Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікаціїї*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

Дослідження шляхів підвищення ефективності навчання цифровій безпеці в AWS
(тема)

Виконала:
студент 2 курсу, групи *ІМІм-20-2*
Абіх І. В.

Спеціальності *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц. Костромицький А.І.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2022 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Абіх І.В.*
(підпис) (прізвище та ініціали)

Керівник _____ *Костромицький А.І.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)

Факультет інфокомунікацій
Кафедра *Інформаційно–мережної інженерії*
Освітній рівень *другий (магістерський)*
Спеціальність *172 "Телекомунікації та радіотехніка"*
(код і повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри ІМІ_____
(підпис)
“____” _____2022 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Абіх Ірині Вікторівні
(прізвище, ім’я, по батькові)

1. Тема роботи *Дослідження шляхів підвищення ефективності навчання цифровій безпеці в AWS*
керівник роботи *Костромицький Андрій Іванович, доц.*
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ВНЗ від « *14* » *березня* 2022 року № *592Ст*
2. Строк подання студентом роботи *20 травня 2022 р.*
3. Вихідні дані до роботи *Провести аналіз існуючих можливостей та платформ для навчання створення безпечної інфраструктури у хмара. Створити власну платформу на основі найкращіх підходів та рекомендоцій, щодо аспектів безпеки у хмарах платформи для навчання та проходження перевірки знань інжинерів.*
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Основні поняття та характеристика технологій хмарних обчислень
2. Безпека данних та інфраструктури в хмарі
3. Аналіз відомих хмарних провайдерів та їх навчальних програм
4. Розробка навчальної платформи
Висновки

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

Слайди у форматі Power Point (назва, мета і актуальність кваліфікаційної роботи, основні поняття та характеристика технологій хмарних обчислень, безпека даних та інфраструктури у хмарі, відомі хмарні провайдери та їх навчальні програми, розробка навчальної платформи та результати.)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*14.03.22*	*виконано*
2	*Підбір літератури за темою роботи.*	*17.03 – 25.03.22*	*виконано*
3	*Виконання розділу 1*	*18.03 – 24.03.22*	*виконано*
4	*Виконання розділу 2*	*24.03 – 02.04.22*	*виконано*
5	*Виконання розділу 3*	*02.04 – 10.04.22*	*виконано*
6	*Виконання розділу 4*	*11.04 – 17.05.22*	*виконано*
7	*Оформлення пояснювальної записки*	*18.05 – 20.05.22*	*виконано*
8	*Оформлення презентаційного матеріалу, підготовка до захисту у ЕК*	*20.05 – 22.05.22*	*виконано*

Дата видачі завдання *14.03.2022 р.*

Студент _____ *Абіх І.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Костромицький А.І.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 17 рис., 1 табл., 18 джерел, 2 додатка

Мета кваліфікаційної роботи - аналіз існуючих можливостей та платформ навчання створенню безпечної інфраструктури у хмарах, побудова на основі найкращих підходів та рекомендацій щодо аспектів безпеки у хмарах платформи для навчання та проходження перевірки знань студентів, cloud, security та devops.

Об'єкт дослідження – безпека інфраструктури в хмарі AWS.

У ході виконання роботи були виявлені основні переваги та недоліки використання хмар, описано загальні принципи хмарних технологій та сервісів, аналіз чинників розвитку хмарних технологій, побудова на основі найкращих підходів та рекомендацій аспекту безпеки інфраструктури і даних в хмарі, а також визначено напрями реалізації цих питань. Проведений аналіз існуючих можливостей та платформ для навчання створенню безпечної інфраструктури у хмарах.

Результатом роботи є створення своєї автоматизованої платформи для навчання та проходження перевірки перевірки знань студентів, security та devops інженерів.

ХМАРНІ ТЕХНОЛОГІЇ, ІНФРАСТРУКТУРА ЯК СЕРВІС, ХМАРНІ ПРОВАЙДЕРИ, СИСТЕМА КОНФІГУРАЦІЇ, БЕЗПЕКА ДАНИХ, БЕЗПЕКА В ХМАРІ

THE ABSTRACT

Explanatory note: 73p., 17 fig., 3 tabl., 18 sources, 2 app.

The purpose of the qualification work is to analyze existing opportunities and training platforms for creating a secure infrastructure in the cloud, to build on the best approaches and recommendations on the aspects of security in the clouds platform for training and passing the knowledge test of students, cloud, security and devops.

The object of the study is infrastructure security in the AWS cloud.

In the course of the work were identified the main advantages and disadvantages of using clouds, described the general principles of cloud technologies and services, analysis of cloud technology development factors, building on the best approaches and recommendations of the security aspect of infrastructure and data in the cloud, as well as directions for the implementation of these issues. Analysis of existing opportunities and platforms for learning how to create a secure infrastructure in the clouds.

The result of the work is the creation of its automated platform for training and testing the knowledge of students, security and devops engineers.

CLOUD TECHNOLOGY, INFRASTRUCTURE AS A SERVICE, CLOUD PROVIDERS, CONFIGURATION SYSTEM, DATA SECURITY, SECURITY IN THE CLOUD

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

API – Application Programming Interface (інтерфейс програмування додатків);
APN – AWS Partner Network (партнерська програма AWS);
AWS – Amazon Web Services (вебсервіси Amazon);
CaaS – Communication as a Service (комунікація як послуга);
DLP – Data Leak Prevention (запобігання витоку даних);
EBS – Elastic Block Storage (еластичне блочне сховище);
EFS – Elastic File System (еластична файлова система);
GCP – Google cloud platform (хмарна платформа Google);
GPU – Graphics Processing Unit (блок обробки графіки);
HaaS – Hardware as a Service (апаратне забезпечення як послуга) ;
HPC – High Performance Computing (високопродуктивні обчислення);
IaaS – Infrastructure as a Service (інфраструктура як послуга);
IAM – Identity and Access Management (ідентифікація та управління доступом);
IBM – International Business Machines (міжнародні бізнес-машини);
IOPS – input/output operations per second (операції вводу / виводу в секунду);
IoT – Internet of Things (інтернет речей);
KMS – Key Management Service (служба управління ключами);
NAT – Network Address Translation (переклад мережевих адрес);
PaaS – Platform as a Service (платформа як послуга);
SaaS – Software as a Service (програмне забезпечення як послуга);
SAP – System Analysis and Program Development;
IT – Information Technologies (інформаційні технології);
SDK – Software Development Kit (комплект програмного забезпечення);
SLA – Service Level Agreement (угода про рівень обслуговування);
SMS – Short Message Service (служба коротких повідомлень);
SNS – Simple Notification Service (проста служба оповіщення);
SQS – Simple Queue Service (просте обслуговування черги);
VLAN – Virtual Local Area Network (віртуальна локальна мережа);
VPC – Virtual Private Cloud (віртуальна приватна хмара);
VPN – Virtual Private Network (віртуальна приватна мережа);;
WAF – Web Application Firewall (брандмауер веб-додатків);
ОС – операційна система;
ПЗ – програмне забезпечення.

ВСТУП

Сучасна людина та інноваційні технології нерозривно пов’язані з поняттям хмарних обчислень.

Хмарні технології знаходять широке застосування у сучасному світі, забезпечуючи нові, економічно ефективні можливості для бізнесу, науки, медицини та освіти.

Хмарний тренд розвитку технологій вже став одним з найважливіших складових бізнесу, перспективного розвитку сучасних компанії, так і необхідною рутиною сьогодення.

Хмарні сервіси є комбінацією існуючих технологічних рішень, які взаємно інтегровані для забезпечення максимальної автоматизації і мінімізації участі людини в їх роботі [1].

Суть концепції хмарних обчислень полягає в наданні користувачеві зручного, безпечного віртуального середовища для зберігання, обробки інформації та обчислень через Інтернет. Хмари поєднують в собі апаратні засоби, програмне забезпечення, канали зв'язку, а також службу технічної підтримки.

Хмарні провайдери пропонують постійний доступ до великого асортименту обчислювальних потужностей та сервісів з максимальною надійністю та безпечністю роботи, вони швидко масштабуються, мають можливості легкої міграції даних, а також системи моніторингу. Які здійснюють контроль масштабів використання ресурсів, виявляють застаріле ПЗ та уразливі елементи вашої інфраструктури.

Хмарні провайдери гарантують захист критично важливої інформації від крадіжки, витоку і втрати за умови коректних налаштувань вашої інфраструктури. Тому для того, щоб створити безпечну хмарну інфраструктуру і зберегти дані, потрібно проходити навчальні курси та тренінги підвищення кваліфікації.

Використання хмарних технологій є актуальним питанням для всіх галузей, а відповідно і навчання створенню безпечної інфраструктури в хмарі набуває особливого значення.

Мета кваліфікаційної роботи - аналіз існуючих можливостей та платформ навчання створенню безпечної інфраструктури у хмарах, побудова на основі найкращих підходів та рекомендацій щодо аспектів безпеки у хмарах платформи для навчання та проходження перевірки знань студентів, cloud,

security та devops інженерів. У даній роботі буде проведено аналіз та описано загальні принципи хмарних технологій та сервісів, хмарних обчислень, аналіз чинників розвитку хмарних технологій, безпеки інфраструктури і даних в хмарі, а також визначено напрями реалізації цих питань. Буде проведений аналіз існуючих можливостей та платформ для навчання створенню безпечної інфраструктури у хмарах, та визначено всі недоліки і переваги. Результатом цього дослідження буде створення своєї платформи для навчання та проходження перевірки знань студентів.

1 ОСНОВНІ ПОНЯТТЯ ТА ХАРАКТЕРИСТИКА ТЕХНОЛОГІЙ ХМАРНИХ ОБЧИСЛЕНЬ

Хмарні обчислення (Cloud computing) - технологія обробки даних, в якій обчислювальні потужності надаються користувачеві як сервіс. Ці ресурси включають інструменти та програми, такі як сховище даних, сервера, бази даних, мережі та програмне забезпечення. Це модель надання постійного та зручного доступу за вимогою через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та відмінені з мінімальними втручанням [4].

Хмара - це середовище для зберігання та обробки даних, яке об'єднує в собі апаратні засоби, програмне забезпечення, мережу і засоби підтримки користувачів [2].

1.1 Розвиток хмарних обчислень

Хмарні обчислення, як термін, існують з початку 2000-х років, але концепція обчислень як послуги існує набагато довше — ще в 1960-х роках, коли комп'ютерні бюро дозволяли компаніям орендувати час на мейнфреймах. У той час з'явилися ідеї, що нагадують хмарні обчисленнями - наприклад, концепція «міжгалактичної комп'ютерної мережі» Дж. К. Р. Ліклайдера [3].

У 1970-ті роки віртуалізація підняла мейнфрейми на новий рівень, а в 1990-х телекомунікаційні компанії почали пропонувати підключення до віртуальної приватної мережі (VPN)[3].

Протягом 1970-х років були розроблені різні віртуальні машини, подібні до тих, які були створені комп'ютерними гігантами, такими як IBM.

25 вересня 2006 року, Amazon Web Services (AWS), поклав початок руху хмарних обчислень. AWS надає широкий набір сервісів, таких як обчислювальні потужності і сховища даних, до цього дня залишаючись провідною і дуже надійною інфраструктурою платформ хмарних веб-сервісів. Незабаром до Amazon приєдналися Google, Apple, Nexflix, Microsoft, і IBM.

У 2010 році такі компанії, як AWS, Microsoft та OpenStack, розробили досить функціональні приватні хмари. OpenStack також зробив відкриту, безкоштовну, саморобну хмару, яка стала дуже популярною і доступною для широкої публіки. Apple запустила iCloud, який фокусується на зберіганні більшої кількості особистої інформації (відео, фотографії, музика, тощо).

Oracle представила свою хмару у 2012 р., пропонуючи три базові моделі для бізнесу: IaaS (інфраструктура як послуга), PaaS (платформа як послуга) та SAAS (програмне забезпечення як послуга).

Усі зверталися до хмари - від розваг, охорони здоров'я, фінансів до уряду, бажання приєднатися до цього нового сектора, відбувалося пришвидшеними темпами. Хмара створювала культурне зрушення, небачене раніше в історії людства. Невеликі стартапи змінювали світ. Багатство створювалося у віддалених місцях, а творчість та інновації стали прерогативою людини.

На цей час більшість провідних IT-вендорів на світовому ринку, включаючи Google, Microsoft, HP, Intel, SAP, IBM, Oracle та інші мають в своїй лінійці рішення cloud computing [1].

Провайдери змагаються в створенні найбільш ефективних програм організації віртуальної інфраструктури. Витрати на хмарні обчислення ростуть швидше, ніж очікувалось. Приблизний прогноз витрат на хмарні обчислення в майбутньому зображений на рис. 1.1.

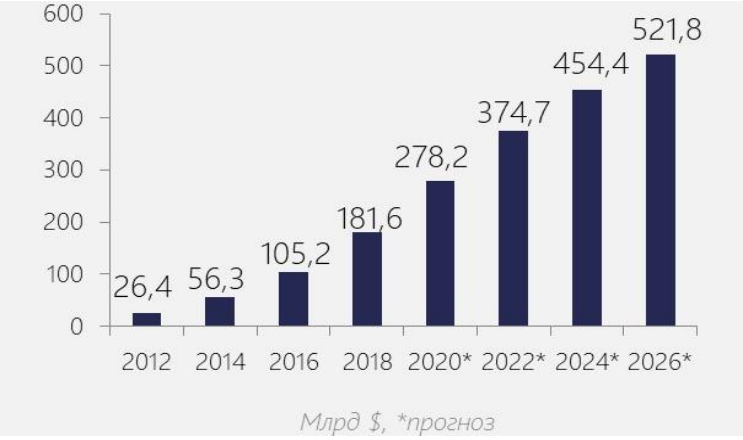

Рисунок 1.1 - Прогноз витрат на хмарні обчислення

1.2 Властивості хмар та основні моделі

Національний Інститут стандартів та технологій NIST визначає наступні характеристики хмар: можливість самообслуговування без участі людини з боку провайдера, наявність широкосмугового доступу до мережі, зосередженість ресурсів на окремих майданчиках для їх ефективного розподілу, швидка масштабованість, ресурси можуть необмежено виділятися і вивільнятися з великою швидкістю в залежності від потреб користувача,

керований сервіс, система управління хмарою автоматично контролює і оптимізує виділення ресурсів, ґрунтуючись на вимірюваних параметрах сервісу [1]. Основні моделі хмарних сервісів зображені на рис. 1.2.

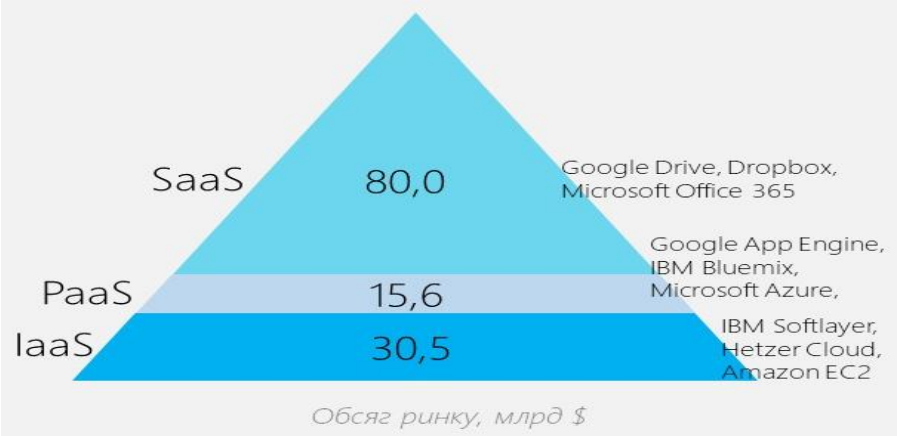

Рисунок 1.2 – Основні моделі хмарних сервісів

Основні моделі надання хмарних послуг:

- програмне забезпечення як послуга (SaaS) – надання у використання додатків провайдера, які працюють в хмарній інфраструктурі. Користувач не керує базовою інфраструктурою хмари, тобто мережами, серверами, операційними системами, системами зберігання і навіть індивідуальними настройками додатків за винятком деяких налаштувань конфігурації програми. Прикладами такої моделі є сервіси Gmail та Google docs та інші [1];
- платформа як послуга (PaaS) – надання споживачеві для розгортання в хмарній інфраструктурі додатків, реалізованих та підтримуваних провайдером послуг. Користувач також не керує базовою інфраструктурою хмари, як і в першому випадку, але має контроль над розгорнутими додатками і деякими параметрами конфігурації середовища хмари. Так, наприклад, Google Apps доступ до додатків відбувається за допомогою браузера чи додатку, тоді як дані зберігаються на серверах Google [1];
- інфраструктура як послуга (IaaS) – надання споживачеві систем обробки, зберігання, мереж та інших фундаментальних обчислювальних ресурсів для розгортання і виконання довільного програмного забезпечення, яке може включати в себе операційні системи і додатки. Користувач теж не керує базовою інфраструктурою хмари, але має контроль над операційними системами, системами зберігання, розгорнутими додатками і деякий контроль вибору мережевих компонентів. Найбільшими постачальниками IaaS є Amazon Web Services, Google Cloud Platform, Microsoft Azure [1].

Також існують такі види менш популярних моделей, як: HaaS (Hardware as a service) – модель надання послуг апаратного забезпечення, WaaS (робоче місце як хмарний продукт). Дає можливість організації віддалених робочих місць співробітників компанії в мережі за допомогою встановленого ПЗ на хмарних платформах, CaaS (Communication as a service) – надання послуг зв'язку як сервісу. Під послугами зв'язку, зазвичай мають на увазі IP-телефонію, пошту або миттєві комунікації, такі як чати або служби обміну миттєвими повідомленнями [5].

Найпопулярнішими хмарними сервісами є SaaS – найприбутковіший за даними останніх досліджень. Друге місце посів сегмент IaaS, на останньому місці – PaaS [1]. Тенденція популярності хмарних сервісів зображено на рисунку 1.3.

Рисунок 1.3 – Тенденція популярності хмарних сервісів

Моделі розгортання хмарного середовища:

- приватна хмара (Private cloud) – це хмарна інфраструктура, підготовлена для ексклюзивного використання однією організацією. Така хмара може перебувати у власності, управлінні і обслуговуванні у самій організації і розташовуватися як на території підприємства, так і за його межами [1];
- хмара спільноти (Community cloud) – це хмарна інфраструктура, створена для ексклюзивного використання декількома організаціями;
- публічна хмара (Public cloud) – це хмарна інфраструктура, створена для відкритого використання широкою публікою, працює на території хмарного провайдера;
- гібридна хмара (Hybrid cloud) – це хмарна інфраструктура, сукупність з двох або більше різних інфраструктур хмар (приватні, громадські або

державні), що мають унікальні об'єкти, але пов'язані між собою стандартизованими або власними технологіями, які дозволяють переносити дані або програми між компонентами [1].

1.3 Переваги та недоліки хмарних технологій

Основні переваги хмарних технологій:

- відмовостійкість;
- підвищена безпека та надійність;
- висока швидкість обробки даних;
- ефективне використання ресурсів;
- регулярне оновлення програмного забезпечення;
- зниження витрат на апаратне і програмне забезпечення, на обслуговування і електроенергію;
- миттєве масштабування на вимогу замовника, в залежності від зміни навантажень;
- непомітна для користувачів міграція на нові версії і нові платформи, замовники завжди працюють з найостаннішими версіями додатків;
- потрібні сервіси доступні практично миттєво – не потрібно ніяких додаткових робіт по розгортанню і конфігурації використовуваних інформаційних систем.

Недоліки хмарних обчислень:

- залежність збереження даних користувача від сторонніх компаній провайдерів;
- не завжди маленьким проектам та стартапам економічно доцільно використовувати хмари;
- пряма заборона чи обмеження, що регулюють державні органи, доступу через Інтернет до критичних даних фінансових організацій, структур забезпечення держбезпеки тощо.

1.4 Майбутнє хмарних технологій

Для створення навчальної платформи потрібно оцінити її доцільність та визначити напрямки програми з урахуванням майбутньої необхідності. Поширення хмарних технологій зростає. За даними Gartner, глобальні витрати на загальнодоступні хмарні послуги у 2021 році становили 332,3 мільярда доларів порівняно з 270 мільярдами доларів у 2020 році [14].

Очікується, що 80% підприємств перейдуть у хмару, а 84% використовують мультихмарний підхід [14]. Оскільки дедалі більше компаній переходять на віддалені об'єкти, хмарний світ відроджується, формуючи майбутні тенденції у сфері хмарних обчислень.

Основні тенденції розвитку хмарних технологій в майбутньому:

– гібридна хмара та мультихмарна інфраструктура – це компроміс між підходами, а саме об'єднання їхніх сильних сторін. Дані, які потребують швидкого та частого доступу, можуть зберігатися на загальнодоступних серверах, а більш конфіденційні дані можуть зберігатися на приватних серверах із контрольованим доступом. Мультихмарна модель допомагає компаніям вибирати різні хмарні пропозиції, що найбільш підходять для їх індивідуальних середовищ додатків, бізнес-вимог та потреб у доступності [15]. Очікується, що до 2023 року обсяг ринку гібридних/мультихмарних середовищ з урахуванням численних переваг зросте до 97,64 млрд. доларів [14]; Приклад організації гібридної хмари зображений на рисунку 1.4.

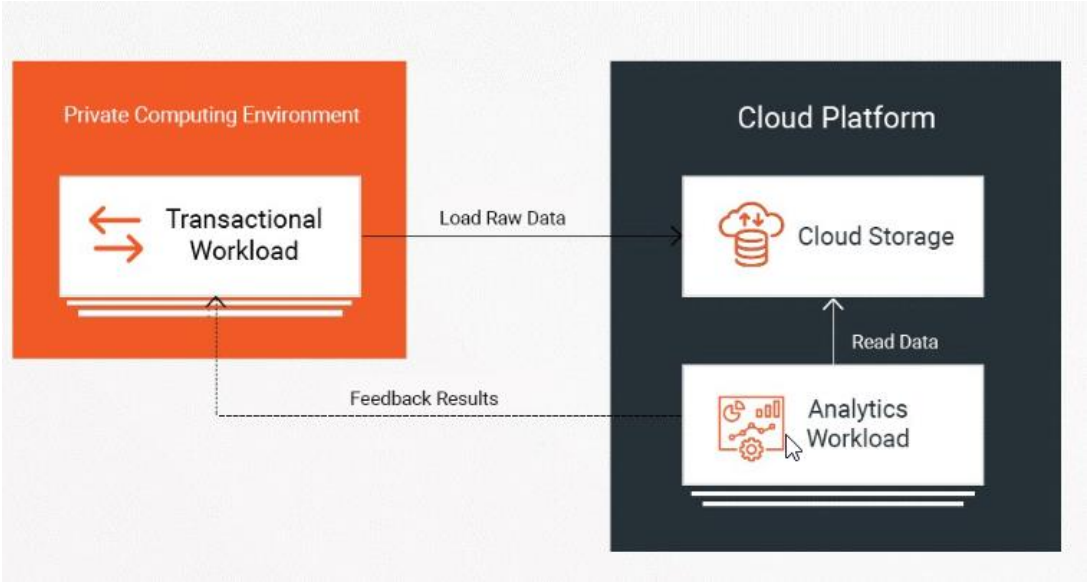

Рисунок 1.4 - Організація гібридної хмари

– IoT (Інтернет речей) – одна з провідних тенденцій хмарних обчислень є зростання платформ IoT, що підтримує хмарні технології. Він збирає дані із конфігурацією віддаленого пристрою. Він також надсилає оповіщення в режимі реального часу для усунення несправностей. IoT підтримує різні протоколи для надання інтелектуальних прогнозів за допомогою моніторингу [15];

– штучний інтелект – одна з найпопулярніших тенденцій хмарних обчислень. До 2025 року глобальна ринкова вартість, за оцінками, перевищить 89 мільярдів доларів на рік;

– безсерверні обчислення – увійшли до п'ятірки найшвидших платформ як послуг (PaaS). Очікується, що попит на безсерверні обчислення зросте на 25% з 2021 до 2026 року. Безсерверна архітектура дозволяє компаніям розробляти та запускати програми без необхідності керувати фізичними серверами. Приклад безсерверної інфраструктури зображений на рисунку 1.5;

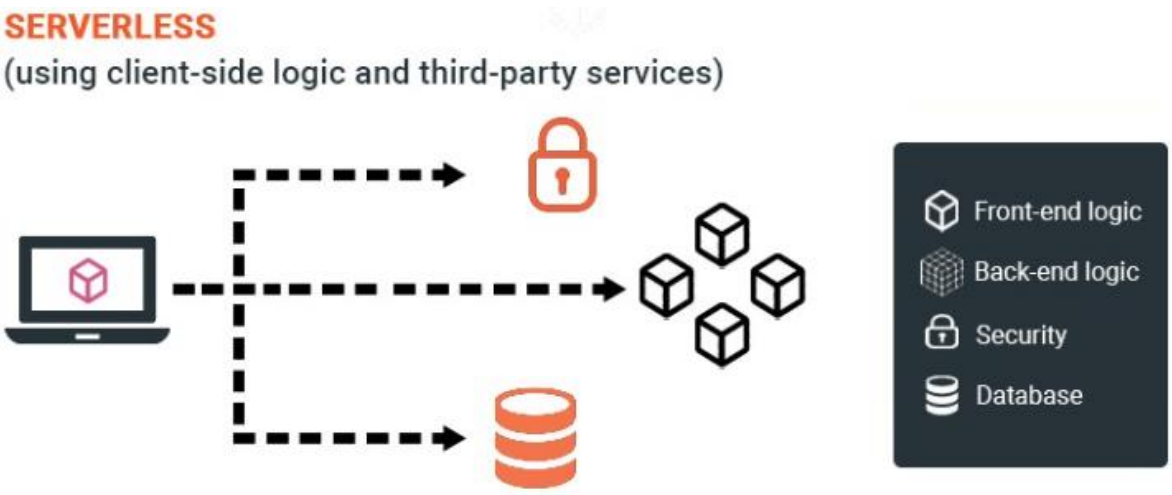

Рисунок 1.5 - Безсерверна архітектура

– резервне копіювання та аварійне відновлення – один з найперспективніших варіантів використання хмари. Якщо вірити звітам Spiceworks, 15% хмарного бюджету виділено на резервне копіювання та аварійне відновлення, що є найвищим розподілом бюджету, за яким слідують хостинг електронної пошти та інструменти підвищення продуктивності;

– контейнери та Kubernetes – тенденція до використання контейнерів продовжуватиме зростати у міру розробки хмарних додатків. Gartner прогнозує, що до 2022 року понад 75% організацій використовуватимуть контейнери. Це дозволяє програмам збільшити швидкість розробки. Kubernetes пропонує атрибути, що створюють стеки сучасної IT-інфраструктури [15];

– підвищення безпеки – ця тенденція має важливе значення у майбутньому хмарних обчислень. Потенційні загрози у хмарних системах усунуті чи будуть усунуті завдяки розвитку в цьому напрямку. Безпека інтегрується з машинним навчанням та штучним інтелектом у хмарі. Це допомагає в автоматизації процесу моніторингу атак та захисту. Безпека даних стане ще розумнішою, автономнішою, надійнішою та відмовостійкою.

Введення DevSecOps – це процес осмислення безпеки інфраструктури із самого початку. Він працює над автоматизацією основних завдань безпеки, впроваджуючи елементи управління та процеси безпеки у свій робочий процес. DevSecOps є однією з основних організаційних змін, які допоможуть підвищити безпеку їх хмарного середовища. До 2022 року не менше 95% збоїв у хмарній безпеці відбувались з вини клієнтів [14].

Тобто для того, щоб підвищити рівень безпеки в хмарі потрібно приділити більше ресурсів на навчання користувачів, для створення безпечної інфраструктури, а отже це відповідає цілям дипломного проекту.

2 БЕЗПЕКА ДАНИХ ТА ІНФРАСТРУКТУРИ В ХМАРІ

Багато компаній, як і раніше, стурбовані безпекою хмарних сервісів, хоча порушення безпеки трапляються зрідка, існує певна кількість міфів, що пояснюються недостатньою поінформованістю клієнтів про хмарні сервіси і наявністю великої кількості не цілком достовірної інформації.

Однак, при правильному підході, хорошому розумінні технології і зваженому виборі постачальника хмарні сервіси здатні забезпечити більшу надійність і захищеність, ніж існуюча в компанії інфраструктура [1].

Професійні провайдери, керуючи публічними хмарами, приділяють більше уваги безпеці, продуктивності і контролю, ніж часто обмежені в можливостях IT-відділи компаній. Тому, користуючись хмарними сервісами надійного провайдера, клієнт, отримує більш високий рівень захисту і стабільність роботи для своїх систем, ніж у своїй локальній [1].

Перелічимо основні причини надійності хмар:

- безпека віртуального середовища клієнта - це одне з основних правил, на яких тримається бізнес хмарного провайдера;
- відповідальність провайдера перед клієнтом регулюється SLA (угодою про рівень послуг та відповідальності);
- хмарний провайдер вкладає значні ресурси в розвиток технологій, систем захисту і збереження даних;
- інфраструктурні рішення хмари обумовлені світовими стандартами безпеки.

2.1 Спільна відповідальність

Для роз'яснення спільної відповідальності постачальників і клієнтів Amazon розділяє концепції "безпека хмари" та "безпека у хмарі". Провайдери зазвичай відповідають за фізичну та мережеву інфраструктуру. Клієнти — за парольну політику, налаштування доступу, та налаштування інфраструктури, які не залежать від сервіс-провайдера.

Спільна відповідальність регулюється угодами та зобов’язаннями. Основним є договір про рівень обслуговування (SLA) між постачальником та замовником послуг. Така угода містить кількісні та якісні характеристики наданих послуг, їх доступність, ступінь підтримки користувачів, час виправлення несправності тощо [4].

Основне розділення обов’язків замовника та провайдера зображено на рисунку 2.1.

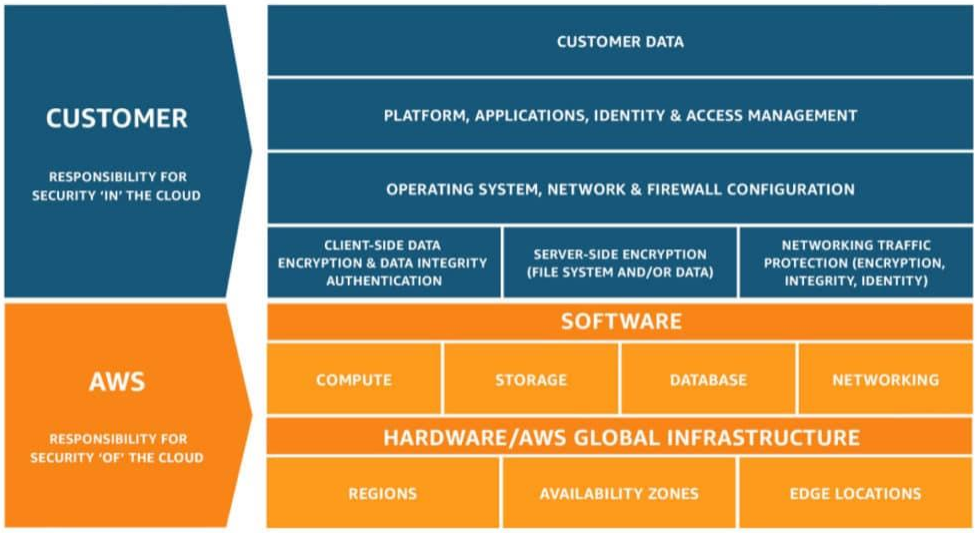

Рисунок 2.1- Відповідальність провайдера та замовника послуг

Провайдер відповідає за безпеку основних компонентів хмари: мережі, накопичувачі, сервери і віртуалізація [1].

Запобігання внутрішніх і зовнішніх загроз всередині хмарної інфраструктури клієнта - це обов'язок клієнта. А саме управління та обслуговування систем контролю доступу, управління політиками і правами доступу користувачів, включаючи парольний захист, стандартне управління оновленнями ОС і додатків, ведення та аналіз реєстраційних журналів, моніторинг активності користувачів.

2.2 Аспекти безпеки даних в хмарі

Безпека в хмарі — це комплекс технологічних рішень, політик та процедур, які реалізовані для захисту хмарних програм та систем, а також пов'язаних даних та доступу користувачів. Основні принципи інформаційної безпеки та управління даними в хмарі – конфіденційність, цілісність та доступність даних [4].

Світовий досвід демонструє, що внутрішні ризики безпеки стали переважати над зовнішніми. Головним джерелом загроз для інфраструктури компанії зараз є зовсім не хакери, а власні співробітники компанії. Згідно з результатами дослідження «CSI Computer Crime and Security Survey», з шкідливими діями персоналу мали справу - 25% респодентів.

Неправильні конфігурації інфраструктури залишаються найпоширенішою проблемою безпеки. Хакери можуть виявити неправильні конфігурації та використовувати їх для атаки, а також можуть отримати доступ до хмар через викрадені облікові дані, шкідливі контейнери та вразливості програмного забезпечення [4].

При розміщенні своєї інфраструктури в хмарі клієнт втрачає контроль над частиною інфраструктури на користь постачальника IaaS. Провайдер виконує обов'язки з управління компонентами інфраструктури, включаючи адміністрування мереж, серверів і систем зберігання даних. При цьому фахівці компанії провайдера, періодично проводять тестування працездатності систем та підтримують клієнтів з інфраструктурних питань. Клієнту при цьому не потрібно налаштовувати обладнання, оновлювати, стежити за ним і лагодити. Ресурси, які потрібні користувачам, вже не обмежуються фізичними можливостями існуючого обладнання, що підвищує ефективність роботи [1].

Ресурси провайдера захищені та ізольовані один від одного, що втручання інших користувачів малоймовірні.

Взаємодія між локальним обладнанням користувача відбувається за допомогою інтернет-каналів, які можуть нести в собі потенційну загрозу безпеці компанії. Зловмисники можуть, наприклад, перехопити веб-сесію або вкрасти паролі для доступу до систем управління. Хмарні провайдери використовують надійні системи аутентифікації і управління політиками прав доступу, а також мають захищені інтернет-канали, що позитивно впливає на рівень безпеки. Окрім парольного захисту хмарні провайдери використовують сертифікати, токени і двоетапну перевірку. До цього ж є функції автоматичного видалення даних аутентифікації користувача, або блокування, якщо він не діє певний час. Також підвищує рівень безпеки поділ користувачів за ролями, згідно з якими кожен отримує лише відповідні йому права на доступ до ресурсів хмари і на окремі дії з ними.

Одна з якостей великих провайдерів – це регіонально рознесені ресурси, рознесення ресурсів в різні підмережі і резервування. Ресурси в яких можливе спільне використання надійно ізольовані [1].

Провайдери володіють стандартизованим процесом виявлення, ідентифікації, аналізу і реагування на інциденти. При значних навантаженнях користувачі можуть відчути падіння продуктивності або недоступність сервісів. Зазвичай, така ситуація обумовлена помилками в налаштуваннях або недостачею ресурсів. З боку великих провайдерів такі ризики мінімізуються.

Найвідоміші провайдери максимально захищені від DoS-атак.

Високий рівень безпеки в хмарному середовищі – це результат продуманої політики інформаційної безпеки. Великі хмарні провайдери налаштовуючи свою інфраструктуру керувалися світовими стандартами, такими як CIS Benchmark, HIPAA, , NIST CSF, PCI DSS, , FedRAMP , ISO 27002, NIST CSF v1.1, FedRAMP та іншими [1].

Як було визначено раніше найуразливішою частиною в роботі з хмарою є користувач, який неправильно може налаштувати власну інфраструктуру, тим самим зробивши її вразливою. AWS так само знайшов способи вирішення даної проблеми, окрім написання документації, створення тренінгів, рекомендацій по налаштуванню того чи іншого ресурсу в системі, розробив сервіси, які сканують налаштовану інфраструктуру, приділяючи особливу увагу віртуальним машинам та контейнерам, уразливості і надають детальний звіт з посиланням на рекомендації від CVE security vulnerability database. Крім цього, є безліч сторонніх систем аналізу вразливостей інфраструктури, такі як Cloud Custodian, Dome9 та інші. Постачальники хмарних послуг також звертаються до штучного інтелекту для захисту даних. Ці програми використовують вбудовані алгоритми для пошуку та виявлення можливих уразливостей у заходах безпеки.

Постачальники хмарних послуг також повинні наймати сторонні компанії з безпеки для регулярного тестування своїх серверів та програмного забезпечення, щоб переконатися, що вони захищені від кіберзлочинців та новітніх шкідливих програм та вірусів. Це зовнішнє тестування підвищує ймовірність того, що ваш хмарний провайдер матиме засоби захисту, необхідні для захисту ваших файлів від хакерів.

Для усунення слабких місць в системі потрібно забезпечувати єдиний рівень безпеки, навіть коли інфраструктура постійно змінюється. Зміни та розширення інфраструктури настають настільки швидкими темпами, важливо, щоб будь-які зміни в мережі здійснювалися в строгій відповідності із загальним планом безпеки. Вимога використовувати належні інструменти, політики і процедури безпеки до того, як будуть задіяні будь-які нові ресурси, дозволяє адаптувати рішення безпеки до змін в інфраструктурі і в додатках [4].

При правильному підході, розумінні технології, зваженому виборі постачальника, постійному навчанні персоналу, хмарні сервіси здатні забезпечити більшу надійність і захищеність, ніж локальна інфраструктура.

3 АНАЛІЗ ВІДОМИХ ХМАРНИХ ПРОВАЙДЕРІВ ТА ЇХ НАВЧАЛЬНИХ ПРОГРАМ

Світовий ринок хмарних технологій зосереджується навколо трьох гігантів: Amazon, Google, та Microsoft, які займають 63% ринку. У США та Європі саме вони є затребуваними у місцевих компаніях. А в Азії ринок практично повністю монополізував Alibaba Cloud. Ринкова частка хмарних провайдерів зображена на рисунку 3.1.

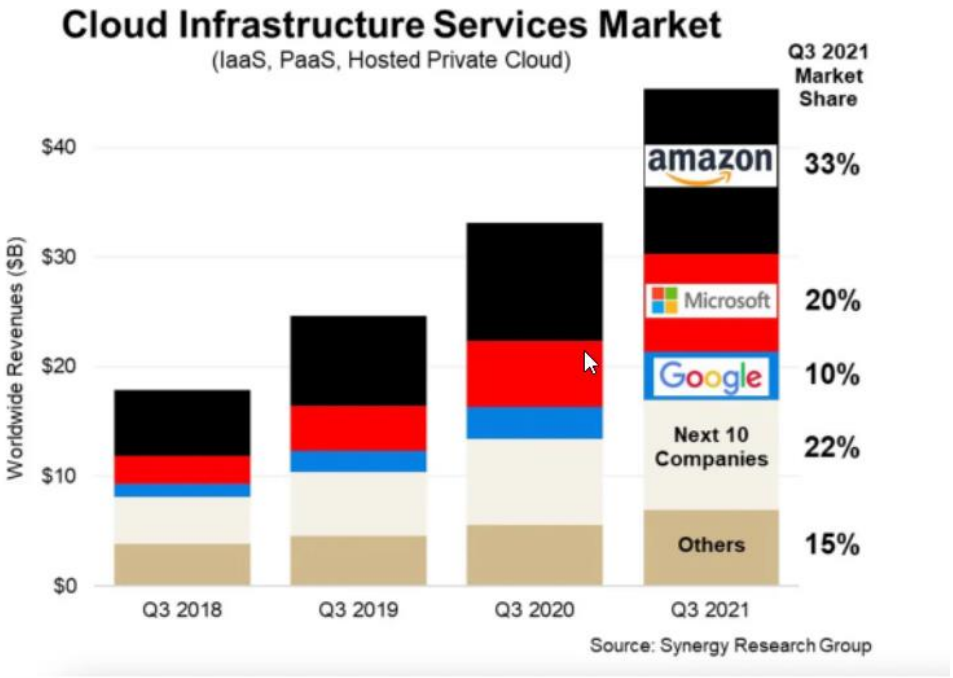

Рисунок 3.1- Ринкова частка хмарних провайдерів

В Україні, крім глобальних хмарних провайдерів, також існують локальні оператори: De Novo, GigaCloud, UCloud, VoliaCloud, Tucha ті інші [1]. Держава вкладає багато ресурсів в розвиток хмарних технологій в Україні, ми бачимо прискорений рух в напрямку цифровізації цивільних послуг. AWS ще наприкінці 2020 р. зареєструвала ТОВ «Амазон Дата Сервісес Україна» [8]. Станом на 2021 рік ринкова частка українських провайдерів становила $6,1 млн – рис. 3.2.

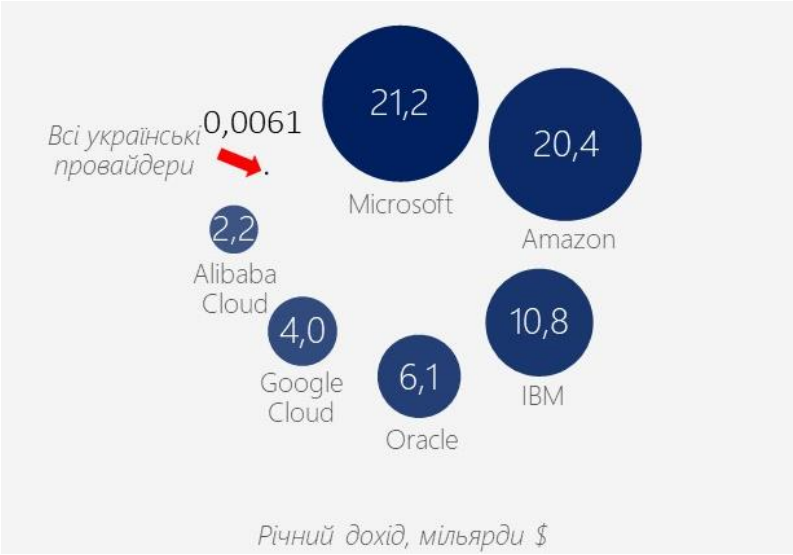

Рисунок 3.2- Річний дохід провайдерів

Аналітична компанія Gartner опублікувала магічний квадрант, AWS відкриває рейтинг найпопулярніших хмарних провайдерів за 2021, вже декілька років перші п’ять учасників незмінні в своїх позиціях. Зображений на рисунку 3.3.

Рисунок 3.3 - Magic Quadrant IaaS

3.1 Вибір хмарного провайдеру для створення власної платформи

Для досягнення мети створення власної навчальної платформи було визначено, що таке хмара, її основні особливості, визначені основні аспекти безпеки в хмарі. Наступний етап - вирішити, в якій хмарі буде розроблена наша платформа. Беручи до уваги результати попередньої атестаційної роботи, в якій я проводила детальний аналіз провайдерів та їх порівняння, мій практичний досвід роботи з провайдером, створювати навчальний додаток буду на основі інфраструктури платформи AWS.

AWS (Amazon Web Services) - це комплексна платформа хмарних обчислень, яка пропонує «інфраструктуру як послугу» (IaaS), «платформу як послугу» (PaaS) і програмне забезпечення як послугу (SaaS) . Широкий спектр програмного забезпечення та послуг, що пропонуються платформою AWS, означає, що Amazon управляє загальнодоступною хмарою безпрецедентного масштабу і щороку з 2010 року визнається світовим лідером галузі згідно магічного квадранту Gartner для хмарної інфраструктури як послуги і яка забезпечує роботу сотень тисяч підприємств більш ніж в 190 країнах по всьому світу [10].

У 2022 році AWS має більше 230 сервісів, сервіси обчислення, зберігання, бази даних, мережі моніторингу, сервіси додатків, розгортання, управління, мобільності, інструменти та сканери для безпеки, інструменти для розробки, робототехніки, зв'язку, сервіс передачі даних з автомобіля та інструменти для Інтернета речей. Сервіси AWS зображені на рис 3.4.

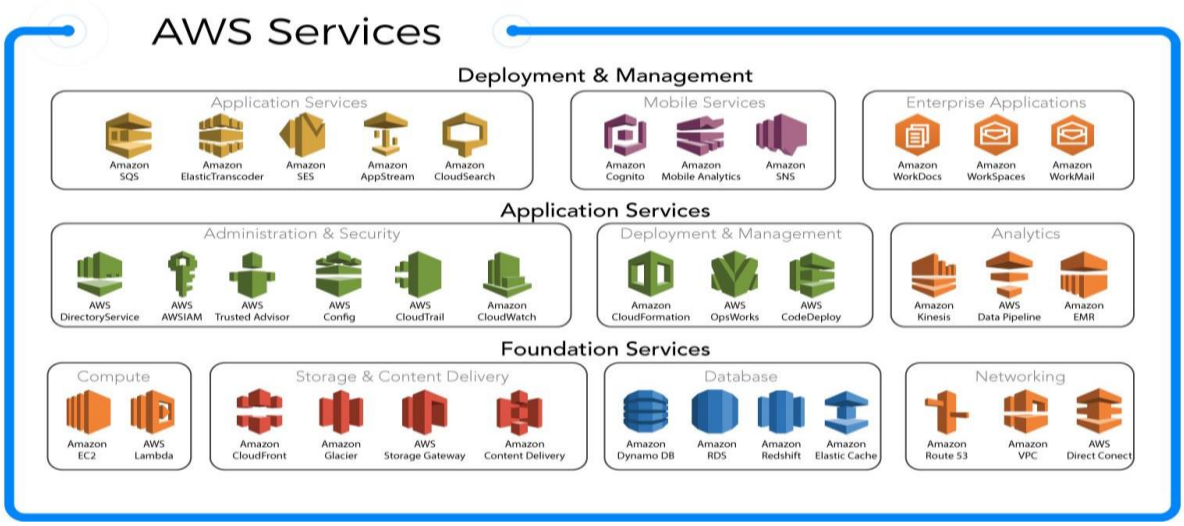

Рисунок 3.4 – Сервіси AWS

Найбільш популярними сервісами є EC2 та Amazon Simple Storage Service, та IAM. AWS запропонував програму сертифікації для комп'ютерних інженерів, одним із перших провайдерів у 2013 році, і зараз AWS створює учбові програми та платформи для студентів вузів та викладачів, та розширює теми курсів і все це безкоштовно.

Хмара AWS охоплює 84 зони доступності у 26 географічних регіонах по всьому світі. Найближчим часом планується створити ще 24 зони доступності та 8 регіонів AWS в Австралії, Канаді, Ізраїлі, Новій Зеландії, Іспанії, Швейцарії та Об'єднаних Арабських Еміратах (OAE) рис. 3.5.

Рисунок 3.5 – Регіони розміщення дата– центрів AWS

Кожен регіон має кілька «зон доступності», рис. 3.6 ,які складаються з одного або декількох центрів обробки даних, кожен з резервним живленням, мережею і ізольованістю один від одного.

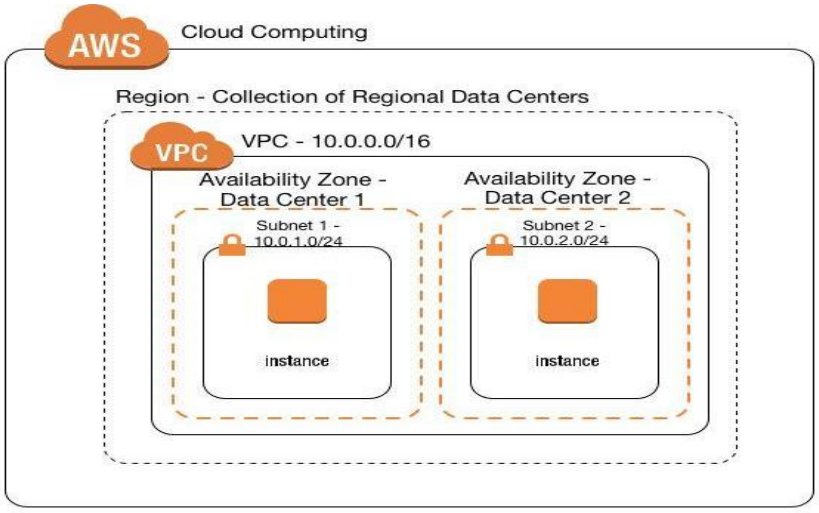

Рисунок 3.6 – Організаційна структура хмари

AWS – це безпечна, надійна технологічна платформа, що пройшла необхідні перевірки і отримала сертифікати, визнані в даній галузі: PCI DSS рівня 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, SOC 1 і звіти перевірки SOC 2. У їх сервісах і центрах обробки даних передбачено декілька рівнів операційного та фізичного захисту, що дозволяє забезпечити збереження і безпеку даних [9].

AWS надає низку хмарних сервісів безпеки, у тому числі AWS Identity and Access Management (IAM), які дозволяють адміністраторам визначати та керувати доступом користувачів до ресурсів. Крім того, організації AWS дозволяють компанії створювати політики для кількох облікових записів AWS та керувати ними [10].

Amazon Web Services також представила інструменти, що автоматично оцінюють потенційні ризики безпеки. Amazon Inspector аналізує середовище AWS на наявність уразливостей, які можуть вплинути на безпеку та відповідність вимогам. Amazon Macie використовує технологію машинного навчання для захисту конфіденційних хмарних даних.

AWS також включає інструменти та сервіси, що забезпечують шифрування на основі програмного та апаратного забезпечення, захист від DDoS - атак, надання сертифікатів Secure Sockets Layer (SSL) і Transport Layer Security (TLS) і фільтрацію потенційно шкідливого трафіку для веб-додатків. AWS створила сервіси KMS і CloudHSM для управління ключами. Надає послугу запобігання втрати даних, керовану штучним інтелектом.

Amazon пропонує найвищі на ринку засоби здійснення обчислень і засоби зберігання даних. Широкий діапазон типів віртуальних машин (136 типів віртуальних машин в 26 родинах віртуальних машин) - надає можливість запуску від невеликих web-систем до найбільших робочих навантажень HPC (High Performance Computing) і SAP [1].

Amazon Relational Database Service, який включає створення баз Oracle, SQL Server, PostgreSQL, MySQL, MariaDB та пропрієтарну високопродуктивну базу даних Amazon Aurora, надає користувачам AWS систему управління реляційними базами даних. Також AWS створив NoSQL базу даних - DynamoDB.

AWS пропонує ряд платформ для розробки та використанні штучного інтелекту, а також готові програми на його основі. Сервіс Amazon Lex створений для голосових та текстових чат-ботів, Amazon Polly для перетворення тексту на мову і Amazon Rekognition для аналізу зображень та осіб. AWS також надає розробникам технології для створення інтелектуальних

програм, заснованих на технологіях машинного навчання. AWS забезпечують підтримку Alexa Voice Services і розробник може використовувати Alexa Skills Kit для створення голосових програм для пристроїв Echo [10].

AWS Mobile Hub пропонує набір інструментів та сервісів для розробників мобільних програм, включаючи AWS Mobile SDK, який надає зразки коду та бібліотеки. Розробник мобільних додатків також може використовувати Amazon Cognito для керування доступом користувачів до мобільних додатків, а також Amazon Pinpoint для надсилання push-повідомлень кінцевим користувачам додатків та подальшого аналізу ефективності цих комунікацій.

Сервіси обміну повідомленнями AWS забезпечують основний зв'язок між користувачами та програмами. Amazon Simple Queue Service (SQS) — це керована черга повідомлень, яка надсилає, зберігає та отримує повідомлення між компонентами розподілених програм, щоб гарантувати, що частини програми працюють належним чином. Amazon Simple Notification Service (SNS) дозволяє компаніям надсилати повідомлення про публікацію/підписку кінцевим точкам, таким як кінцеві користувачі або служби. SNS включає функцію обміну мобільними повідомленнями, що дозволяє надсилати push-повідомлення на мобільні пристрої. Amazon Simple Email Service (SES) надає IT-фахівцям та маркетологам платформу для відправлення та отримання електронних листів [10].

AWS пропонує інструменти розробки доповненої реальності (AR) та віртуальної реальності (VR) через сервіс Amazon Sumerian. Він дозволяє користувачам створювати програми AR та VR, а також дозволяє користувачам тестувати та публікувати програми у браузері.

AWS виявився лідером у моєму рейтингу, створеному під час написання минулої кваліфікаційної роботи, за низкою переваг - в ході технічного експерименту, він має зручний інтерфейс, багато програм лояльності, гарні програми навчання, має величезну спільноту, та багато сервісів.

3.2 Навчальні програми хмарних провайдерів

Для того, щоб створити свою ефективну навчальну платформу необхідно проаналізувати ринок, визначити, які навчальні платформи та сертифікації існують, які в них є недоліки та переваги, що можна покращити та на що потрібно звернути увагу.

Хмарні обчислення – один з головних трендів останнього часу, що активно розвивається.

Освоєння цієї технології вимагає здобуття нових навичок і від IT–фахівців, і від користувачів. Перед фахівцями досвід роботи з хмарами відкриває перспективи кар'єрного зростання, а користувачам такі знання стануть у нагоді, щоб самостійно знаходити потрібні сервіси та ефективно застосовувати їх для бізнесу.

У цій галузі є кілька напрямків: по–перше, вендори навчають використанню своїх продуктів — правильному управлінню порталом самообслуговування, розумінню тарифів, створенню власних рішень на їх платформі. Такі курси можна пройти, наприклад, за продуктами Amazon, Google або Microsoft, CSSP, Oracle.

Крім того, існують курси з платформ, які використовуються для створення приватних або публічних хмар, наприклад, за продуктами VMware, OpenStack. Дещо відокремлено стоять спеціальні курси з окремих SaaS– і PaaS–рішень, у тому числі з аналізу та управління даними. Такі курси орієнтовані на розробників ПЗ та архітекторів рішень. І нарешті, є комплексні курси щодо побудови безпеки у хмарі або проектування хмарної інфраструктури.

Курси можуть бути розбиті на наступні групи:

- загальноосвітні, які освітлюють як працюють хмари;
- користувальницькі, найчастіше орієнтовані конкретні пропозиції постачальників;
- поглиблені, призначені консультантам та розробникам хмарної системи.

Як правило, наприкінці навчання можна пройти сертифікацію, це дозволяє підтвердити рівень знань спеціаліста. Крім того, ряд вендорів потребує сертифікації від компаній–партнерів для отримання відповідного статусу, тому спеціалістам хмарних провайдерів та інтеграторів необхідна сертифікація.

Первинними цілями підготовки та складання сертифікаційних іспитів є розширення, поглиблення та структурування знань з хмарної платформи. Важливо розуміти, що навіть, якщо ви постійно та регулярно працюєте з продуктом, часто ви добре і глибоко розумієте окремі сервіси продукту, іноді слабко торкаючись інших. Коли ви готуєтеся до іспиту, то в процесі підготовки охоплюєте досить широкий спектр різноманітних тем, сервісів, функціоналу продукту та платформи, що дозволяє розширити професійний кругозір.

Іншим плюсом отримання сертифікатів є те, що це може бути бажаним, а іноді обов'язковим вимогам замовника принаймні фахівців на проект або просто вимогою до позиції у роботодавця. Важливим моментом є те, що

наявність певної кількості сертифікованих фахівців іноді просто необхідна для підтримання певного рівня партнерського статусу компанії–партнера з вендором. Однак, було б помилково думати, що сертифікація сама по собі істотно збільшить вашу вартість на ринку праці як фахівця. Знання мають бути підкріплені досвідом роботи з продуктом у реальних проектах.

3.3 Види сертифікацій та навчальних програм

3.3.1 AWS (Amazon Web Services)

Amazon зараз є найбільшим постачальником хмарних послуг. Він обслуговує мільйони підприємств та приватних осіб у всьому світі. З хмарною сертифікацією AWS можна відповідати багатьом спеціальностям сертифікованого професіонала.

Від навичок кібербезпеки, впровадження шифрування, мережний інжинеринг, зберігання та управління даними. Сертифікації діляться на три основні рівні, початковий з досвідом до 6 місяців, середній від 1 року та високий від 2–х років досвіду використання. Починаючи із середнього рівня, йде поділ на напрями, для адміністраторів, архітекторів, розробників та для девопс інженерів. Окремою категорією є сертифікації за спеціальностями такими як: машинне навчання, аналіз даних, просунутий рівень архітектури мереж, бази даних та безпека [10].

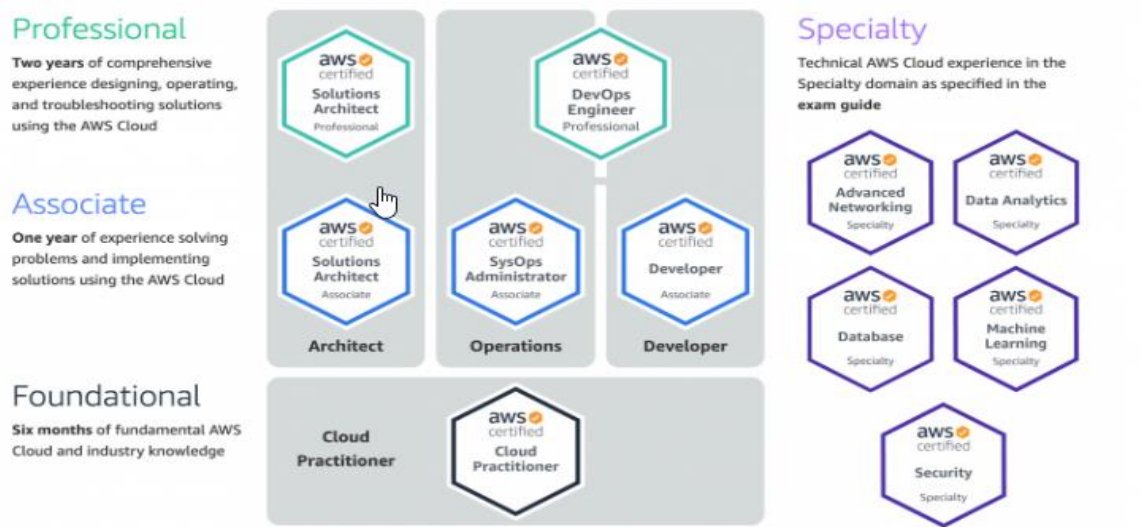

Рисунок 3.5 – Види сертифікацій AWS

Підготуватися до сертифікації можна на платформах AWS. Хмарний провайдер надає докладну документацію та відео лекції, а також пробне тестування. Враховуючи величезну складність іспиту, фахівці вважають за доцільне готуватися відразу на декількох платформах, наприклад, таких як linux–academy, A Cloud Guru і Whizlabs отримуючи доступ не просто до відео матеріалу, але й виконуючи захоплюючі лабораторні роботи.

3.3.2 Microsoft Azure

У даний час Microsoft займає другу за величиною частку простору хмарних обчислень. Вони пропонують кілька сертифікатів в області служб баз даних та хмарних обчислень. Фахівці з хмарних обчислень Azure є одними з найпопулярніших професіоналів у галузі хмарних технологій. Сертифікація передбачає кілька ступенів: при складанні одного з іспитів ви отримуєте статус Microsoft Certified Professional (MCP) [13].

Першим етапом сертифікаційного шляху є статус Cloud Platform Microsoft Certified Solutions Associate (MCSA). Другим щаблем є статус Microsoft Certified Solutions Expert (MCSE), для його отримання необхідно мати статус MCSA та доповнити скласти ще один із іспитів цього списку [13]:

- 70–533: Implementing Microsoft Azure Infrastructure Solutions
- 70–535: Architecting Microsoft Azure Solutions

Успішне складання обох іспитів дозволило пройти перший ступінь сертифікації по хмарній платформі Microsoft Azure та отримати статус: Cloud Platform Microsoft Certified Solutions Associate (MCSA).

Офіційна документація – це, на мій погляд, один із найкращих ресурсів для підготовки до іспиту. Вона чудово структурована, інформативна, легко читається та сприймається, забезпечена великою кількістю прикладів коду, команд та практичних вправ для закріплення теоретичних матеріалів. Також для підготовки до іспиту можна скористатися електронним підручником.

Azure Architecture Center – відмінний ресурс, у якому зібрані найкращі практики та досвід Microsoft із проектування різних рішень у Azure. Велика увага приділяється різним архітектурним патернам та його застосовності у різних сценаріях. Також даються рекомендації, як реалізовувати той чи інший архітектурний шаблон, використовуючи сервіси Azure. Спробувати розгорнути той чи інший архітектурний шаблон в Azure легко і просто, використовуючи посилання на розгортання шаблонів ARM через Azure Portal [13].

Навчальні курси сторонніх ресурсах. На порталі edx досить багато офіційних навчальних курсів від Microsoft, включаючи матеріали з Microsoft Azure. Інші ресурси, такі як Udemy або Linux Academy також можуть бути корисними як додаткові матеріали.

3.3.3 Google cloud platform

Сертифікація Google має велике значення для демонстрації вашої ефективності у використанні продуктів Google Cloud.

Сфери діяльності варіюються від адміністрування даних, ідентифікації хмари, мережевих ресурсів, загальної хмарної інженерії до інших спеціальностей, що надаються Google Associate Cloud Engineering Certification. Абсолютно як і перші хмари з списку має і документацію і різні підготовчі курси [12].

3.3.4 Сертификация IBM Cloud

IBM також є великим гравцем у сфері хмарних послуг. Багато компаній зі списку також шукають для роботи фахівців з хмарною сертифікацією IBM.

Такі сертифікати, як сертифіковані IBM розробники додатків, є одними з найпопулярніших серед підприємств та агенцій з найму.

Іспит тестує кандидатів у галузі Red Hat OpenShift, Virtual Private Cloud, аналітики баз даних, безпеки та багато іншого.

3.3.5 Cloud Security Alliance

Cloud Security Alliance (CSA) – це некомерційна організація, яка просуває дослідження передових методів захисту хмарних обчислень та використання хмарних технологій для захисту інших форм обчислень. CSA використовує досвід галузевих фахівців, асоціацій та урядів, а також своїх корпоративних та індивідуальних членів, щоб пропонувати дослідження, навчання, сертифікацію, заходи та продукти, що стосуються хмарної безпеки [19].

Вони займаються управлінням хмарних даних, працюють над розробкою принципів та зіставленням їх з новими технологіями та методами, щоб гарантувати конфіденційність, доступність, цілісність, конфіденційність та безпеку даних у загальнодоступних та приватних хмарах. Займаються розробкою варіантів використання та реалізації Інтернету речей, а також

створенням дієвих посібників, які дозволяють фахівцям з безпеки забезпечувати безпеку своїх розгортань. Також досліджують безпеку контейнерів, додатків та мікросервісів.

Cloud Security Alliance також пропонує професійні сертифікати хмарної безпеки.

- CSA CCSK (Сертифікат знань про хмарну безпеку) — це веб-перевірка компетентності людини з основних питань хмарної безпеки. Метою CCSK є забезпечення розуміння проблем безпеки та кращих практик у різних галузях хмарних обчислень. Рекомендується для IT-аудиторів, CCSK потрібен для деяких частин програми CSA STAR.
- CSA CCSP (Certified Cloud Security Professional) – це глобальний сертифікат, що відображає найвищий стандарт знань у сфері безпеки хмарних обчислень. Він був створений спільно Альянсом безпеки хмарних обчислень та Міжнародною радою зі стандартизації – розпорядниками інформаційної безпеки та безпеки хмарних обчислень. Програма CCSP рекомендується для досвідчених фахівців у галузі IT/ІКТ (інформаційно-комунікаційних технологій), які займаються архітектурою IT; проектування веб- та хмарної безпеки; інформаційна безпека; управління, ризики та відповідність або IT-аудит. Крім того, CCSP корисний для людей, які працюють з організаціями, які віддані DevSecOps, Agile або бімодальним IT-практикам [19].

Беручи до уваги, що безпека в Інтернет просторі, так само як і в хмарних середовищах, набирає популярності, і компанії роблять все можливе, щоб забезпечити хоча б базові навички працівників, та проаналізувавши ринок, я бачу невелику кількість платформ, що представляють курси з безпеки в хмарному середовищі. Є обмежена кількість навчальних програм, які складаються виключно теоретичного матеріалу, і максимум тестів за темою курсу, різної якості і високої ціни, наприклад курс лекцій Advanced Cloud Security Practitioner від CSA коштує 2200$ і це не найвища ціна на ринку (курс не включає практичні роботи). Тож я бачу нагальну проблему, в недостатності матеріалів для навчання, ціні матеріалів, недостатності платформ з практичним навчанням. Практика як елемент навчального процесу проводиться з метою закріплення та розширення знань і є неодмінною частиною навчання чи вдосконалення спеціалістів будь- якого рівня. Тож створена мною платформа буде базуватися на практичних засадах.

4 РОЗРОБКА НАВЧАЛЬНОЇ ПЛАТФОРМИ

У міру того, як хмарні обчислення стають мейнстримом, зростають і проблеми безпеки, пов'язані з ними.

Більшість користувачів публічних хмар розуміють, що це спільна відповідальність між постачальником хмарних послуг та користувачами.

За даними Gartner, 95% всіх збоїв у хмарній безпеці відбуваються через неправильні конфігурації. Експерти зазначили, що людям, які бажають працювати з хмарами, доведеться постійно оновлювати та розширювати знання.

Навчання у сфері хмар – процес динамічний та безперервний. Він вимагає постійного підживлення знаннями, причому практичними знаннями – потрібно тестувати технології та їх оновлювати, розбиратися в сервісах, що часто оновлюються, і бути постійно в темі. Саме тому для сертифікації фахівців замало пройти курс у навчальних платформах. Вирішальну роль відіграє самопідготовка: вебінари, лабораторні роботи, очні заходи, книги, електронні інформаційні ресурси та блоги, які найчастіше проводяться англійською мовою, та практика. Вивчивши ринок, я побачила недостатність практичних, лабораторних робіт з безпеки в хмарі. Тому створена платформа зосереджена на практиці, але якщо буде необхідно можливо додати і лекційний матеріал. Правильне виконання тестів на проникнення в середовище AWS - складне завдання, яке вимагає знань і практики в різних областях. Для проведення гідного тесту потрібні знання AWS, так і знання слабких місць хмари.

Проблема, полягає в тому, що нині немає простого способу перевірити та визначити ці навички. Як приклад: для веб–додатків є різноманітні ресурси для безпосередньої багаторазової перевірки ваших знань, навичок та прийомів. Ці ресурси включають такі речі, як програми пошуку помилок, CTF і віртуальні машини/веб–застосунки з вразливістю, які ви можете налаштувати на своєму персональному комп'ютері для всіх видів тестування (наприклад, WebGoat OWASP).

Немає таких ресурсів для вивчення методів тестування на проникнення та атак на середовища AWS. AWS та хмара в цілому з кожним днем все більше і більше впроваджуються компаніями по всьому світу, а це означає, що зловмисники також заохочуються.

Щоб задовольнити ці потреби, була створена платформа, головною метою якої є навчання ризикам безпеки в AWS, перевірка знань, вивчення методів атак, та тестування середовища.

4.1 Публічна основа проекту

Відправною точкою, ідеєю для створення моєї навчальної платформи став публічний проект Cloud Goat (CG) від Rhino Security Labs.

Компанія Rhino Security Labs, що займається тестуванням на проникнення, пропонує комплексні оцінки безпеки. Напрямок роботи виявлення вразливостей у різних технологіях, наприклад, AWS та IoT.

Cloud Goat представляє собою продукт для тестування свої знать та освоєння нового матеріалу в області безпеки, має декілька версій та активно розробляється, є рекламним продуктом компанії в тому числі. Продукт компанії має 11 сценаріїв різної складності створення уразливої інфраструктури для AWS, встановлює необхідні програми та розгортає інфраструктуру за допомогою Doker, ядро продукту написано на python.

Я думала над тим, що хочу створити інтерактивну платформу з мультикористувацьким режимом, контролем проходження, нотифікаціями і графічним представленням результатів учасників. Щоб з цією платформою можна було влаштовувати масові заходи, під час яких фахівці з різного рівня вирішують будь-яку проблему на певний час, або використовувати в рамках лабораторних робіт. Звісно CG однокористувацький, і його не можливо використовувати повністю, а лише ідею і логіку сценаріїв рівнів, яку так само потрібно повністю переробити.

4.2 Створення навчальної платформи

Отже, основними цілями розробки проекту стала побудова навчальної платформи в означених напрямках.

Основні напрямки розробки проекту:

– розробка механізму нотифікації (старт курсу, підписка на нотифікації, старт раундів, проходження сценаріїв, завершення курсу);

– створення механізмів контролю проходження (старт проходження, та кінець, аналіз прогресу проходження користувача);

– мультикористувацький режим (можливість одночасного проходження сценаріїв користувачами, оптимізація ресурсів);

– візуалізація процесу проходження курсу;

– автоматизація розгортання курсу та інших процесів.

Розглянемо глобальну ідею додатку – студент приймає на себе роль зловмисника, який повинен знайти вразливості системи та досягнути зазначеної мети. На кожному раунді для нього створюється своя інфраструктура та цілі. Для кожного раунду студенту дається список сервісів, які можуть бути задіяні та опис задачі, що дає йому напрямок, у якому потрібно шукати вразливості.

Додаток створює вразливе за своєю конструкцією середовище AWS декількох типів, а також потрібну інфраструктуру для контролю проходження раундів та нотифікацій та фінальний дашборд з прогресом участі в режимі реального часу.

4.2.1 Опис структури платформи

Для створення інфраструктури я створила окрему віртуальну машину за допомогою Vagrant. Vagrant - це спеціальне програмне забезпечення для створення та конфігурування та управління віртуального середовища розробок. Для цього я описала потрібну конфігурацію віртуальної машини у спеціальному Vagrant файлі наведений у додатку А. В цьому файлі я встановила Terraform, AWS CLI, Jenkins та інші додаткові налаштування.

Terraform – це інструмент від компанії Hashicorp, для декларативного керування інфраструктурою. Для нього створена власна мова конфігурації HCL. Вона сумісна з JSON і використовується для створення файлів конфігурації, що описують інфраструктурні ресурси, які потрібно розгорнути. Даний інструмент, описує хмарну інфраструктуру у вигляді списку ресурсів, пов'язаних один з одним і які можуть бути згруповані в модулі. Файли конфігурації описують для Terraform компоненти, необхідні для запуску окремого додатка або масштабної інфраструктури. Terraform генерує план виконання, що описує, що він буде робити для досягнення бажаного стану, а потім виконує його для побудови описаної інфраструктури. Під час виконання він направляє виклики до API хмарного провайдера [18].

AWS CLI - це уніфікований інструмент для керування сервісами AWS.

Jenkins – це програмна система з відкритим вихідним кодом Java, призначена для забезпечення процесу безперервної інтеграції програмного забезпечення [11]. Він дозволяє автоматизувати частину процесу розробки програмного забезпечення, в якому не обов'язкова участь людини, забезпечуючи безперервну інтеграцію функцій. Jenkins є безкоштовним інструментом, що володіє величезними можливостями у вигляді тисяч плагінів, які постійно додаються та оновлюються.

Для конфігурації Jenkins серверу були написані два конфігураційні файли з основними налаштуваннями, наведені у додатку А.

Я створила Jenkins job, що по таймеру, або за мануальним запуском стартує запуск створення інфраструктури сценаріїв та старту курсу. Інфраструктура платформи створюється завчасно за допомогою Terraform.

Вся інфраструктура описана за допомогою terraform і буде описана нижче.

Для виконання функцій контролю проходження раундів, нам потрібна база даних у даному випадку Dynamo DB. Dynamo DB – система управління базами даних класу NoSQL у форматі «ключ – значення», куди ми будемо записувати користувацькі дані за допомогою лямбда функцій. Amazon Lambda – це безсерверний обчислювальний сервіс, керований подіями, який дозволяє запускати код практично для будь–якого типу додатків або серверних служб без надання послуг або керування серверами.

Для нотифікації я використовую Amazon SNS – служба обміну повідомленнями, Amazon Simple Queue Service (SQS) – сервіс чергових повідомлень, база даних, лямда функції та терраформ Насамперед було застосовано, більше технологій та сервісів, ніж показано та описано в цьому підрозділі. На рисунку 4.1 зображена глобальна структура платформи.

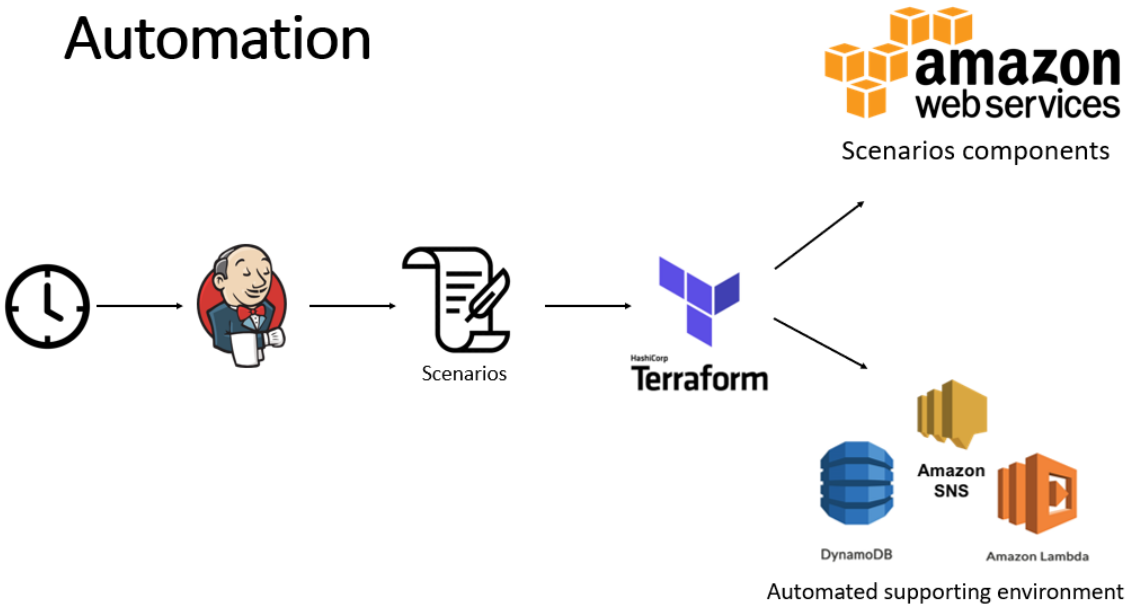

Рисунок 4.1 – Глобальна структура додатку

4.2.2 Створення мультикористувацького режиму

Одною з цілей було зробити систему, яка може працювати як і для індивідуального використання, так і для одночасного проходження великої кількості студентів, наприклад для створення конкурсу, або відбору кандидатів на практику чи роботу.

Чинники для врахування:

- виключення взаємного впливу та колізій (створення індивідуальної інфраструктури для кожного учасника, розмежувати права таким чином, щоб жодний студент не міг впливати на роботу інших студентів);
- обходження лімітів Amazon, на використання ресурсів у великих обсягах;
- економічність використання ресурсів (можливість створення деяких спільних ресурсів, автоматичне видалення непотрібних ресурсів та інше).

Структура мультикористувацького режиму зображена на рис. 4.2.

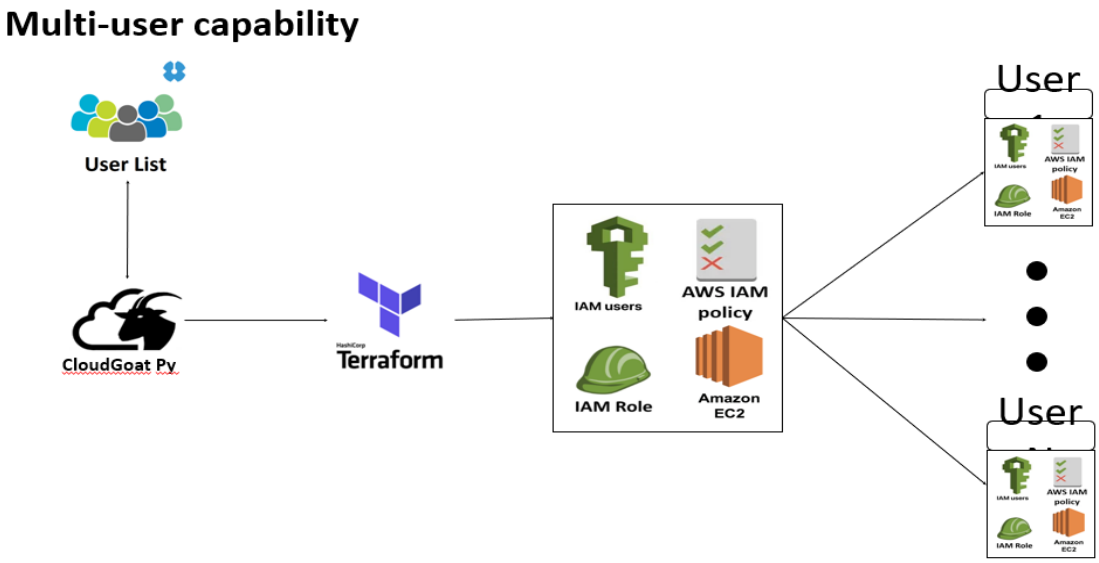

Рисунок 4.2 – Мультикористувацький режим

Створили файл, в якому знаходяться поштові адреси учасників, терраформ обробляє ці адреси, записує їх в базу даних, а також за допомогою регулярного виразу, відокремлює поштові спецсимволи та назву пошти, і записує в базу даних ім’я та прізвище (це буде потрібно для технічних потреб), також він надалі створює іменовані ресурси для кожного користувача окремо за допомогою модуля терраформ. Наприклад, для кожного користувача створюється в AWS IAM користувач, ролі та полісі.

AWS Identity and Access Management (IAM) забезпечує точний контроль доступу у всіх сервісах AWS. За допомогою IAM ви можете вказати, хто може отримувати доступ до певних сервісів та ресурсів та за яких умов [11]. Користувачам IAM або сервісам AWS можна присвоїти ролі для отримання

тимчасових даних для доступу, які вони можуть використовувати для викликів API AWS. IAM роль – це набір IAM полісі, полісі – це список ресурсів та дій з ними, правильно створювати на кожну групу дозволів окрему полісі.

А усі сценарії вже змінені з урахуванням лімітів, економії, а головне - виключення взаємного впливу та колізій.

4.2.3 Створення системи моніторінгу

Наступною ціллю є створення моніторингу проходження раундів, для цього використовуємо такі сервіси як, AWS CloudTrail – відстежує та записує активність облікового запису у вашій інфраструктурі AWS, надаючи контроль над зберіганням, аналізом [11]. Amazon CloudWatch – служба моніторингу та спостереження. За допомогою цих сервісів, усі данні студента платформи агрегуються за допомогою лямбда функцій та записуються в базу даних. Система моніторінгу проходженні рівнів зображена на рис. 4.3.

Наприклад, ми знаємо, щоб в пройти одне з завдань, користувачу потрібно, виконати список дії, наприклад, aws iam set-default-policy – це команда, яка назначає поліс, і які належать користувачеві.

Під кожний раунд написана власна функція, яка шукає правильні команди у правильному порядку, вона також фіксує швидкість проходження, що запобігає обману та списуванню з боку студента. Якщо виникають якісь питання про чесність студента завжди можна відфільтрувати його дії у CloudTrail за ім’ям і якщо, крім заданих команд, студент не виконував інші, це може означати тільки знайдені відповіді.

Тож лямда запускається при старті раунду, шукає вказані дії у CloudTrail, якщо вона їх знаходить то фіксує час проходження раунду та записує у базу даних.

Функція нотифікацій бачить новий запис у базі даних про проходження раунду і надсилає користувачу лист з вітанням, та завданням для наступного раунду, далі детальніше. Складності з якими я зустрілась на даному етапі, існують деякі дії користувача, що надходять у CloudTrail з затримкою, наприклад, дії деякі дії з IAM, це могло б вплинути на результати у фінальній таблиці, або на час проходження, але так як затримка фіксована і для кожної дії своя і відома, для даного випадку вона складає 15хв, це не впливає на фінальні результати.

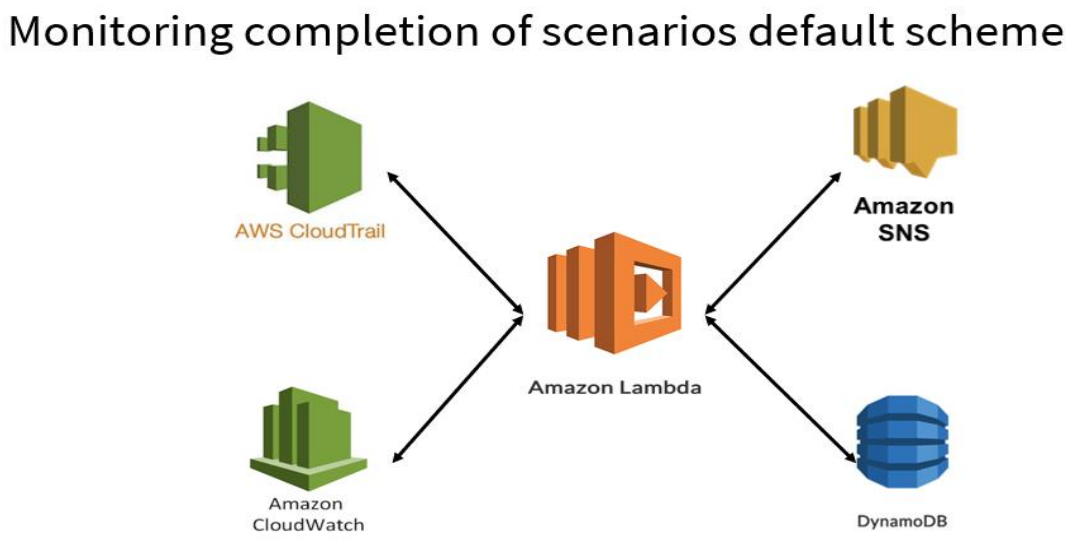

Рисунок 4.3 – Моніторинг проходження рівнів

4.2.4 Створення системи нотифікацій

Було застосовано декілька підходів для підвищення надійності та забезпечення доставки повідомлень. Для створення системи нотифікацій були використані Amazon Lambda, SNS, SQS, база даних DynamoDB.

Створено низку лямбда функцій, які забезпечують різні види нотифікацій, обробки тексту, запис результатів відправки в базу даних, щоб знати, що користувач отримав лист, та не відправляти його повторно. Було використано в якості шаблонів Dunia 2, які записані в базу даних, інформація до яких підставляється з самої таблиці чи зі змінних терраформу.

Типи створених нотифікацій:

- старт курсу (вітання та вступне слово про курс);
- підписка на системні нотифікації SNS;
- старт раунду, загальний опис та завдання;
- листи з ключами доступу;
- завершення раунду;
- кінець курсу (оголошення результатів, та вітання).

4.3 Основні напрямки вразливостей для створення платформи

Cloud Security Alliance нещодавно опублікував звіт The Treacherous 12 - докладний список найбільш значних загроз хмарній безпеці. Список був складений шляхом опитування галузевих експертів та об'єднання результатів з

аналізом ризиків для визначення загроз, які найбільш поширені для організацій, що зберігають дані у хмарі. Список включає:

- виток даних;
- недостатнє управління ідентифікацією, обліковими даними та доступом;
- небезпечні інтерфейси та API;
- системні вразливості;
- злом облікового запису;
- зловмисні інсайдери;
- розширені постійні загрози;
- втрата даних;
- недостатня комплексна перевірка;
- зловживання та неправомірне використання хмарних сервісів;
- відмова в обслуговуванні;
- загальні технологічні вразливості.

При атаці на будь–яку інфраструктуру AWS студенту як зловмиснику потрібно до множини цілей. Цей список ілюструє основні цілі користувача платформи, на які йому слід звернути увагу:

- підвищення привілеїв;
- реєстрація, моніторингу відхилень;
- перелік даних та інформації;
- ексфільтрація даних;
- постійний доступ.

Інші цілі атак зловмисників:

- знищення (видалення ресурсів);
- викуп (утримання ваших ресурсів/даних у заручниках);
- виснаження грошей/ресурсів (наприклад, атаки типу «відмова в обслуговуванні»);
- криптомайнінг (запуск майнерів криптовалюти в особистому кабінеті);
- атаки, орієнтовані на клієнта (націлені на користувачів послуг, які клієнт пропонує публічно).

4.4 Опис рівнів платформи

Рівні платформи були створені з урахуванням списку вразливостей наведеному у розділі 4.3.

Створена інфраструктура для 5 раундів, кожний раунд має свої цілі та особливості.

4.4.1 Рівень 1 - вразливе налаштування політик IAM

Перший рівень, простий за складністю і не потребує багато часу для розв'язання. Задіяні ресурси – один IAM користувач та п'ять версій IAM політик. Даний рівень ілюструє уразливість варіювання політик. Ціль рівня підвищення привілеїв.

Зловмисник, починаючи з користувача IAM, має лише кілька обмежених - на перший погляд невинних - привілеїв. Він аналізує привілеї користувача та помічає дозвіл SetDefaultPolicyVersion, що дозволяє отримати доступ до 4 інших версій політики. Після перегляду старих версій політики зловмисник виявляє, що одна з версій пропонує повний набір прав адміністратора.

Він відновлює повну версію політики адміністратора, отримуючи повні права адміністратора та можливість виконувати будь-які шкідливі дії за власним бажанням.

Як останній крок зловмисник може вибрати повернення версії політики користувача до вихідної, тим самим приховавши свої дії та справжні можливості користувача IAM.

4.4.2 Рівень 2 - неправильно налаштований проксі–сервер EC2

Даний рівень невеликий за обсягом та середньої важкості, ресурси які були задіяні: IAM, S3, EC2. Ціль рівня – викрадення файлів.

Зловмисник знаходить IP-адресу екземпляра EC2 і після певної розвідки розуміє, що він діє як зворотний проксі-сервер. Це звичайне явище, особливо для організацій, які переходять із локального використання в хмару.

Після деяких досліджень зловмисник використовує `CURL`, щоб відправити запит на веб-сервер і встановити заголовок хоста на IP-адресу служби метаданих EC2. Спеціально створена команда CURL зловмисника виконується успішно, повертаючи ідентифікатор ключа доступу, секретний ключ доступу та маркер сеансу профілю екземпляра IAM, приєднаного до екземпляра EC2.

Маючи в руках облікові дані ролі IAM, зловмисник тепер може досліджувати хмарне середовище жертви, використовуючи дозволи, надані цій ролі.

Зловмисник отримує доступ до сховища даних S3 та знаходить кілька файлів, повних конфіденційної інформації, і може завантажити їх на свою локальну машину для розповсюдження чи продажу даних.

4.4.3 Рівень 3 -вразливість інстанс профайлів

Даний рівень середньої важкості та середній за обсягом, створено IAM користувача та EC2 інстанс. Ціль рівня - видалити cg-super-critical-security-server і відкрити шлях для подальших підступних дій.

Починаючи з користувача IAM "Scenario3_user", зловмисник використовує свої обмежені привілеї для вивчення середовища. Спочатку дивиться, які EC2 інстанси створені у середовищі, знаходить свою ціль - "cg-super-critical-security-server" - але не в змозі вплинути безпосередньо на ціль, зловмисник шукає інший шлях. Він вирішує подивитись наявні профілі та ролі EC2 в обліковому записі, визначивши профіль екземпляра, який він може використовувати, і перспективну роль. Далі зловмисник створює нову пару ключів EC2, та створює новий екземпляр EC2 з цією парою ключів, що означає, що тепер він має до нього доступ.

Він створює роль EC2 на повний доступ на профайл інстанса. На останньому етапі експлойту зловмисник приєднує до екземпляра EC2 профайл екземпляра з повними правами адміністратора.

Отримавши доступ і використовуючи новий екземпляр EC2 як проміжну платформу, зловмисник може виконувати команди AWS CLI з повними правами адміністратора, наданими роллю приєднаного профілю.

Зловмисник, нарешті, може припинити роботу EC2 "cg-super-critical-security-server", завершивши сценарій.

4.4.4 Рівень 4 - експлойт веб–програми SSRF

Даний рівень середньої важкості та середній за обсягом, створено IAM користувача та EC2 інстанс та S3. Ціль рівня – запустити лямбду функцію.

Як користувач IAM Scenario4_1_user, зловмисник досліджує середовище AWS і виявляє, що може подивитись які лямбда-функції створені в обліковому записі. У функції Lambda зловмисник знаходить ключі доступу AWS, що належать іншому користувачу – користувачу IAM Scenario4_2_user.

Тепер, працюючи як Scenario4_2_user, зловмисник виявляє екземпляр EC2, на якому запущено веб-додаток, уразливий до вразливості SSRF. SSRF

(підробка запиту на стороні сервера) – це атака, яка дозволяє надсилати запити від імені сервера до зовнішніх або внутрішніх ресурсів.

Використовуючи вразливість SSRF за допомогою параметра `?url=...`, зловмисник викрадає ключі AWS із служби метаданих EC2. Використовуючи ключі від екземпляра EC2, зловмисник знаходить приватний сегмент S3, що містить інший набір облікових даних AWS для більш потужного користувача: Scenario4_3_user.

Тепер, працюючи як Scenario4_3_user, з повними привілеями адміністратора, зловмисник може викликати оригінальну функцію Lambda для завершення сценарію.

4.4.5 Рівень 5- експлойт бази даних

Даний рівень високої важкості та середній за обсягом, створено два IAM користувача, ELB, S3, EC2, RDS. Це перший рівень в якому є декілька варіантів проходження. Ціль рівня – дістати секретні данні з бази даних.

Користувач IAM Scenario5_1_user, зловмисник досліджує середовище AWS і виявляє веб-додаток, розміщений за захищеним Load Balancer. Потім зловмисник перераховує сегменти S3, виявляючи один, який містить журнали Load Balancer. Переглядаючи вміст журналів Load Balancer, зловмисник бачить, що веб-програма має секретну сторінку адміністратора.

Відвідавши секретну URL-адресу адміністратора, зловмисник виявляє, що веб-програма вразлива до атаки віддаленого виконання коду (RCE) через секретний параметр, вбудований у форму.

Зловмисник використовує цю вразливість, щоб отримати доступ до оболонки до екземпляра EC2, на якому розміщено веб-програму.

Перший варіант проходження рівня. Тепер, працюючи через екземпляр EC2 (і, отже, працюючи з більш широкими дозволами своєї ролі), зловмисник може отримати доступ до приватного сховища даних S3.

Усередині сховища S3 зловмисник знаходить текстовий файл, залишений безвідповідальним розробником, який містить облікові дані для входу в базу даних RDS. Далі зловмисник використовує екземпляр EC2 для виявлення бази даних RDS, на яку посилається файл облікових даних.

Нарешті, зловмисник може отримати доступ до бази даних RDS за допомогою знайдених облікових даних і отримує мету сценарію: секретний текст, що зберігається в базі даних RDS.

Другий варіант проходження раунду. Вражений раптовим натхненням, зловмисник запитує службу метаданих EC2 і виявляє облікові дані та адресу бази даних RDS. Далі він отримує доступ до бази даних RDS за допомогою знайдених облікових даних і отримує мету сценарію: секретний текст, що зберігається в базі даних RDS.

Третій варіант проходження від іншого користувача, може бути окремим рівнем. Зловмисник Scenario5_2_user досліджує середовище AWS і виявляє, що може переглянути список сховищ даних S3, використовуючи свої початкові ключі. Він виявляє кілька S3 сховищ, але має права лише до одного з них. Усередині цього сховища він знаходить SSH ключі.

Зловмисник знаходить EC2 за балансувальником навантаження. Зловмисник виявляє, що ключі SSH, знайдені в сегменті S3, підходять до EC2.

Тепер, працюючи через екземпляр EC2 (і, отже, працюючи з його роллю замість Scenario5_2_user), зловмисник може виявити та отримати доступ до приватного сегмента S3.

Усередині приватного сегмента S3 зловмисник знаходить текстовий файл, залишений безвідповідальним розробником, який містить облікові дані для входу в базу даних RDS.

Зловмисник виявляє базу даних RDS, на яку посилаються у файлі облікових даних.

Він отримає доступ до бази даних RDB, використовуючи облікові дані, які вони знайшли, і отримати мету сценарію: секретний текст, що зберігається в базі даних RDS.

4.5 Візуалізація проходження раундів та результати роботи

Для виконання мети візуалізації були створені лямбди функції, які перевіряли процес проходження, а також функція, яка створює та оновлює таблицю з результатами проходження в режимі реального часу, наведений на рис. 4.4.

Рисунок 4.4 – Приклад створеної візуалізації

Для того, щоб протестувати створену платформу платформу, було запрошено 15 учасників з різним досвідом роботи з AWS та кваліфікацією. Для проходження 5 рівнів їм було дано 8 годин часу, та можливість отримувати підказки. Результати проходження наведені у таблиці 4.1. junior middle senior

Таблиця 4.1 – Дослідження роботи платформи

Учасники	Досвід	Кількість пройдених рівнів	Час проходження	Використані підказки	Не пройдені рівні
Учасник 1	Senior	5	6 год. 37 хв.	-	-
Учасник 2	Senior	5	7 год. 7 хв.	-	-
Учасник 3	Senior	4	7 год. 11хв.	-	5
Учасник 4	Middle	5	6 год. 45 хв.	1	-
Учасник 5	Middle	5	6 год. 28 хв.	2	-
Учасник 6	Middle	5	7 год. 30 хв.	3	-
Учасник 7	Middle	4	5 год. 42 хв.	2	5
Учасник 8	Middle	3	3 год. 7хв.	2	3, 5

Продовження таблиці 4.1

Учасник 9	Junior	4	6 год. 39 хв.	4	5
Учасник10	Junior	4	6 год. 14 хв.	5	5
Учасник 11	Junior	3	4 год. 12 хв.	1	3, 5
Учасник 12	Junior	3	2 год. 15 хв.	3	4, 5
Учасник 13	Junior	3	3 год. 46 хв.	2	4, 5
Учасник 14	Student	3	4 год. 10 хв.	7	4, 5
Учасник 15	Student	2	2 год. 16 хв.	4	3, 4, 5

Слід зазначити, що серед учасників, не було фахівців з хмарної безпеки, були спеціалісти різного рівня кваліфікації та навичок спеціалізації – Devops. З результатів проходження видно прямопропорційну залежність часу проходження раундів та кількість успішно завершених раундів від кваліфікації та досвіду роботи з задіяними технологіями. Середній час проходження 5 рівнів – 6 год. 53хв, 4 рівнів – 5 год. 33хв. 3 рівнів – 3 год. 44хв. Найбільш складним рівнем як і очікувався виявився 5 рівень його пройшли 33.33% респондентів. Четвертий рівень також виявився складним, та зайняв багато часу для його проходження, його пройшли 73.33%. Третій рівень пройшли 80% учасників, а 2 і 1 – 100%. Також було помічено, що підказки значно пришвидшують проходження рівнів та запобігають заходженню у глухий кут.

Також респондентами було перевірено відповідність заявлених до продукту вимог і реально реалізованої функціональності, який здійснюють шляхом спостереження за його роботою. Була помічена правильність відповіді для всіх можливих вхідних даних, виконання функцій за прийнятний час, практичність, сумісність із програмним забезпеченням та операційними системами, цікаво складені раунди та налагоджений процес.

ВИСНОВКИ

У ході виконання роботи були виявлені основні переваги та недоліки використання хмар, описано загальні принципи хмарних технологій та сервісів, аналіз чинників розвитку хмарних технологій, побудова на основі найкращих підходів та рекомендацій аспекту безпеки інфраструктури і даних в хмарі, а також визначено напрями реалізації цих питань.

Проведений аналіз існуючих можливостей та платформ для навчання створення безпечної інфраструктури у хмарах та визначено всі недоліки і переваги. В роботі підкреслено важливість безпеки даних та навчання співробітників компаній.

Результатом цього є створення своєї автоматизованої платформи для навчання та проходження перевірки знань студентів, security та devops інженерів.

В процесі роботи над кваліфікаційно роботою було опубліковано декілька тез. За темами: “Безпека використання хмарних провайдерів та способи її досягнення на прикладі використання Cloud Custodian”, “Аналіз та порівняння організації хмарної інфраструктури різних провайдерів”.

Були виконані основні етапи створення додатка: – нотифікації учасника (старт курсу, підписка на нотифікації, старт раунду, проходження, завершення курсу); – контроль проходження (старт проходження, та кінець, аналіз прогресу проходження користувача); – мультикористувацький режим – (можливість одночасного проходження сценаріїв користувачами, оптимізація ресурсів); – автоматизація розгортання курсу та інших процесів. Створено 5 раундів, яких студенти можуть проявити себе. Задіяно безліч ресурсів, та різні типи вразливостей інфраструктури. Був проведений іспит платформи на практиці. Учасниками було перевірено відповідність заявлених до продукту вимог і реально реалізованої функціональності, який здійснюють шляхом спостереження за його роботою. Визначена правильність відповіді для всіх можливих вхідних даних, виконання функцій за прийнятний час, практичність, сумісність із програмним забезпеченням та операційними системами, цікаво складені раунди та налагоджений процес

Таким чином всі вимоги технічного завдання виконано в повному обсязі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Порівняльний аналіз сервісів хмарних провайдерів в межахконцепції IaaS [Електронний документ] / Упорядник І. В. Абіх. – Харків: ХНУРЕ, 2020. – 67 с.

2. Comparing Cloud Providers: Amazon vs. Google vs. Microsoft [Електронний ресурс] – Режим доступу до ресурсу https://www.inovex.de/blog/comparing–cloud–providers/ – 20.05.2022 р. – Загл. з экрану.

3. Mell, Peter and Grance, Timothy The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST (20 October 2011).

4. Cloud Computing [Електронний ресурс] – Режим доступу до ресурсу https://sgs4business.com/news/khmarna-bezpeka-kliuchovi-poniattia-zahrozy-ta-rishennia.html/ – 18.05.2022 р. – Загл. з экрану.

5. Облачные вычисления [Електронний ресурс] – Режим доступу до ресурсуhttps://www.tadviser.ru/index.php/Статья:Облачные_вычисления_(Cloud_computing) – 18.05.2022 р. – Загл. з экрану.

6. Безопасность виртуальной инфраструктуры [Електронний ресурс] – Режим доступу до ресурсу https://security-news.today/bezopasnost-virtualnoj-oblachnoj-infrastruktury/–18.05.2022 р. – Загл. з экрану.

7. Що таке хмарні сервіси і чому вони так стрімко розвиваються [Електронний ресурс] – Режим доступу до ресурсу https://businessviews.com.ua/ru/tech/id/hmari– dlja– biznesu– 2003/ – 18.05.2022 р. – Загл. з экрану.

8. Cloud Computing [Електронний ресурс] – Режим доступу до ресурсу https://www.gartner.com/ – 20.05.2022 р.

9. Overview of Amazon Web Services [Електронний ресурс] – Режим доступу до ресурсу https://d1.awsstatic.com/whitepapers/aws–overview.pdf – 20.05.2022 р. – Загл. з экрану.

10. Amazon Web Services (AWS) [Електронний ресурс] – Режим доступу до ресурсу https://www.techtarget.com/searchaws/definition/Amazon-Web-Services 21.05.2022 р. – Загл. з экрану.

11. Amazon Web Services [Електронний ресурс] – Режим доступу до ресурсу https://en.wikipedia.org/wiki/Amazon_Web_Services 21.05.2022 р. – Загл. з экрану.

12. Google Cloud Platform [Електронний ресурс] – Режим доступу до ресурсу https://en.wikipedia.org/wiki/Google_Cloud_Platform 21.05.2022 р. – Загл. з экрану.

13.Microsoft Azure [Електронний ресурс] – Режим доступу до ресурсу https://ru.wikipedia.org/wiki/Microsoft_Azure 20.05.2022 р. – Загл. з экрану.

14.Future of Cloud Computing [Електронний ресурс] – Режим доступу до ресурсу https://www.cloudpanel.io/blog/future-of-cloud-computing/ 21.05.2022 р. – Загл. з экрану.

15.What Is The Future Of Cloud Computing 2025 [Електронний документ] – Режим доступу до ресурсу https://techjournal.org/the-future-of-cloud-computing-2025/– 5.05.2022 р. – Загл. з екрану

16.Terraform [Електронний документ] – Режим доступу до ресурсу https://www.terraform.io/ 5.05.2022 р. – Загл. з екрану

17.Cloud Security Alliance (CSA) [Електронний документ] – Режим доступу до ресурсу https://www.techtarget.com/searchsecurity/definition/Cloud-Security-Alliance-CSA 5.05.2022 р. – Загл. з екрану

18.Методичні вказівки з виконання атестаційної роботи бакалавра для студентів усіх форм навчання напряму 6.050903 «Телекомунікації» по кафедрі «Інформаційно– мережна інженерія» [Електронний документ] / Упоряд. А.І. Костромицький. – Харків: ХНУРЕ, 2017. – 37