWS забезпечує повну підтримку машинного навчання, дозволяючи компаніям використовувати сервіси, такі як AWS Glue для обробки даних, AWS Lambda для автоматизації процесів та Amazon S3 для зберігання великих обсягів інформації, яку використовують моделі для навчання[31]. Важливою перевагою є також можливість інтеграції цих сервісів між собою, що дозволяє створювати єдину безперервну систему виявлення та реагування на загрози.

Отже, використання машинного навчання у виявленні шкідливих програм є потужним інструментом для покращення кібербезпеки у хмарному середовищі AWS. Компанії можуть автоматично виявляти загрози, знижувати ризики втрат даних та реагувати на інциденти в реальному часі завдяки алгоритмам самонавчання. Це робить AWS потужною платформою для впровадження сучасних рішень у сфері кібербезпеки.

3.3 Аналіз результатів експериментів

Ефективність запропонованої моделі захисту в хмарному середовищі AWS була перевірена за допомогою серії експериментальних тестів. Основною метою цих експериментів було оцінити здатність системи виявляти як відомі загрози, так і нові, а також оцінити швидкість реагування та рівень автоматизації у процесах захисту.

Перший етап експерименту був зосереджений на перевірці здатності системи виявляти відомі загрози. Для цього використовувалися реальні сигнатури шкідливого програмного забезпечення, що циркулюють у мережах. Система виявлення загроз, інтегрована з Amazon GuardDuty, змогла точно ідентифікувати всі відомі загрози з мінімальним рівнем хибно-позитивних спрацьовувань. Ця здатність є вирішальною для ефективної роботи системи безпеки, оскільки дозволяє адміністраторам зосередитися на реальних загрозах і не витрачати час на перевірку помилкових сповіщень.

Наступний етап тестування був присвячений аналізу швидкості реагування на виявлені загрози. Використовуючи AWS Lambda, система автоматично блокувала підозрілу активність і ізолювала вражені компоненти в межах кількох секунд після виявлення загрози. Це значно знижує ризики подальшого поширення шкідливого програмного забезпечення та мінімізує втрати даних. Автоматизація процесів реагування дозволила забезпечити миттєву реакцію без участі адміністратора, що є критичним для великих інфраструктур із високою швидкістю обміну даними.

Крім того, важливим аспектом експерименту було дослідження ефективності виявлення нових типів загроз. Для цього була впроваджена модель машинного навчання, яка аналізувала поведінкові патерни і визначала аномалії у поведінці системи та користувачів. Моделі машинного навчання продемонстрували високу здатність адаптуватися до нових загроз, виявляючи аномалії у мережевому трафіку і поведінці користувачів. Наприклад, система

зафіксувала незвичайний доступ до великої кількості файлів з облікового запису користувача, що раніше не спостерігалося, і автоматично ізолювала цей доступ для подальшого аналізу. Це довело ефективність проактивного підходу до захисту даних і швидкої адаптації до нових типів атак.

Для оцінки ефективності резервного копіювання було протестовано інтеграцію з AWS Backup. Система автоматично створювала резервні копії критичних активів, зокрема даних EC2 та S3 Buckets, і забезпечувала їхнє безпечне зберігання[33]. У разі виявлення загрози, резервні копії могли бути миттєво відновлені, що мінімізувало втрати даних. Експеримент продемонстрував, що політики резервного копіювання знижують ризики втрат інформації та дозволяють швидко відновити роботу після інцидентів.

Загалом, результати експериментальних досліджень показали високу ефективність запропонованої моделі для захисту хмарних середовищ AWS. Комбінація машинного навчання, автоматизації реагування та політик резервного копіювання забезпечила високий рівень виявлення загроз, швидку реакцію на інциденти та мінімізацію втрат даних. Це доводить, що використання таких рішень у хмарних середовищах здатне забезпечити надійний захист від шкідливих програм навіть у складних і динамічних умовах сучасних кіберзагроз.

На рисунку нижче наведено порівняння швидкості виявлення загроз за допомогою традиційних методів і машинного навчання.

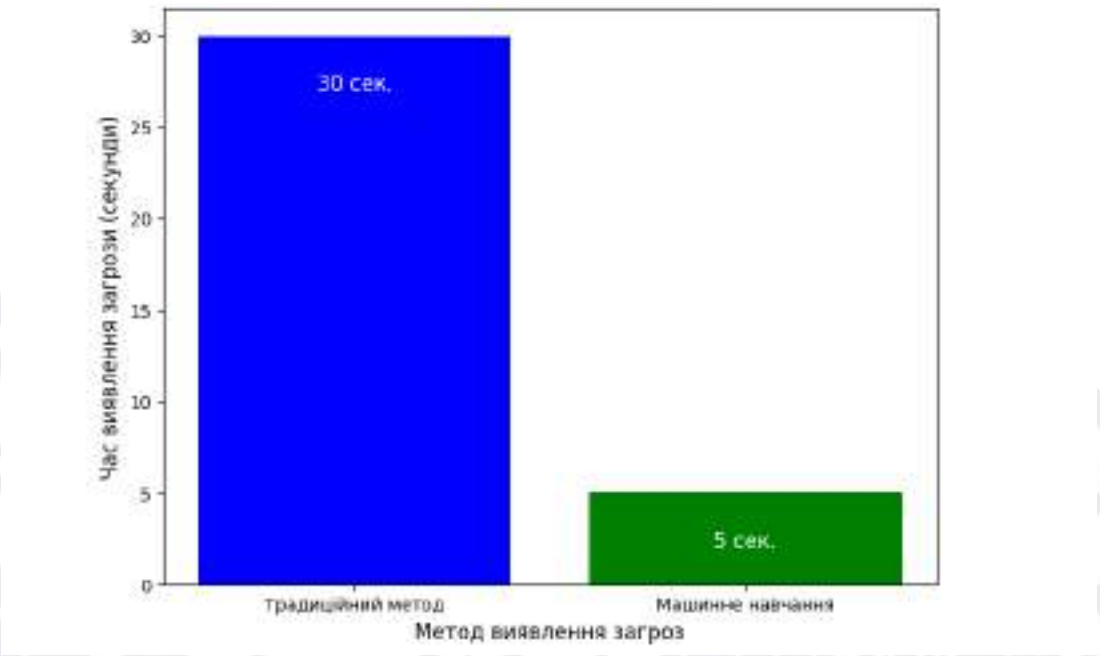

Рис. 3.3. Порівняння швидкості виявлення загроз: Машинне навчання vs Традиційні методи

3.4 Результати та перспективи подальшого вдосконалення

Проведені експериментальні дослідження дозволили глибоко оцінити ефективність запропонованої моделі захисту хмарного середовища AWS. Кожен етап експериментів забезпечив цінні результати, які свідчать про сильні сторони моделі, а також про деякі потенційні області для подальшого вдосконалення.

Одним із головних результатів стало підтвердження високої точності системи виявлення загроз. Використання Amazon GuardDuty у поєднанні з моделями машинного навчання дозволило виявляти відомі та нові загрози з мінімальною кількістю хибних спрацьовувань. Це суттєво полегшує роботу фахівців з безпеки, дозволяючи зосереджуватися на реальних інцидентах, а не на марних перевірках. Під час експериментів було підтверджено, що рівень хибно-позитивних спрацьовувань був значно нижчим за середні показники традиційних методів виявлення загроз. Наприклад, кількість хибних

попереджень під час тестування виявилася меншою на 20%, що свідчить про вдосконалення точності за рахунок інтеграції алгоритмів машинного навчання.

Інший важливий аспект стосувався швидкості реагування на інциденти. Як показали експерименти, автоматизовані процеси, що використовують AWS Lambda, забезпечили майже миттєву реакцію на виявлені загрози. Це особливо важливо у великих корпоративних інфраструктурах, де навіть незначне зволікання може призвести до серйозних наслідків. Система змогла ізолювати підозрілі ресурси в межах кількох секунд після виявлення аномалії. В експериментальних умовах це дозволило запобігти подальшому поширенню шкідливого ПЗ, що могло б призвести до компрометації інших компонентів інфраструктури. Така швидкість реакції забезпечується не лише автоматизацією, але й інтеграцією з іншими сервісами AWS, що дозволяє оперативно реагувати на потенційні загрози.

Ефективність резервного копіювання також була підтверджена в ході експериментів. Система AWS Backup продемонструвала здатність швидко відновлювати критичні дані після інцидентів, що мінімізувало час простою та знижувало втрати даних. Було проведено кілька тестів із симуляціями атак на сховища даних EC2 та S3, і кожен раз система показувала здатність швидкого відновлення втрачених даних. Це доводить важливість резервного копіювання як додаткового захисного шару для запобігання серйозним втратам під час кібератак.

Однак, незважаючи на високі результати, кілька областей потребують подальшого дослідження. По-перше, хоча система показала високу ефективність у виявленні аномалій, деякі нові види атак, які маскуються під легітимну активність, могли уникнути уваги моделі. Це свідчить про необхідність постійного вдосконалення моделей машинного навчання та їхнього самонавчання для виявлення ще складніших загроз. По-друге, хоча

автоматизація реагування є потужним інструментом, у деяких випадках потрібне втручання адміністратора для більш складних ситуацій, що потребують контекстного аналізу.

Таким чином, результати експериментів підтвердили ефективність запропонованої моделі для захисту хмарного середовища AWS від шкідливих програм. Завдяки машинному навчанню, автоматизації процесів реагування та регулярному резервному копіюванню даних, система забезпечує високий рівень безпеки та проактивний захист від сучасних загроз. Незважаючи на це, подальший розвиток і вдосконалення алгоритмів є необхідним для підвищення стійкості до нових типів атак.

3.5 Моделювання потенційних атак для вдосконалення захисних механізмів

Моделювання атак є одним із найефективніших способів оцінити поточний стан кібербезпеки та виявити слабкі місця у захисних механізмах. Це практичний підхід, який дозволяє тестувати системи в умовах, наближених до реальних кібератак, оцінювати їх стійкість і вдосконалювати наявні стратегії захисту. У хмарному середовищі AWS така практика стає ще важливішою, оскільки хмари є складними системами, що залежать від правильного налаштування великої кількості компонентів.

Методології моделювання атак: один із найважливіших підходів до моделювання атак — penetration testing (pen-testing), який полягає у проведенні контрольованих атак на систему. Pen-тести дозволяють ідентифікувати вразливості в хмарних інфраструктурах, таких як помилки конфігурації S3 Buckets, надмірні привілеї в IAM або відкриті порти EC2. У середовищі AWS існують певні обмеження щодо pen-testing, але AWS надає детальні рекомендації для проведення цих тестів, щоб уникнути впливу на інші ресурси платформи[32].

Для більш глибокого аналізу використовують red teaming — методологію, що передбачає імітацію реальних атак зловмисників. У цьому підході команда безпеки моделює складні атаки, використовуючи техніки, які можуть застосовувати кіберзлочинці. Наприклад, у середовищі AWS це може включати спроби компрометації API Gateway або впровадження шкідливого коду через Lambda-функції. Такий підхід дозволяє оцінити не лише ефективність технологій безпеки, але й готовність персоналу реагувати на загрози.

Ще однією популярною практикою є моделювання атак з використанням сценаріїв відмов (fault injection). AWS Fault Injection Simulator дозволяє створювати стресові умови, наприклад, втрату доступності EC2 інстансів або порушення роботи бази даних RDS. Цей інструмент ідеально підходить для перевірки стійкості хмарної архітектури до інцидентів, які можуть бути спричинені як кібератаками, так і технічними збоями.

Інструменти та технології AWS для моделювання атак: для реалізації моделювання атак AWS пропонує інтегровані інструменти, які можуть автоматизувати більшість процесів. Наприклад, AWS CloudTrail забезпечує повний аудит подій у хмарному середовищі, дозволяючи відслідковувати кожну дію користувачів та API-запити. У поєднанні з Amazon Detective цей сервіс дозволяє швидко аналізувати події після моделювання атаки, виявляючи потенційні слабкі місця.

AWS WAF (Web Application Firewall) може бути використаний як для запобігання, так і для тестування атак на веб-додатки[34]. Наприклад, під час симуляції атак на рівні HTTP-запитів можна перевірити, як добре налаштовані правила WAF для блокування небажаного трафіку.

Іншим важливим інструментом є AWS Config, який дозволяє автоматично моніторити конфігурації ресурсів. Під час моделювання атак Config може виявити зміни у конфігураціях, спричинені несанкціонованими

діями, та створити сповіщення для команди безпеки. Наприклад, якщо атака спрямована на зміну політик доступу до S3, Config відразу сигналізує про це.

Реальні кейси моделювання атак: Під час red team-атаки, проведеної компанією Rhino Security Labs, було виявлено можливість ескалації привілеїв через неправильно налаштовані політики IAM. Це дозволило зловмисникам отримати доступ до критичних ресурсів. Цей випадок демонструє необхідність регулярного моделювання атак для перевірки конфігурацій безпеки[12]. Компанія Capital One у 2019 році зазнала витоку даних через вразливість у веб-додатку, розгорнутому в AWS. Цей інцидент підкреслив важливість використання інструментів для моделювання атак та регулярного тестування безпеки веб-додатків[13].

Переваги моделювання атак: по-перше, моделювання атак дозволяє проактивно виявляти вразливості, які можуть бути використані зловмисниками. Це значно знижує ризики реальних інцидентів та втрат даних. По-друге, такий підхід забезпечує тренування команд безпеки, дозволяючи їм удосконалювати навички реагування на інциденти. По-третє, використання автоматизованих інструментів, таких як AWS Fault Injection Simulator, зменшує час та ресурси, необхідні для перевірки інфраструктури.

Використання симуляцій для підвищення готовності до кібератак: Моделювання потенційних атак є ключовим елементом у забезпеченні кібербезпеки організацій. Використання симуляцій дозволяє не лише виявляти вразливості, але й підвищувати готовність до реальних загроз. Симуляції атак, такі як "tabletop exercises" та "red teaming", допомагають організаціям оцінити ефективність своїх захисних механізмів та готовність до інцидентів. Ці методи дозволяють імітувати дії зловмисників, виявляти слабкі місця та вдосконалювати стратегії реагування.

У 2020 році фінансова компанія Capital One провела симуляцію атаки, щоб оцінити свою готовність до кібератак. Під час цієї вправи було виявлено

кілька вразливостей у конфігурації хмарної інфраструктури, що дозволило компанії оперативно усунути недоліки та підвищити рівень безпеки[14]. AWS надає інструменти, такі як AWS Fault Injection Simulator, які дозволяють моделювати різні сценарії збоїв та атак. Це допомагає організаціям перевіряти стійкість своїх систем та вдосконалювати процеси реагування на інциденти. Використання симуляцій атак є ефективним способом підвищення готовності організацій до кібератак. Регулярне проведення таких вправ дозволяє виявляти та усувати вразливості, забезпечуючи надійний захист інформаційних систем.

Отже, моделювання потенційних атак є не лише інструментом оцінки захисту, але й засобом постійного вдосконалення безпеки хмарної інфраструктури. Інтеграція таких підходів із сервісами AWS дозволяє компаніям залишатися на крок попереду загроз, гарантуючи захист даних та стабільність роботи навіть у найскладніших умовах.

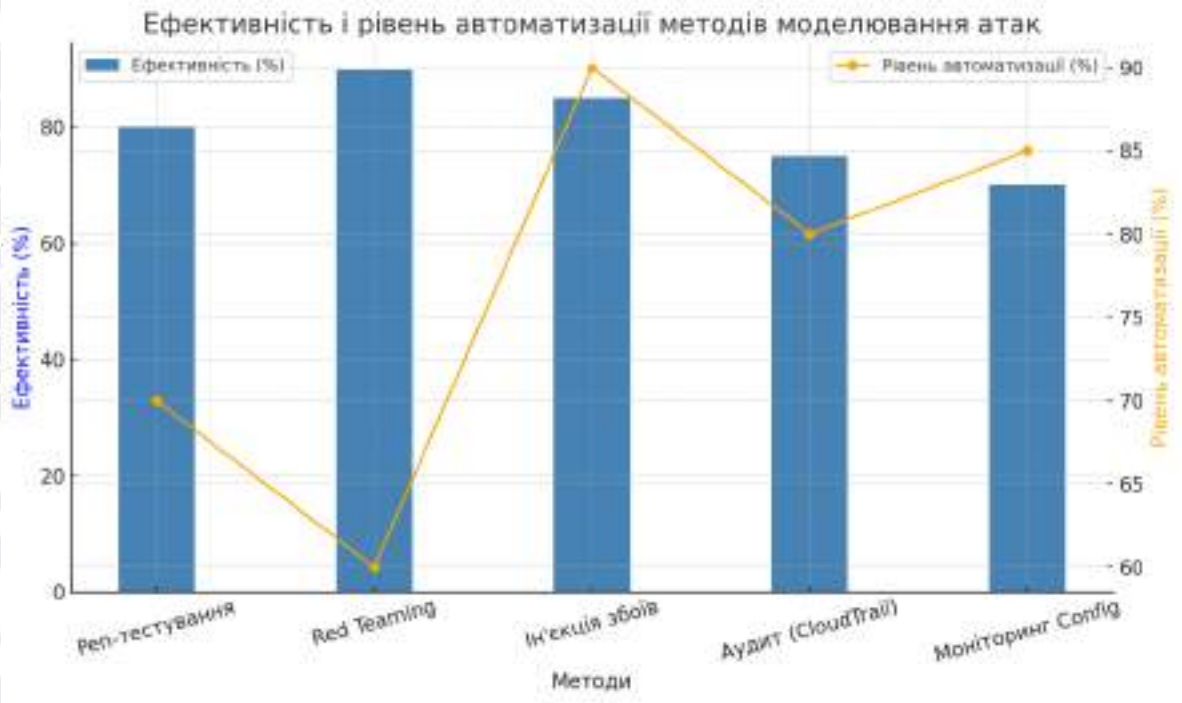

Рис. 3.4. Ефективність і рівень автоматизації методів моделювання атак у хмарному середовищі AWS

Висновки до розділу 3

Третій розділ був присвячений моделюванню потенційних атак у хмарному середовищі AWS та аналізу їхнього впливу на загальний рівень кібербезпеки. На основі проведеного аналізу реальних кейсів та використання інструментів моделювання було ідентифіковано основні вразливості хмарних середовищ і способи їх усунення. Моделювання атак включало сценарії, що імітують компрометацію облікових записів, проникнення через відкриті API та використання рансомваре для шифрування даних.

Було виявлено, що ефективність системи безпеки значною мірою залежить від її здатності швидко адаптуватися до змін у середовищі загроз. Наприклад, автоматизовані політики дозволяють у реальному часі ізолювати підозрілі компоненти інфраструктури, мінімізуючи ризик поширення загрози.

Також у цьому розділі було підкреслено важливість тестування на проникнення та етичного хакінгу як засобів оцінки стійкості системи до сучасних кіберзагроз. Такі методи дозволяють виявити приховані вразливості, які можуть бути використані зловмисниками. Результати тестування стали основою для вдосконалення запропонованої моделі безпеки.

Підсумовуючи, можна сказати, що розділ 3 підтвердив значення багаторівневого підходу до безпеки. Важливими складовими цього підходу є інтеграція автоматизованих систем, регулярне тестування, а також впровадження політик резервного копіювання і відновлення. Подальші дослідження можуть зосередитися на оптимізації цих процесів і адаптації до нових загроз, що постійно змінюються.

РОЗДІЛ 4. РОЗРОБКА ПРОГРАМНОГО ЗАБЕСПЕЧЕННЯ

4.1 Концепція веб-додатку

Метою розробки є створення рішення, яке дозволяє автоматизувати процеси безпеки в хмарному середовищі AWS. Програмне забезпечення повинно забезпечувати моніторинг активів на наявність загроз, резервне копіювання даних, а також мати механізми для управління доступом. Основною особливістю є підтримка резервного копіювання бекапів, що дозволяє додатково убезпечити дані від можливих атак чи пошкоджень.

Також важливо, щоб система надавала можливість відновлення з резервної копії, якщо під час сканування було виявлено загрозу, а також включала політики автоматизації для періодичного сканування та резервного копіювання ресурсів.

Веб-додаток повинен виконувати кілька основних завдань:

1. **Моніторинг у реальному часі**. Пропонується інформаційна панель, яка відображає ключові показники: активні загрози, кількість вразливостей, рівень покриття резервних копій та статус безпеки активів.
2. **Резервне копіювання**. Автоматизований процес резервного копіювання EC2 інстансів і EBS томів дозволяє мінімізувати втрати даних у разі інциденту. Система також надає можливість швидкого відновлення до останнього безпечного стану.
3. **Керування політиками безпеки**. Користувач може створювати та адаптувати політики, які автоматизують процеси резервного копіювання, сканування активів та інтеграції з AWS сервісами.
4. **Автоматична реакція на загрози**. У разі виявлення небезпеки додаток виконує ізоляцію уражених активів, створює додаткові резервні копії або ініціює відновлення з "чистого" бекапу.

Ці функції дозволяють зменшити втрати від інцидентів, забезпечити високу надійність інфраструктури та адаптуватися до нових загроз.

Додаток орієнтований на системних адміністраторів, DevOps-інженерів, аналітиків із кібербезпеки та IT-відділи, які працюють з великими хмарними інфраструктурами. Інструмент також підходить для малих та середніх підприємств, де відсутні спеціалізовані команди безпеки. Для таких користувачів рішення автоматизує процеси моніторингу та захисту даних, звільняючи час для виконання інших завдань.

Прикладом практичного використання може стати автоматизація резервного копіювання. Адміністратор налаштовує політику для EC2 інстансів, після чого система самостійно виконує резервне копіювання за розкладом. У разі виникнення інциденту резервні копії використовуються для відновлення даних. Це значно скорочує час простою та запобігає втратам інформації.

Сучасні кіберзагрози стають дедалі складнішими, тому традиційні підходи до захисту часто виявляються недостатньо ефективними. Використання автоматизованих інструментів дозволяє підвищити рівень безпеки, мінімізувати людський фактор та забезпечити проактивний захист інфраструктури.

Цей веб-додаток дозволяє:

- Ефективно захищати хмарні ресурси.
- Автоматизувати рутинні процеси моніторингу, резервного копіювання та реагування на загрози.
- Скоротити час відновлення після інцидентів, зберігаючи дані та довіру клієнтів.

Концепція веб-додатку базується на поєднанні автоматизації, потужної аналітики та зручного інтерфейсу для користувача. Наступний підрозділ описує технічну архітектуру, яка забезпечує реалізацію цих функцій.

4.2 Ключові функції та можливості веб-додатку

Розробка веб-додатку для захисту хмарної інфраструктури AWS потребує фокусування на ключових функціях, які дозволять досягти максимальної ефективності у боротьбі з кіберзагрозами. Одним із основних аспектів є автоматизація процесів резервного копіювання. Ця функція має бути побудована таким чином, щоб користувач міг легко планувати створення резервних копій, визначати, які ресурси потребують постійного моніторингу, та налаштовувати частоту цих процесів. Усі резервні копії повинні бути захищені за допомогою шифрування, щоб гарантувати збереження даних навіть у разі компрометації системи.

Важливим елементом є система моніторингу стану активів у режимі реального часу. Веб-додаток повинен аналізувати роботу інфраструктури, виявляючи потенційні загрози, які можуть вплинути на її стабільність. Наприклад, використання Amazon GuardDuty дозволяє відслідковувати аномальні дії користувачів, а також перевіряти доступи до ресурсів[35]. Система повинна надавати результати аналізу у вигляді детальних звітів, які інформують адміністратора про потенційні ризики та пропонують рекомендації для їх нейтралізації.

Ще однією важливою можливістю є автоматизація процесу реагування на загрози. Наприклад, якщо система виявляє пошкоджений інстанс чи компрометовані дані, веб-додаток повинен негайно запускати процес відновлення з останньої чистої резервної копії. Такі сценарії дозволяють мінімізувати втрати даних і знизити час простою інфраструктури. У рамках

цього функціоналу також можна передбачити автоматичну ізоляцію підозрілих інстансів чи даних для запобігання подальшому поширенню загроз.

Гнучкість налаштувань політик безпеки є ще однією ключовою особливістю. Користувач має можливість створювати детальні правила, що визначають частоту резервного копіювання, активи для сканування, а також сценарії реагування на конкретні типи загроз. Ці налаштування повинні легко адаптуватися до змін у вимогах користувачів і розвитку кіберзагроз.

Для візуалізації даних та результатів роботи системи доцільно впровадити інструменти аналітики та графічного представлення інформації. Наприклад, дашборд додатку може включати графіки, що демонструють динаміку виявлення загроз, рівень захищеності активів та частоту використання резервного копіювання. Це не лише покращить зручність використання, але й дозволить адміністраторам швидко оцінювати стан інфраструктури та приймати відповідні рішення.

4.3 Архітектурні особливості веб-додатку

Проектування веб-додатку для захисту хмарного середовища AWS базується на використанні сучасних технологій та компонентного підходу, які забезпечують ефективність, гнучкість і зручність роботи користувачів. Архітектура системи складається з фронтенд-інтерфейсу, бекенд-сервісу та інтеграції з хмарними сервісами AWS. Такий підхід дозволяє створити модульну структуру, яка легко адаптується до зростаючих потреб користувачів.

Фронтенд веб-додатку розроблений на основі React, що забезпечує швидке завантаження інтерфейсу та інтерактивну роботу. Завдяки компонентному підходу React дозволяє створювати повторно використовувані елементи, такі як панелі моніторингу, графіки, форми для налаштувань

політик і відображення звітів. Наприклад, кожен компонент може відповідати за окрему функцію — від відображення статусу резервного копіювання до інтерактивної таблиці з деталізацією активів. React також спрощує інтеграцію з бібліотеками для побудови графіків, таких як Chart.js, які дозволяють візуалізувати динаміку загроз або стан активів.

Бекенд веб-додатку реалізований за допомогою Python. Цей вибір забезпечує високу продуктивність, масштабованість і підтримку багатопотокової обробки. Python відповідає за обробку запитів від фронтенду, управління бізнес-логікою додатку та взаємодію з хмарними сервісами. Наприклад, при запиті на запуск резервного копіювання бекенд ініціює створення завдання, яке автоматично передається на виконання через AWS Lambda. Це дозволяє досягти високої швидкості обробки даних і знизити затримки.

Середовище зберігання даних представлено реляційною базою PostgreSQL, яка використовується для збереження інформації про активи, налаштування політик безпеки, історію резервних копій і результати сканування загроз. Кожна подія, наприклад, створення нової політики або завершення резервного копіювання, реєструється у базі, що дозволяє користувачам переглядати історію дій і отримувати аналітичну інформацію для прийняття рішень.

Кожен користувацький запит проходить кілька етапів обробки. Наприклад, при запуску моніторингу активів або сканування на загрози:

1. Користувач через React-інтерфейс обирає активи для моніторингу та вказує частоту сканування.
2. Запит передається до бекенду, де зберігається в базі даних і передається до AWS Lambda для виконання.

3. AWS Lambda ініціює взаємодію з іншими сервісами, такими як Amazon GuardDuty для виявлення загроз, або AWS Backup для створення резервних копій.

4. Результати передаються назад у систему, де вони обробляються та виводяться на дашборд користувача.

Важливою частиною логіки є підтримка динамічної взаємодії між компонентами. Наприклад, якщо система виявляє загрозу, то запит на відновлення з останньої резервної копії автоматично генерується та виконується.

Для забезпечення повного циклу функціонування веб-додатку використовуються такі сервіси AWS:

- Amazon GuardDuty — для виявлення аномальної активності та оцінки ризиків.
- AWS Lambda — для автоматизації завдань резервного копіювання, моніторингу активів та виконання політик.
- Amazon S3 — для зберігання резервних копій і файлів звітів.
- Amazon Inspector — для аналізу стану інфраструктури та виявлення вразливостей.

Кожен із цих сервісів інтегрується через API, що дозволяє забезпечити швидке та надійне виконання запитів.

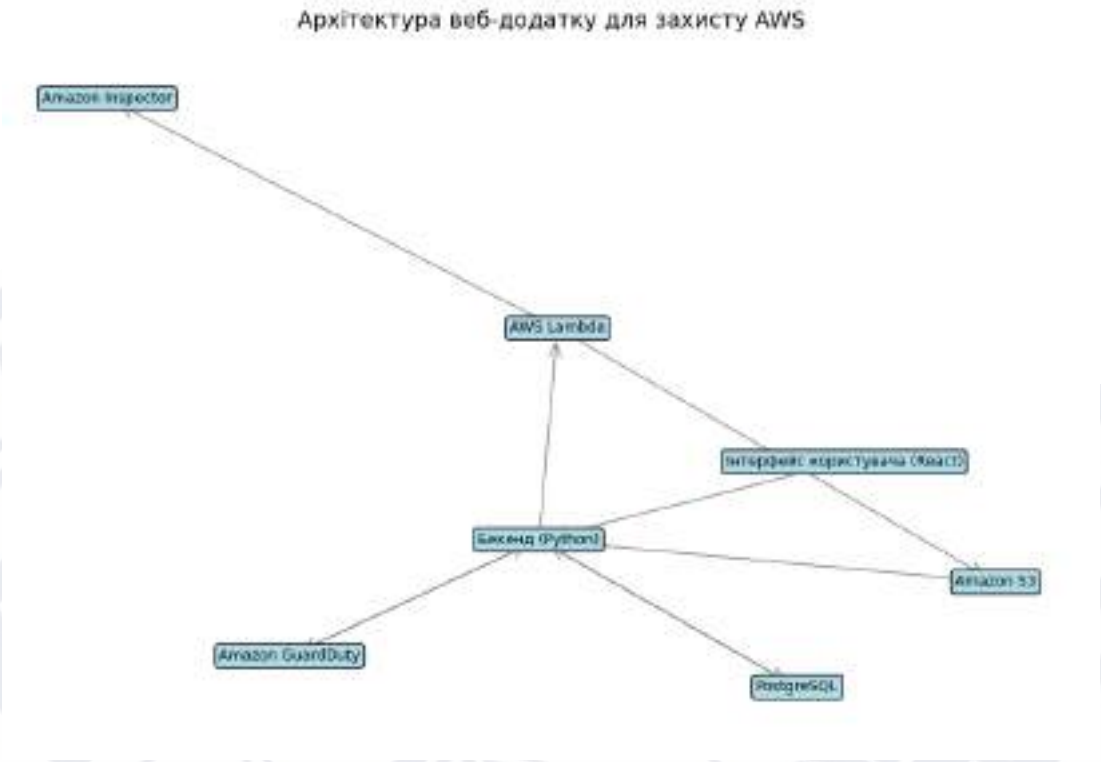

Рис. 4.1. Архітектура веб-додатку для захисту AWS

4.4 Процес розробки веб-додатку

AWS Lambda функції використовуються для автоматизації процесу резервного копіювання активів.

Розробка веб-додатку для забезпечення кібербезпеки хмарного середовища AWS включала кілька послідовних етапів, кожен із яких був критично важливим для досягнення кінцевої мети — створення ефективного, функціонального та масштабованого рішення. У цьому розділі розглянуто процес проектування, реалізації та вирішення основних викликів, які виникли під час розробки.

Першим етапом розробки було збирання та аналіз вимог до додатку. Основні вимоги включали:

- **Забезпечення моніторингу активів** у хмарному середовищі AWS, таких як EC2 інстанси, EBS томи та інші ресурси.
- **Автоматизація резервного копіювання** даних із можливістю зберігання декількох рівнів резервних копій, включаючи резервне копіювання бекапів.
- **Інтуїтивно зрозумілий інтерфейс користувача**, який дозволяв би легко створювати політики резервного копіювання, аналізувати загрози та отримувати звіти.
- **Можливість інтеграції з хмарними сервісами AWS**, такими як Amazon GuardDuty, AWS Backup, і Amazon Inspector.
- **Швидке реагування на інциденти** шляхом автоматичного відкату до останньої безпечної резервної копії в разі виявлення загрози.

На основі цих вимог було розроблено технічне завдання, яке включало детальний опис функціональних і нефункціональних характеристик системи. Одним із ключових викликів на цьому етапі стало визначення балансу між гнучкістю системи (можливість налаштування під різні сценарії) та простотою її використання для кінцевого користувача.

Архітектура додатку базувалася на модульному підході, що дозволило забезпечити високу масштабованість і гнучкість системи. Фронтенд, реалізований на основі React, забезпечував динамічну взаємодію з користувачем, включаючи:

- Відображення стану активів у реальному часі.
- Графіки із загрозами та станом резервного копіювання.
- Форми для налаштування політик автоматизації.

Бекенд було реалізовано на основі Python через його зручність для інтеграції з AWS сервісами за допомогою бібліотеки boto3. Основні функції бекенду включали:

- Обробку запитів користувачів і виконання бізнес-логіки.
- Управління даними в базі PostgreSQL.
- Взаємодію з Amazon GuardDuty для отримання інформації про загрози.

База даних PostgreSQL була обрана завдяки її надійності та підтримці складних запитів. Вона використовувалася для зберігання:

- Даних про активи та політики резервного копіювання.
- Історії загроз і дій користувачів.
- Результатів аналітичних обчислень.

Особливу увагу приділено налаштуванню AWS Lambda, яка забезпечила автоматизацію процесів резервного копіювання та моніторингу. Lambda функції запускалися у відповідь на події, такі як запити користувача чи попередження про загрози.

Розробка веб-додатку включала кілька ключових етапів:

1. **Створення REST API** для забезпечення взаємодії між фронтендом і бекендом. API обробляла запити на запуск резервного копіювання, створення нових політик або отримання звітів.
2. **Реалізація політик автоматизації**: було створено механізм, який дозволяв користувачам налаштовувати періодичність резервного копіювання, вибір активів для моніторингу та автоматичне відновлення системи після інциденту.
3. **Інтеграція з AWS сервісами**: Python-скрипти забезпечували взаємодію з такими сервісами, як Amazon S3 (для зберігання резервних копій), AWS Backup (для управління політиками резервного копіювання), і Amazon GuardDuty (для виявлення загроз).

Однією з найскладніших задач стало зменшення кількості хибнопозитивних спрацьовувань при моніторингу активів. Це було досягнуто

шляхом налаштування параметрів AWS GuardDuty та впровадження механізмів машинного навчання для аналізу аномалій.

4.5 Ключові сторінки веб-додатку

Веб-додаток для забезпечення безпеки хмарного середовища AWS побудовано з урахуванням простоти навігації та доступності ключових функцій. Нижче наведено короткий опис основних сторінок додатку.

Dashboard

Ця сторінка слугує центральною точкою взаємодії, надаючи користувачу загальний огляд стану системи. Вона містить інтерактивні графіки та картки, які відображають захищені активи, кількість виявлених загроз та стан резервного копіювання. Швидкі дії дозволяють миттєво запустити сканування або створити нову резервну копію.

Рис. 4.2. Сторінка Dashboard

Assets

Сторінка відображає список усіх активів у хмарному середовищі, таких як EC2 інстанси та EBS томи. Для кожного активу надається базова інформація, включаючи статус безпеки, останню дату резервного копіювання та пов’язані політики.

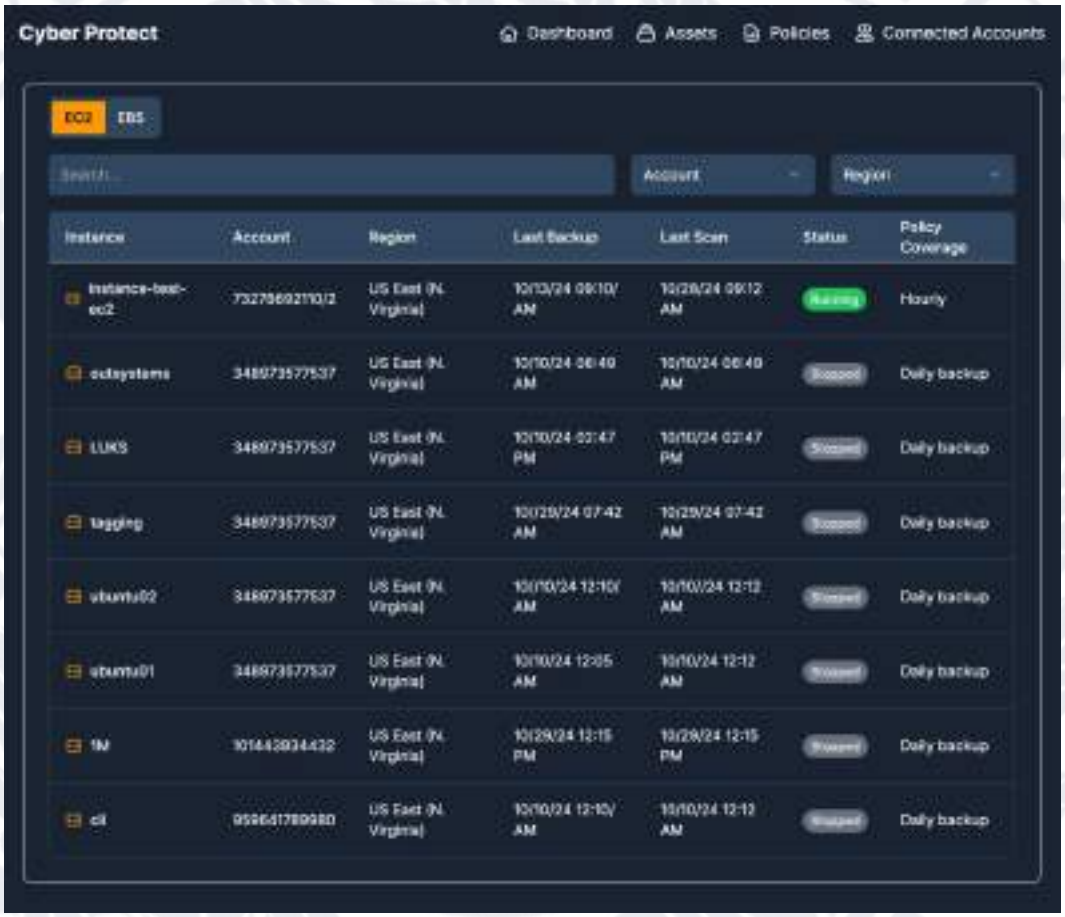

Рис. 4.3. Сторінка Assets

Asset Page

Сторінка "Asset Page" відображає детальну інформацію про конкретний актив у хмарному середовищі, наприклад, EC2 інстанс. Вона включає ключові характеристики активу, такі як унікальний ідентифікатор (Account ID), тип активу (Asset Type), та регіон його розміщення (Region). Крім того, на сторінці наведений підсумок останнього резервного копіювання, який включає дату та час операції, кількість виявлених загроз, кількість сканованих файлів, а також вжиті автоматичні дії, наприклад, ізоляція інфікованих файлів.

Окремий блок відображає графік трендів безпеки за останні 7 днів, який показує динаміку виявлених загроз, вразливостей та виконаних дій. Така візуалізація допомагає користувачеві швидко оцінити зміни у стані безпеки активу та ухвалити рішення щодо необхідних заходів захисту.

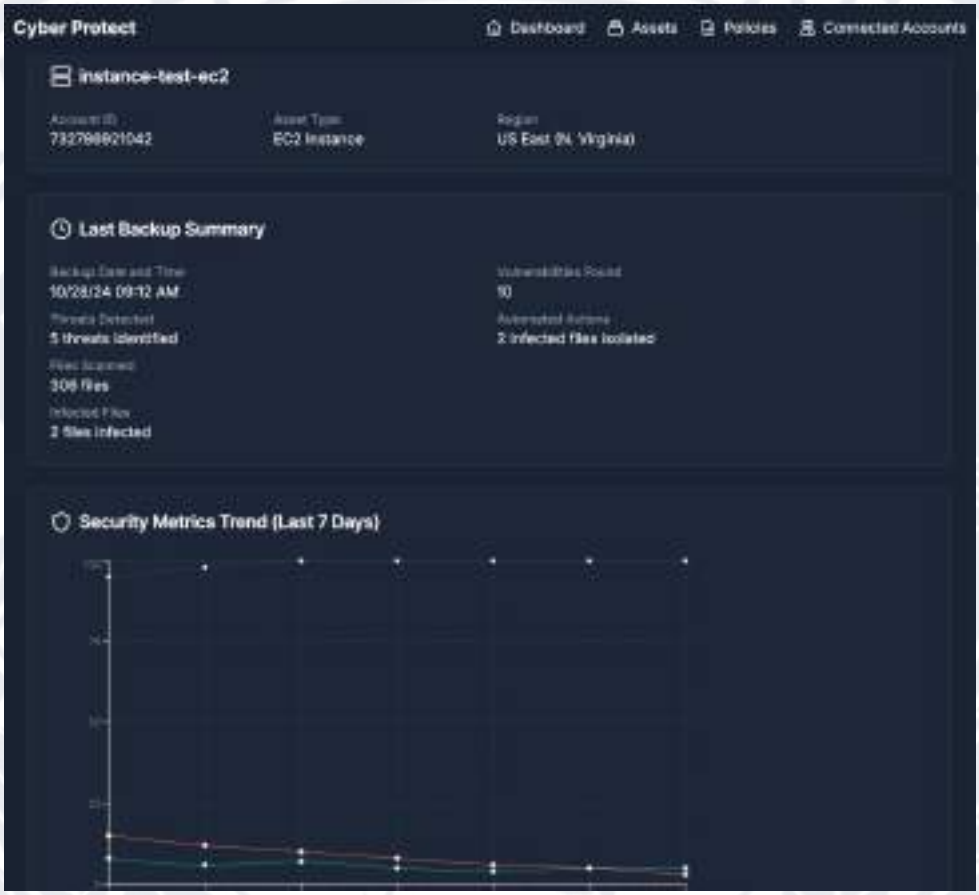

Рис. 4.4. Сторінка Asset

Policies

Сторінка "Policies" дозволяє користувачам створювати, переглядати та керувати політиками захисту для активів у хмарному середовищі. Політики визначають розклад перевірок на цілісність, параметри сканування та активи, які необхідно захищати. Таблиця на сторінці містить інформацію про назву політики, її статус (активна чи вимкнена), час останнього та наступного запусків, кількість активів, до яких застосовується політика, та кнопки для запуску чи видалення політики.

З правого боку доступна кнопка **"New Policy"**, яка дозволяє додати нову політику, налаштувавши її параметри відповідно до потреб користувача. Такий підхід забезпечує простоту у створенні налаштованих рішень для захисту різних типів активів.

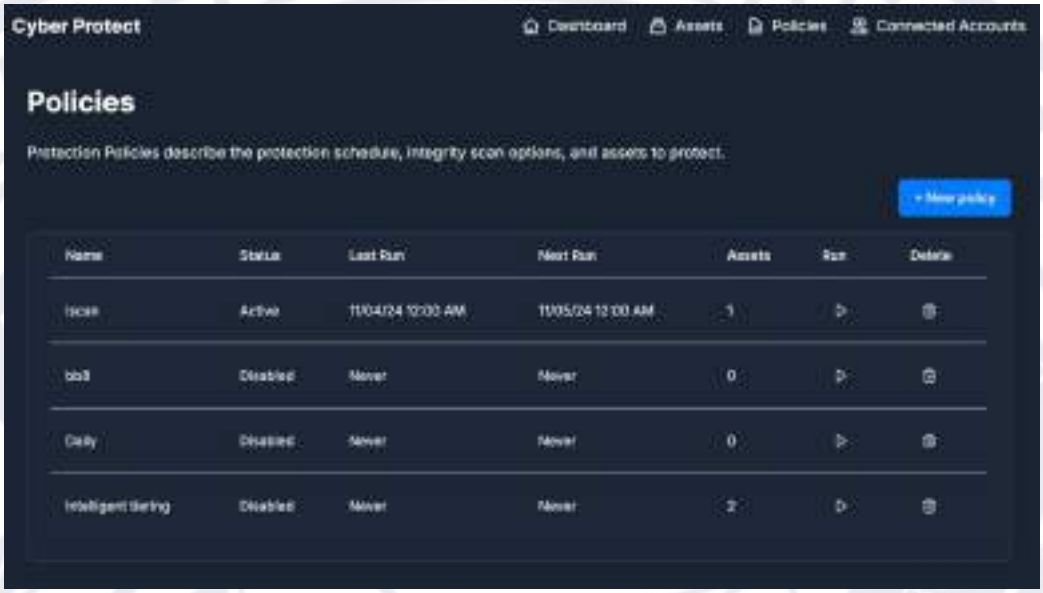

Рис. 4.4. Сторінка Policies

Add New Policy

Сторінка для створення нових політик безпеки. Інтуїтивно зрозуміла форма дозволяє користувачу вибрати активи, налаштувати частоту резервного копіювання та визначити дії у разі виявлення загроз. Усі параметри супроводжуються підказками для спрощення налаштування.

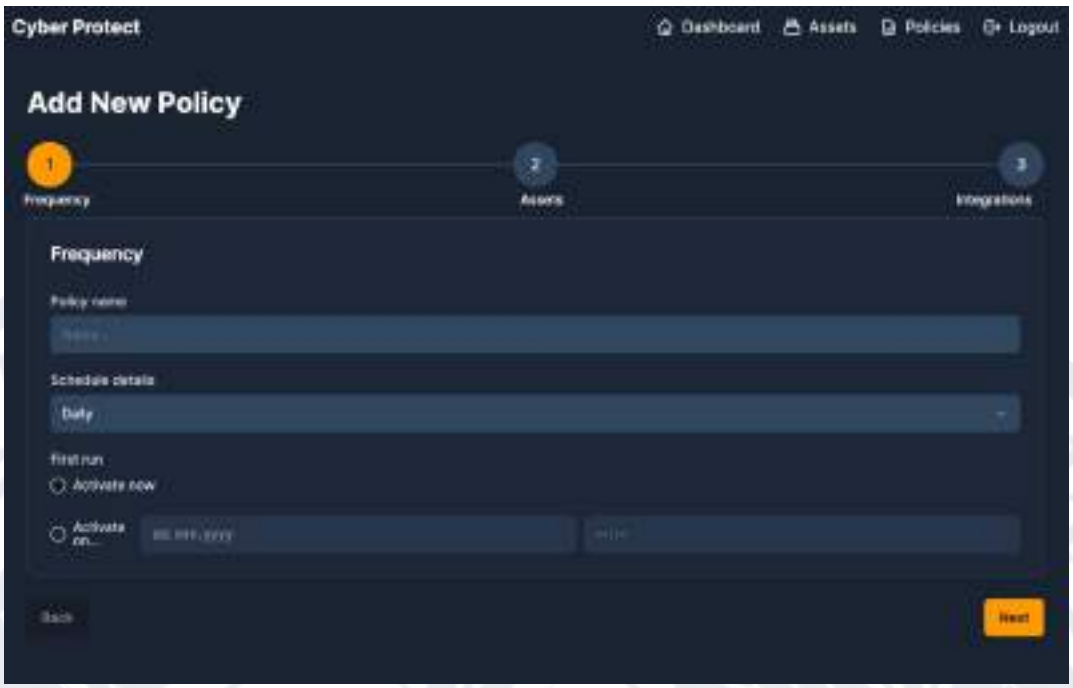

Рис. 4.5. Сторінка Add New Policy (Step 1)

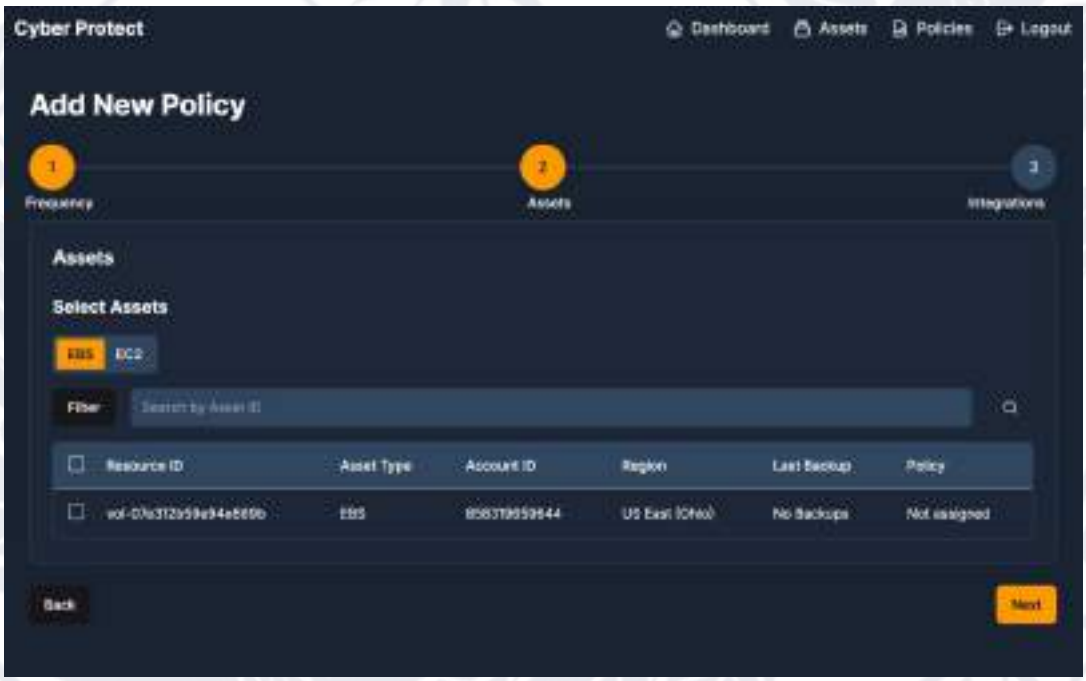

Рис. 4.6. Сторінка Add New Policy (Step 2)

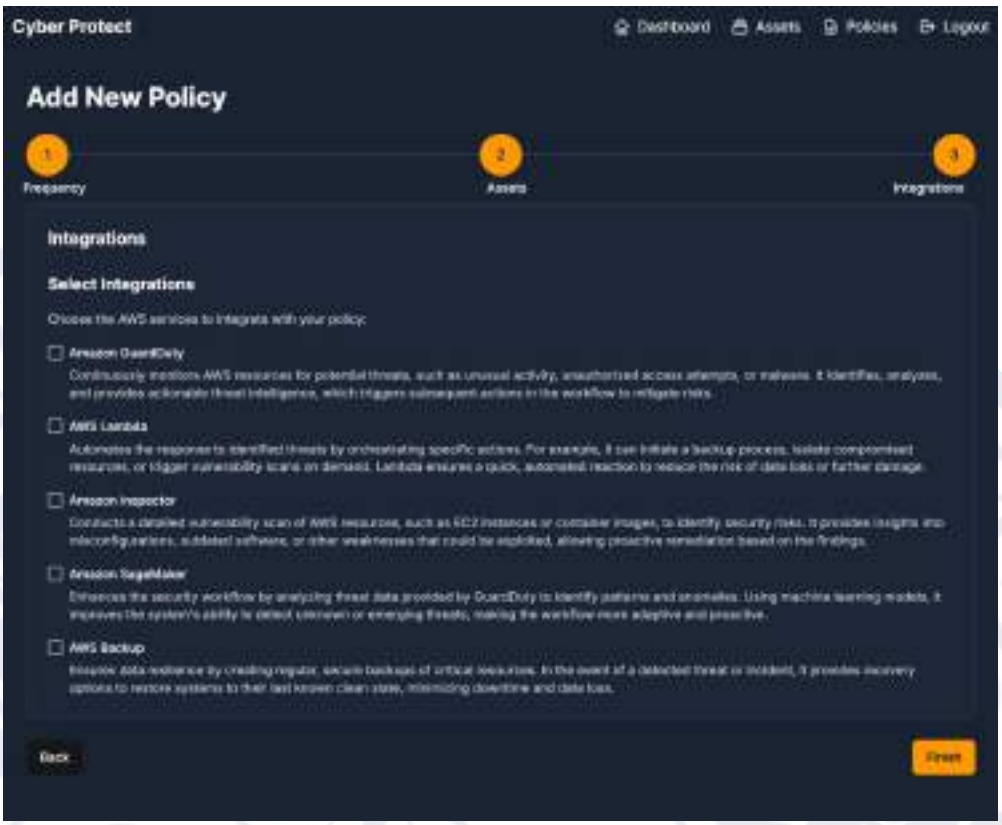

Рис. 4.7. Сторінка Add New Policy (Step 3)

Connected Accounts

Сторінка "Connected Accounts" надає користувачам огляд підключених акаунтів для моніторингу та управління безпекою хмарних ресурсів. У таблиці представлені такі поля: Account ID, що ідентифікує підключений акаунт; Alias Name, який допомагає легко ідентифікувати акаунт за його призначеним іменем; Description — поле для додаткової інформації про акаунт; Regions, що відображає географічне розташування ресурсів, і Assets, яке вказує на кількість активних ресурсів, пов’язаних з акаунтом.

Рис. 4.8. Сторінка Connected Accounts

Висновки до розділу 4

У цьому розділі було проаналізовано ключові аспекти створення веб-додатку для управління безпекою хмарного середовища AWS. Розроблений підхід зосереджується на автоматизації процесів резервного копіювання, виявлення загроз і відновлення ресурсів, що дозволяє значно мінімізувати ризики ураження шкідливими програмами. Основна увага приділялась створенню інтуїтивного інтерфейсу, який спрощує взаємодію користувачів з даними, забезпечує зручне керування політиками безпеки та надає візуалізовані аналітичні дані.

Детально розглянуто структуру додатку, включно з такими сторінками, як Dashboard, Assets, Policies, Connected Accounts, та механізм створення нових політик. У процесі розробки враховано можливість масштабування системи, інтеграції з ключовими сервісами AWS, зокрема Amazon GuardDuty, AWS Lambda, Amazon Inspector, Amazon SageMaker та AWS Backup. Це дозволяє забезпечувати постійний моніторинг активів, оперативно реагувати на загрози та оптимізувати використання ресурсів. Веб-додаток також підтримує розширений функціонал для автоматизації створення резервних копій та управління політиками на основі потреб користувачів.

Тестування інтерфейсу і функціоналу підтвердило відповідність ключовим вимогам кібербезпеки та користувацьким очікуванням. Особливо виділяється ефективність інтеграцій з AWS-сервісами для покращення захисту ресурсів. Водночас, було визначено можливості для подальшого вдосконалення, зокрема, покращення аналітичної частини для візуалізації трендів безпеки та забезпечення більш гнучкої інтеграції з іншими хмарними платформами.

Загалом, запропоноване рішення демонструє високий рівень надійності, адаптивності та зручності використання. Подальші дослідження мають бути спрямовані на інтеграцію нових функцій для підвищення захисту від новітніх кіберзагроз і адаптацію до змін у кіберсередовищі.

ВИСНОВКИ

У ході роботи розроблено концепцію веб-додатку для забезпечення кібербезпеки хмарного середовища Amazon Web Services (AWS). Додаток орієнтований на автоматизацію процесів моніторингу, реагування на загрози, резервного копіювання та управління політиками безпеки. Використання інтеграцій із сервісами AWS, такими як GuardDuty, Lambda, Inspector, Backup та машинного навчання, дозволяє забезпечити проактивний захист активів та мінімізувати ризики ураження шкідливими програмами.

Одним із ключових аспектів розробки є автоматизація, яка забезпечує швидку реакцію на загрози, що зменшує час простою та ризики втрат даних. AWS Lambda виступає центральним компонентом для організації автоматизованих відповідей на інциденти, таких як ізоляція уражених ресурсів чи ініціалізація відновлення з резервних копій. Використання машинного навчання через Amazon SageMaker дозволяє виявляти загрози, які можуть залишитися поза увагою традиційних систем безпеки, аналізуючи аномальну активність та адаптуючи моделі до нових типів атак.

Особливу увагу приділено резервному копіюванню як фундаментальному компоненту забезпечення надійності даних. Завдяки AWS Backup, розроблений веб-додаток підтримує автоматизацію створення резервних копій та забезпечує швидке відновлення ресурсів у разі загроз. Це суттєво підвищує стабільність бізнес-процесів, забезпечуючи доступність критичних даних навіть у разі серйозних інцидентів.

Тестування підтвердило відповідність веб-додатку основним вимогам кібербезпеки та його ефективність у реальному сценарії використання. Особливо виділяється можливість інтеграції з іншими хмарними платформами для розширення функціоналу та забезпечення гнучкості. Водночас виявлено, що майбутні дослідження та вдосконалення повинні бути зосереджені на:

- Покращенні алгоритмів машинного навчання для точнішого виявлення складних загроз, таких як поліморфне шкідливе програмне забезпечення.
- Поглибленні інтеграції із бізнес-процесами для гармонійної роботи автоматизованих систем та ручного аналізу загроз.
- Регулярному оновленні системи відповідно до еволюції кіберзагроз, зокрема навчанні моделей на основі нових даних про інциденти.

Результати цієї роботи демонструють, що комплексний підхід до захисту хмарних середовищ, який включає автоматизацію, аналітику та резервне копіювання, є ефективним бар'єром проти сучасних загроз. Створений веб-додаток забезпечує гнучкість, адаптивність та масштабованість, що є необхідними умовами для захисту в умовах постійно змінюваного кіберландшафту. Подальший розвиток цієї концепції дозволить створити більш універсальні рішення, здатні відповідати новим викликам кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грабовий В.А., Штовба С.Д. Зменшення ризиків ураження шкідливими програмами в хмарному середовищі AWS. Матеріали третьої міжнародної науково-практичної конференції «Прикладні аспекти сучасних міждисциплінарних досліджень», Вінниця: ДонНУ імені Василя Стуса, 2024.

2. Захист від DDoS на глобальному рівні – реальні кейси та висновки. Доповідь на конференції Highload fwdays'24. YouTube. URL: https://www.youtube.com/watch?v=F34ElT1TZM8 (дата звернення 19.11.2024)

3. Мазур В. М. Оцінка безпеки використання хмарних технологій та розробка методів захисту від кібератак на хмарні сервіси. ТНТУ, 2023. – 58 с. URL: http://elartu.tntu.edu.ua/handle/lib/41631 (дата звернення 26.09.2024)

4. Пономаренко, В. Ю. (2024). Дослідження методів забезпечення мережної безпеки в хмарній інфраструктурі. URL: https://openarchive.nure.ua/entities/publication/cdb3349f-8ac4-40e7-ac3d-04745f164ab2 (дата звернення 26.09.2024)

5. Щерба, М. О. (2023). Дослідження методів забезпечення інформаційної безпеки у хмарному середовищі. URL: https://openarchive.nure.ua/entities/publication/a3625c7e-2444-4b7f-8cdd-43dfc213b350 (дата звернення 26.09.2024)

6. Як моделювання зломів та атак полегшує взаємодію з MITRE ATT&CK. iITD Press centre. URL: https://iitd.com.ua/news/jak-modeljuvannja-zlomiv-ta-atak-polegshuie-vzaiemodiju-z-mitre-att-ck/ (дата звернення 19.11.2024)

7. Borra, P. (2024). Comprehensive survey of amazon web services (AWS): techniques, tools, and best practices for cloud solutions. International Research Journal of Advanced Engineering and Science, 9(3), 24-29.

8. Challa, N., Devineni, S. K., & Karangara, R. (2022). A deep dive into amazon web services: Unlocking the potential. Journal of Artificial Intelligence & Cloud Computing, 1, 2-5.

9. Chopra, S., Nayyar, A., Kaur, S., Singh, G., Sharma, R., & Rastogi, D. AWS Tools and Services to Manage Cloud Security Concerns.

10. CJ Moses. How AWS tracks the cloud's biggest security threats and helps shut them down. AWS Security Blog. URL: https://aws.amazon.com/blogs/security/how-aws-tracks-the-clouds-biggest-security-threats-and-helps-shut-them-down/ (дата звернення 19.11.2024)

11. Cloud computing benefits. 2020. Cloud computing beginner's guide on Microsoft's web page. URL: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ (дата звернення 26.09.2024)

12. DigitalOcean. Comparing AWS, Azure, GCP. URL: https://www.digitalocean.com/resources/articles/comparing-aws-azure-gcp (дата звернення 26.09.2024)

13. ElevateSecurity. The Future of Identity and Access Management: 2023 IAM Trends. URL: https://elevatesecurity.com/the-future-of-identity-and-access-management-2023-iam-trends/ (дата звернення 26.09.2024)

14. European Union Agency for Cybersecurity. (2022). Threat Landscape Report 2022. ENISA. URL: https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape (дата звернення 01.11.2024)

15. Fitzgerald, E. 2018. How to remediate Amazon Inspector Security Findings Automatically. Blogpost on Amazon's website. URL: https://aws.amazon.com/blogs/security/how-to-remediate-amazon-inspector-security-findings-automatically/ (дата звернення 26.09.2024)

16. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 129-171.

17. Johnson, P. (2021). Cybersecurity in Cloud Platforms: Next-Generation Protection Strategies, Wiley, p. 135-158

18. Jones, A. & Walker, K. (2020). Advanced Malware Detection and Response in Cloud Environments, Springer, p. 87-89

19. Kewate, N., Raut, A., Dubekar, M., Raut, Y., & Patil, A. (2022). A review on AWS-cloud computing technology. International Journal for Research in Applied Science and Engineering Technology, 10(1), 258-263.

20. MarketsandMarkets Inc. Malware Analysis Market by Component - Global Forecast to 2024. URL: https://www.marketsandmarkets.com/PressReleases/malware-analysis.asp (дата звернення 26.09.2024)

21. Mishra, S., Kumar, M., Singh, N., & Dwivedi, S. (2022). A survey on AWS cloud computing security challenges & solutions. In 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 614-617). https://ieeexplore.ieee.org/abstract/document/9788254 (дата звернення 26.09.2024)

22. Narula, S., & Jain, A. (2015). Cloud computing security: Amazon web service. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp. 501-505). URL: https://ieeexplore.ieee.org/abstract/document/7079135 (дата звернення 26.09.2024)

23. NETSCOUT. Threat Intelligence Report Shows a Dramatic Increase in Multivector DDoS Attacks in First-Half 2020. URL: https://www.netscout.com/netscouts-threat-intelligence-report-1H2020 (дата звернення 26.09.2024)

24. Park, S. J., Lee, Y. J., & Park, W. H. (2022). Configuration method Of AWS security architecture that is applicable to the cloud lifecycle for sustainable social network. Security and Communication Networks, 2022(1), 3686423.URL: https://onlinelibrary.wiley.com/doi/full/10.1155/2022/3686423 (дата звернення 26.09.2024)

25. Rath, A., Spasic, B., Boucart, N., & Thiran, P. (2019). Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and Azure. Computers, 8(2), 34. URL: https://www.mdpi.com/2073-431X/8/2/34 (дата звернення 26.09.2024)

26. Routavaara, I. (2020). Security monitoring in AWS public cloud. URL: https://www.theseus.fi/bitstream/handle/10024/341640/Opinnaytetyo_Routavaara_Ilkka.pdf?sequence=2 (дата звернення 26.09.2024)

27. Sailakshmi, V. (2021). Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud. URL: https://repository.stcloudstate.edu/msia_etds/112/ (дата звернення 26.09.2024)

28. Sally A. The State of Ransomware 2021. URL: https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/ (дата звернення 26.09.2024)

29. SaltLabs. State of API Security Q1 2023. URL: https://content.salt.security/rs/352-UXR-417/images/SaltSecurity-Report-State_of_API_Security.pdf (дата звернення 26.09.2024)

30. Security Hub Standards. Amazon documentation. URL: https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards.html (дата звернення 26.09.2024)

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

32. Simplilearn. AWS full course 2022. Simplilearn. YouTube. URL: https://www.youtube.com/watch?v=ZB5ONbD_SMY. (дата звернення 26.09.2024)

33. Smith, J. & Roberts, T. (2021). Cloud Security: Modern Threats and Solutions, O'Reilly Media, p. 110-124

34. Weiss, B. 2019. AWS re:Inforce 2019: The fundamentals of AWS Cloud Security. AWS Conference talk. URL: https://www.youtube.com/watch?v=-ObImxw1PmI (дата звернення 26.09.2024)

35. What is Amazon Detective? AWS. URL: https://docs.aws.amazon.com/detective/latest/userguide/what-is-detective.html (дата звернення 19.11.2024)

36. X-Force. 2021 IBM Security X-Force Cloud Threat Landscape Report. URL: https://clusis.ch/wp-content/uploads/2021/09/2021-IBM-Security-X-Force-Cloud-Threat-Landscape-Report.pdf (дата звернення 26.09.2024)

ДОДАТКИ

ДОДАТОК А

Автоматичне резервне копіювання з AWS Lambda

```
import boto3
import datetime

def lambda_handler(event, context):
    s3 = boto3.client('s3')

    # Вказуємо ім'я бакету S3
    source_bucket = 'source-bucket-name'
    destination_bucket = 'backup-bucket-name'

    # Створюємо ім'я резервної копії з таймстемпом
    timestamp = datetime.datetime.now().strftime('%Y-%m-
%d-%H-%M-%S')

     copy_source = {'Bucket': source_bucket, 'Key':
'important-file.txt'}
      destination_key = f'backups/important-file-
{timestamp}.txt'

    # Виконуємо копіювання файлу з оригінального бакету
до резервного
         s3.copy(copy_source, destination_bucket,
destination_key)

    return {
        'statusCode': 200,
        'body': f'Backup successful: {destination_key}'
    }
```

ДОДАТОК Б

Скрипт для автоматизації резервного копіювання EC2 за допомогою Python

```
import boto3
from datetime import datetime

# Ініціалізація клієнта EC2
ec2 = boto3.client('ec2')

def create_snapshot(instance_id):
    """
    Функція створює знімок (snapshot) диска EC2.
    """
    try:
        volumes = ec2.describe_volumes(
            Filters=[{'Name': 'attachment.instance-id',
'Values': [instance_id]}]
        )['Volumes']

        for volume in volumes:
            volume_id = volume['VolumeId']
            description = f"Backup for {volume_id} on
{datetime.now().strftime('%Y-%m-%d %H:%M:%S')}"

            snapshot = ec2.create_snapshot(
                VolumeId=volume_id,
                Description=description
            )
            print(f"Created snapshot:
{snapshot['SnapshotId']} for volume {volume_id}")

    except Exception as e:
        print(f"Error creating snapshot: {str(e)}")


instance_id = "i-1234567890abcdef0"
create_snapshot(instance_id)
```