Харківський національний університет ім. В. Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав. кафедрою БІСТ

проф. Сватовський І. І._____

« » червня 2023р.

Пояснювальна записка

До кваліфікаційної роботи бакалавра

Спеціальність: 125 Кібербезпека

на тему: «Аналіз та дослідження вимог до кіберзахисту при використанні хмарних обчислень»

оцінка « » Керівник к.т.н. Єсіна М. В.
(прізвище та ініціали/підпис)

Голова ЕК Рецензент к.т.н. Бобух В. А.
(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець студентка групи КБ-42

Новосьолова С. С.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка до дипломної роботи включає в себе 60 сторінок, 6 рисунків, 2 таблиці, 1 додаток, який займає 2 сторінки, та 21 джерело за переліком посилань.

Об’єктом дослідження виступають технології та методи забезпечення безпеки інформаційних ресурсів у хмарних сервісах для зберігання та обробки даних.

Предметом дослідження виступають вимоги до кіберзахисту при використанні хмарних обчислень.

Мета дипломної роботи полягає в аналізі та дослідженні хмар і хмарних обчислень, забезпеченні реалізації моделі загроз і вимог до кіберзахисту, порушника і безпеки при використанні хмар та хмарних обчислень.

Методи дослідження даної роботи це методи математичного моделювання, методи прикладної криптології, методи порівняльного аналізу та експертного оцінювання.

Ця робота важлива для розуміння проблем безпеки в хмарних обчисленнях та вироблення рекомендацій щодо забезпечення безпеки інформаційних ресурсів в цьому контексті. Дослідження може бути важливим для організацій та окремих спеціалістів, які займаються розробкою та впровадженням хмарних рішень з урахуванням аспектів кіберзахисту.

Ключові слова: ХМАРА, ВИМОГИ ДО КІБЕРЗАХИСТУ, МОДЕЛЬ РОЗГОРТАННЯ ХМАРИ, СТАНДАРТИ БЕЗПЕКИ, ХМАРНІ ОБЧИСЛЕННЯ, ЦІЛІ КІБЕРЗАХИСТУ.

ABSTRACT

The explanatory note to the thesis includes 60 pages, 6 figures, 2 tables, 1 appendix that occupies 2 pages, and 21 sources for the list of references.

The object of research are technologies and methods of ensuring the security of information resources in cloud services for data storage and processing.

The subject of the study is the requirements for cyber protection when using cloud computing.

The purpose of the thesis is performed in the analysis and research of clouds and cloud computing, ensuring the implementation of the threat model and requirements for cyber protection, security and safety when using clouds and cloud computing.

The methods of research of this work are methods of mathematical modelling, methods of applied cryptology, methods of comparative analysis and expert evaluation.

This work is important for understanding security issues in cloud computing and developing recommendations for securing information resources in this context. Research can be the addresses of organizations and individual specialists used in the development and implementation of cloud solutions, taking into account the aspects of cyber security.

Keywords: CLOUD, CYBER DEFENSE REQUIREMENTS, CLOUD DEPLOYMENT MODEL, SECURITY STANDARDS, CLOUD COMPUTING, CYBER DEFENSE GOALS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

НСД – Несанкціонований доступ
ВМ – Віртуальна машина
ІБ – Інформаційна безпека
ІТ – Інформаційні технології
ІТС – Інформаційно-телекомунікаційна система
СУІБ – Система управління безпекою
AWS – Amazon Web Services
BPaaS – Business-Process-as-a-Service
CIS – Center for Internet Security
CMS – Content Management System
CSP – Content Security Policy
FaaS – Function-as-a-Service
GDPR – General Data Protection Regulation
IaaS – Infrastructure-as-a-Service
IAM – Identity and Access Management
IBM – International Business Machines
IEC – International Electrotechnical Commission
ISMS – information security management system
ISO – International Organization for Standardization
NIST – National Institute of Standards and Technology
PaaS – Platform-as-a-Service
PCI DSS – Payment Card Industry Data Security Standard
SaaS – Software-as-a-Service
SECaaS – Security-as-a-Service
SLA – Service-level agreement
SP – Special Publication

ВСТУП

В сучасному світі хмарні обчислення являють собою одну з найбільш перспективних технологій, що використовуються в різних галузях бізнесу та науки. Зростаюча популярність хмарних сервісів призвела до того, що кількість даних, що підлягають обробці та збереженню в хмарі, постійно збільшується. Одночасно з цим, збільшується й загроза злочинним діянням в хмарному середовищі, яка може викликати втрату даних або порушення їх цілісності, конфіденційності та доступності.

Ця кваліфікаційна робота присвячена аналізу та дослідженню вимог до кіберзахисту при використанні хмарних обчислень. У цьому контексті проведено оцінку сьогочасного стану проблеми заснованого на аналізі науково-технічної літератури та патентного пошуку. В роботі зазначено, які задачі вже вирішені практично, а також, які існують недостатності знань у названій предметній області. Досліджено діяльність провідних організацій і фахівців у цій галузі, а також світові тенденції вирішення поставлених задач.

Мета роботи – це дослідження вимог до кіберзахисту при використанні хмарних послуг та розроблення рекомендацій стосовно підвищення рівня кібербезпеки в цьому середовищі. Результати цього дослідження можуть застосовуватись в галузі розробки та експлуатації хмарних сервісів, а також у сферах інформаційної безпеки й кіберзахисту. Хмарні обчислення зарекомендували себе як ефективний і економічний спосіб забезпечення інформаційних потреб бізнесу та користувачів. Проте, при користуванні хмарними технологіями, постає задача забезпечення безпеки в хмарному середовищі. Це викликає необхідність ретельного аналізу та дослідження вимог до кіберзахисту при використанні хмарних обчислень.

Результати дослідження будуть корисними для організацій, які користуються хмарними технологіями для збереження та обробки даних, а також для фахівців з кібербезпеки, котрі займаються захистом цих даних.

1 ОГЛЯД, АНАЛІЗ ТА ДОСВІД ВИКОРИСТАННЯ ХМАР ТА ХМАРНИХ ОБЧИСЛЕНЬ

1.1 Загальна концепція хмарних обчислень

Хмарна інфраструктура або хмара – являє собою набір динамічно розподілених та налаштованих хмарних ресурсів, що можуть оперативно надаватись користувачеві хмарних сервісів і вивільнятись через локальні та глобальну мережі передачі інформації.

Технологія хмарних обчислень – це технологія, яка забезпечує віддалений доступ до хмарної інфраструктури за запитом користувача через електронну комунікаційну мережу.

Хмарна послуга – представляє собою застосування технологій хмарних обчислень для надання хмарних ресурсів.

Користувач хмарних послуг – це фізичні та (або) юридичні особи, які, для задоволення особистих потреб, користуються хмарними сервісами.

Надавач хмарних послуг – фізична особа-підприємець або юридична особа, що надає одну або кілька хмарних послуг незалежно або об’єднавшись з іншими постачальниками хмарних послуг [1].

Основні моделі надання послуг в хмарних сервісах та їх характеристики:

- Інфраструктура як послуга (Infrastructure-as-a-Service (IaaS)) – хмарна послуга, яка, використовуючи хмарні обчислення, забезпечує надання користувачу хмарних послуг ресурсів зберігання, обчислювальних ресурсів чи систем електронних комунікацій. До прикладів IaaS належать: GigaCloud, Microsoft Azure, IBM Softlayer, Amazon EC2, Hetzener Cloud.
- Платформа як послуга (Platform-as-a-Service (PaaS)) – це хмарний сервіс, який за допомогою хмарних обчислень, надає користувачеві хмарних сервісів доступ до інфраструктури та комп’ютерних застосунків, таких як: операційні системи, системні комп’ютерні програми, програмні засоби управління базами даних і для комп’ютерного програмування. Приклади

сервісів PaaS: VMWare Cloud Foundry, Microsoft Azure, IBM Bluemix, Google App Engine.

- Програмне забезпечення як послуга (Software-as-a-Service (SaaS)) – ще одна модель надання послуг, яка являє собою надання користувачам хмарних сервісів доступ до прикладних комп'ютерних програм за допомогою комп'ютерних програм-агентів чи онлайн-сервісів, використовуючи технологію хмарних обчислень. Сервіси SaaS: Google Doc, Dropbox, Microsoft Office 365. [2].
- Безпека як послуга (Security-as-a-Service (SECaaS)) – послуги кіберзахисту, що надаються користувачеві хмарних сервісів за допомогою хмарних ресурсів.

Доступні й інші моделі обслуговування (часто більш спеціалізовані). До них належать такі послуги, як Business-Process-as-a-Service (BPaaS), у якому весь горизонтальний чи вертикальний бізнес-процес надається разом як комбінація пов'язаних служб IaaS, PaaS і SaaS. До більш спеціалізованих послуг також можна додати Function-as-a-Service (FaaS) – це підмножина SaaS, у якій код програми виконується лише у відповідь на певні події чи запити. Однак переважна більшість цих пропозицій є підтипами або розширеннями основних моделей послуг хмарних обчислень.

На рисунку 1.1 подано концептуальну модель хмарного сервісу.

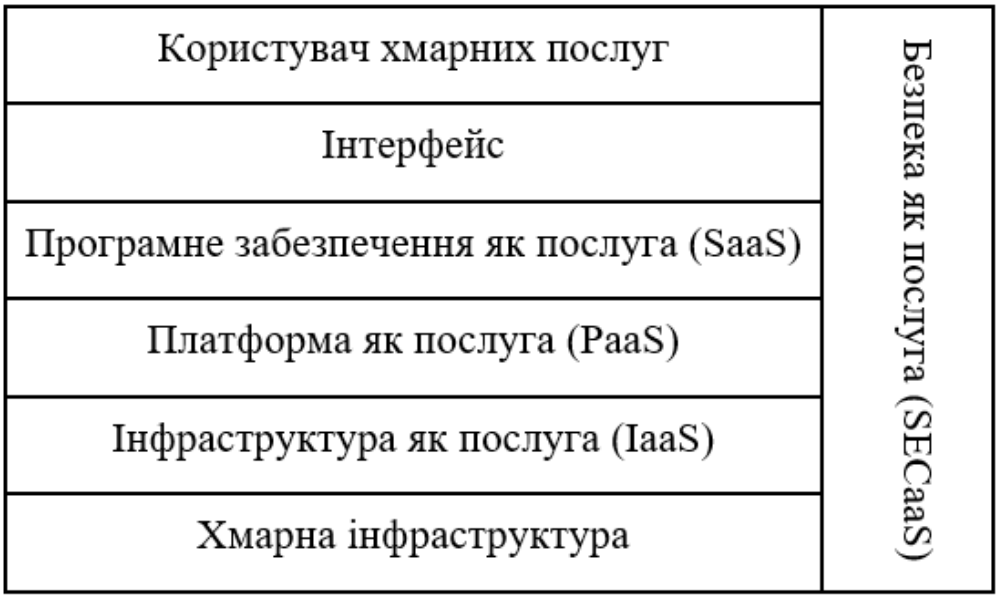

Рисунок 1.1 – Концептуальна модель хмарного сервісу

Використання хмарних технологій допомагає уникнути необхідності локальної наявності інших застосунків та сервісів, а також ресурсів для обробки та зберігання інформації. Основні послуги провайдерів хмарних сервісів надаються виділенням дискового простору, за допомогою технології мережевого доступу обчислювальних потужностей, а також – використанням різних сервісів. Такий підхід до надання послуг надає безліч переваг, оскільки раціоналізує використання ресурсів користувачами, оскільки не потребують купівлі, утримання та захисту власних серверів, забезпечення необхідної обчислювальної потужності, розгортання та підтримки комп'ютерної інфраструктури, а також локальної наявності та підтримки програм та інших сервісів. Тож, користувач платить лише за ресурси, якими користується, а саме – за ресурси, які орендує в провайдерів для виконання певної задачі. В такому випадку надавач послуг забезпечує постійну доступність інформації та ресурсів і можливість гнучкого масштабування [3].

1.2 Переваги хмарних обчислень

До переваг хмарних обчислень для користувачів можна віднести наступні показники:

1) Ефективність використання ресурсів. При використанні хмарних сервісів, користувач не витрачає кошти на покупку, налаштування та підтримку власного обладнання, забезпечення захищеності ресурсів та необхідної інфраструктури.

2) Гнучкість та масштабованість. Хмарні обчислення дають користувачам можливість збільшувати чи зменшувати ресурси в залежності від їхніх вимог.

3) Доступність. Користувачі можуть з легкістю отримувати доступ до обчислювальних ресурсів з будь-якої куточку планети, в якому є підключення до Інтернету.

4) Безпека. Провайдери хмарних сервісів забезпечують високий рівень захищеності даних і систем забезпечення відновлення після відмов.

З точки зору надавачів хмарних послуг, існують такі переваги:

1) Економічні переваги. Провайдери можуть знизити витрати на IT-інфраструктуру, а також забезпечити більш ефективне використання обчислювальних ресурсів.

2) Гнучкість та масштабованість. Надавачі можуть легко збільшувати чи зменшувати потужність та зберігання даних в залежності від змін потреб клієнтів.

3) Покращення доступності та надійності. Надавачі можуть забезпечити надійність своїх послуг та зменшити час відновлення після відмов.

4) Безпека. Надавачі можуть забезпечити високий рівень безпеки систем забезпечення відновлення після відмов і даних [4].

1.3 Недоліки хмарних обчислень

Крім позитивних аспектів, застосування хмарних обчислень має слабкі місця.

З недоліків застосування хмарних обчислень користувачами виділяють:

1) Залежність від Інтернет-з’єднання. Для доступу до хмарних послуг користувачам необхідне постійне та стабільне Інтернет-з’єднання. Відсутність доступу до Інтернету або його нестабільність можуть стати перешкодою у роботі з хмарними додатками та послугами.

2) Проблеми з безпекою. Хмарні обчислення містять потенційні ризики безпеки, такі як злом та крадіжка даних. Користувачі можуть не мати повного контролю над своїми даними, які знаходяться в хмарі, а це може викликати ризик витоку конфіденційної інформації.

3) Проблеми з надійністю. Відмова обладнання та системи хмарних послуг призводить до недоступності послуг та даних користувачів. Хоча більшість провайдерів хмарних послуг намагаються забезпечити надійність та стійкість системи, але все ж можуть виникати проблеми, які призведуть до тимчасової недоступності послуг.

4) Проблеми із сумісністю. Деякі хмарні додатки можуть бути несумісними з певними операційними системами або пристроями, що призводить до проблем при роботі з ними.

Щодо надавачів послуг, то для них присутні такі недоліки хмарних сервісів:

1) Високі витрати на інфраструктуру та обладнання. Надавачі хмарних послуг мають багато інвестувати в програмне забезпечення, інфраструктуру та обладнання, щоб забезпечити стабільну та безперебійну роботу хмарних сервісів.

2) Конкуренція. З огляду на високий попит хмарних обчислень серед користувачів, конкуренція на ринку хмарних послуг дуже висока. Це спонукає провайдерів надавати більш функціональні можливості, в тому числі –

вдосконалені системи захисту, за меншої вартості для щоб охопити більшу частку ринку.

3) Проблеми з безпекою. Хмарні послуги можуть стати об’єктом хакерських атак, що може викликати витік конфіденційної інформації клієнтів. Провайдери хмарних послуг повинні забезпечити належний рівень безпеки даних користувачів.

4) Проблеми з юридичними питаннями. Надавачі хмарних сервісів мають дотримуватися юридичних норм та стандартів тих країн, в яких надаються їхні послуги. Це вимагає від провайдерів хмарних послуг значних зусиль та ресурсів.

5) Залежність від інтернет-з'єднання. Надавачі хмарних послуг повинні створити стійку мережеву інфраструктуру для забезпечення доступності послуг та уникнення їх неефективності в умовах обмеженої пропускної здатності.

6) Ризики безпеки. Надавачі хмарних послуг повинні використовувати механізми захисту даних (шифрування, автентифікації та інші) для гарантування безпеки важливих даних користувачів, які зберігаються та обробляться серверами провайдерів хмарних послуг, для уникнення крадіжки, злому або витоку цих даних.

7) Проблеми зі сумісністю. Різні хмарні платформи можуть мати різні стандарти і протоколи, що може спровокувати проблеми зі сумісністю між різними хмарними сервісами. Це може обмежити можливості користувачів і створити труднощі для інтеграції з іншими системами.

8) Вартість. Хмарні обчислення можуть коштувати більше, ніж локальне зберігання та обробка даних, за умови використання великої кількості ресурсів або зберігання великих обсягів даних. Надавачі хмарних послуг повинні забезпечувати прозорість у витратах і ефективне управління ресурсами для зниження витрат користувачів [4].

1.4 Моделі розгортання хмар

Для опису відносин між надавачем хмарних послуг та їх користувачем використовують моделі розгортання хмари. Згідно положень Національного інституту стандартів та технологій США (NIST) існує чотири моделі розгортання хмари, такі як: публічна, приватна, суспільна та гібридна.

1.4.1 Публічна модель розгортання хмари

Розвиток і впровадження публічних хмарних сервісів є одним із найважливіших зрушень в історії корпоративних обчислень. Відкрита хмара – це тип хмарних обчислень, у якому сторонній постачальник послуг створює обчислювальні ресурси, які можуть включати будь-що. Це можуть бути готові до використання програмні додатки для окремих віртуальних машин, повна інфраструктура корпоративного рівня та платформи розробки, доступні користувачам за допомогою мережі Інтернет. Такі ресурси можуть бути доступними безкоштовно або доступ може продаватися відповідно до моделі ціноутворення на основі передплати чи плати за користування.

Постачальник публічної хмари володіє та адмініструє центрами обробки даних, в яких виконуються робочі навантаження клієнтів. Постачальники послуг беруть на себе відповідальність за обслуговування всього апаратного забезпечення та інфраструктури та забезпечують підключення до мережі з високою пропускною здатністю для забезпечення швидкого доступу до програм і даних. Хмарний постачальник також керує основним програмним забезпеченням віртуалізації.

Публічні хмарні архітектури – це середовища з кількома клієнтами, в яких користувачі спільно використовують набір віртуальних ресурсів, які автоматично надаються та розподіляються між окремими орендарями через інтерфейс самообслуговування. Виходячи з цього, робочі навантаження кількох орендарів можуть одночасно запускати екземпляри центрального процесору на спільному фізичному сервері. Однак дані кожного клієнта хмари логічно ізольовані від даних інших клієнтів.

На рисунку 1.2 наведено схему публічної моделі розгортання хмари.

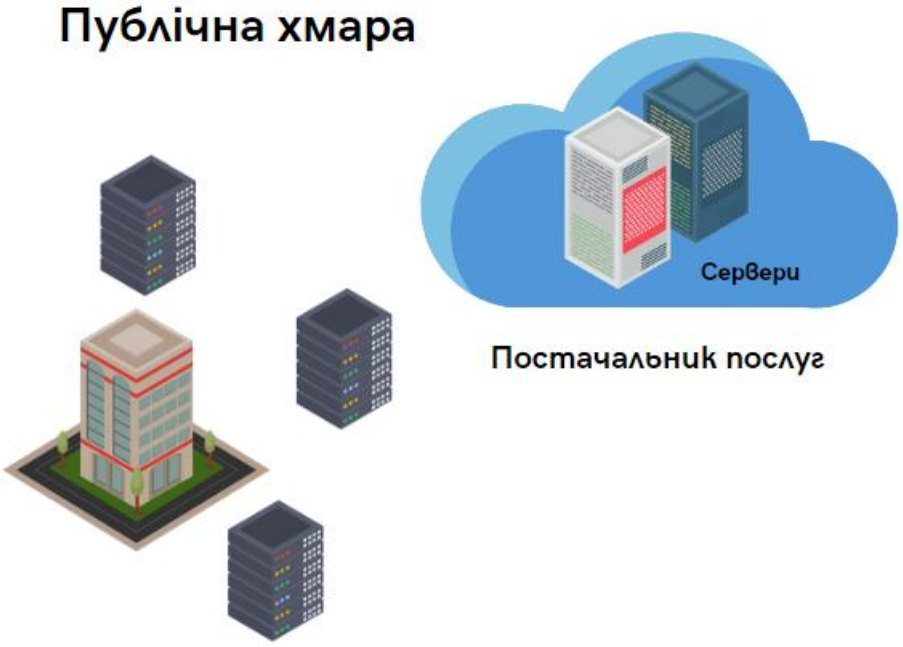

Рисунок 1.2 – Схема публічної моделі розгортання хмари

Багато підприємств переносять частини своєї обчислювальної інфраструктури в публічну хмару, оскільки відкриті хмарні сервіси є еластичними та легко масштабованими, швидко пристосовуючись до стабільно зростаючих вимог робочого навантаження. Також значною перевагою є надання більшої ефективності при меншій вартості і скорочення витрат на обладнання та локальну інфраструктуру. Це спричинило стрімке зростання ринку публічних хмарних обчислень, яке, з огляду на сучасні тенденції, триватиме і надалі.

Недоліки публічної хмари включають наступне:

- Менший спектр можливостей налаштування додатків та інфраструктури, у порівнянні з приватними хмарами.

- Гірший контроль і безпека, оскільки робочі навантаження виконуються за брандмауером орендаря, хоча загальна безпека залежить від власного середовища орендаря.

- Ускладнений алгоритм відповідності галузевим або державним нормам.

Публічна хмара зазвичай передбачає нижчі авансові та поточні витрати, ніж приватна хмара. Нові публічні хмарні пропозиції, такі як віртуальні приватні хмари, надають багато тих самих переваг, що й приватні хмарні обчислення, не накладаючи таких самих витрат або тягар управління [5].

1.4.2 Приватна модель розгортання хмари

Приватна хмара – це середовище хмарних обчислень, призначене для одного клієнта. Вона поєднує багато переваг хмарних обчислень із безпекою та контролем локальної IT-інфраструктури.

Приватна хмара (також відома як внутрішня хмара або корпоративна хмара) – це середовище хмарних обчислень, у якому всі апаратні та програмні ресурси призначені виключно для одного клієнта та доступні лише для нього. Приватна хмара поєднує багато переваг хмарних обчислень, включаючи еластичність, масштабованість і легкість надання послуг, із контролем доступу, безпекою та налаштуванням ресурсів локальної інфраструктури.

Багато компаній обирають приватну хмару замість публічної хмари (хмарні обчислювальні послуги, які надаються через інфраструктуру, спільну для кількох клієнтів), оскільки приватна хмара є простішим (або єдиним) способом задовольнити їхні нормативні вимоги. Інші обирають приватну хмару, тому що їхні робочі навантаження пов’язані з конфіденційними документами, інтелектуальною власністю, особистою інформацією, медичними документами, фінансовими даними чи іншими конфіденційними даними.

Створюючи архітектуру приватної хмари відповідно до принципів власної хмари, організація дає собі можливість легко переміщувати робочі навантаження в загальнодоступну хмару або запускати їх у середовищі гібридної хмари (змішаної приватної та публічної хмари).

Приватна хмара – це середовище з одним клієнтом, тобто всі ресурси доступні лише одному клієнту – це називається ізольованим доступом. Приватні хмари зазвичай розміщуються локально в центрі обробки даних клієнта. Але приватні хмари також можна розмістити в інфраструктурі

незалежного хмарного провайдера або побудувати на основі орендованої інфраструктури, розміщеної у зовнішньому центрі обробки даних. Моделі управління також відрізняються: клієнт може керувати всім самостійно або передати часткове чи повне управління постачальнику послуг.

На рисунку 1.3 наведено схему публічної моделі розгортання хмари.

Рисунок 1.3 – Схема приватної моделі розгортання хмари

Крім однокористувацької моделі, приватна хмара базується на технологіях, які дозволяють замовнику надавати та налаштовувати віртуальні сервери та обчислювальні ресурси на вимогу для швидкого та легкого (або навіть автоматичного) масштабування у відповідь на сплески у використанні та трафіку. Це допомагає реалізації резервування для забезпечення високої доступності та оптимізації використання ресурсів у цілому.

Ці технології включають наступне:

- Віртуалізація, яка дає змогу абстрагувати IT-ресурси від базового фізичного обладнання та об’єднати їх у необмежені групи ресурсів обчислення, сховища, пам’яті та мережевої ємності, які потім можна розподілити між кількома віртуальними машинами (ВМ), контейнерами чи іншими віртуалізованими елементами IT-інфраструктури. Усуваючи

обмеження фізичного обладнання, віртуалізація забезпечує максимальне використання обладнання, дозволяє ефективно його використовувати для кількох користувачів і програм, а також робить можливими масштабованість, гнучкість і еластичність хмарних сервісів.

- Програмне забезпечення для керування надає адміністраторам централізований контроль над інфраструктурою та запущеними на ній додатками. Це дає змогу оптимізувати безпеку, доступність і використання ресурсів у середовищі приватної хмари.

- Автоматизація пришвидшує завдання, такі як ініціалізація сервера та інтеграція, які в іншому випадку потрібно було б виконувати вручну та неодноразово. Автоматизація зменшує потребу в людському втручанні, роблячи можливим самообслуговування ресурсів.

Крім того, користувачі приватної хмари можуть прийняти власну архітектуру хмарних додатків і практики, такі як контейнери та мікросервіси, що може забезпечити ще більшу ефективність і гнучкість і забезпечити плавний перехід до публічної хмари або гібридного хмарного середовища в майбутньому.

Переваги приватної хмари:

Використання приватної хмари дає змогу всім підприємствам, навіть тим, які працюють у суворо регульованих галузях, скористатися багатьма перевагами хмарних обчислень без шкоди для безпеки, контролю та налаштування. Конкретні переваги приватної хмари включають наступне:

- Повний контроль над вибором обладнання та програмного забезпечення. Клієнти приватної хмари можуть вільно купувати апаратне та програмне забезпечення, що їм подобається, а не лише програмне та апаратне забезпечення, котре пропонує постачальник хмарних технологій.

- Свобода будь-яким чином налаштовувати обладнання та програмне забезпечення. Клієнти приватної хмари можуть налаштовувати сервери будь-яким способом, а також можуть налаштовувати програмне забезпечення за потреби за допомогою доповнень або за допомогою спеціальної розробки.

- Краща видимість безпеки та контролю доступу, адже всі робочі навантаження виконуються за власним брандмауером клієнтів.

- Повне дотримання нормативних стандартів. Клієнти приватної хмари не змушені покладатися на галузеву та нормативну відповідність, яку пропонує постачальник хмарних послуг.

Недоліки приватної хмари:

Головним недоліком приватної хмари є вища вартість, яка може включати витрати на придбання та встановлення нового обладнання і програмного забезпечення та витрати на керування ним (що може включати наймання додаткового IT-персоналу). Іншим недоліком є дещо обмежена гнучкість – коли організація інвестує в апаратне та програмне забезпечення для своєї приватної хмари, збільшення ємності або нових можливостей потребує додаткових закупівель. Віртуальна приватна хмара та керовані хмарні служби можуть певною мірою зменшити ці недоліки [6].

1.4.3 Суспільна модель розгортання хмари

Суспільна хмара – це хмарна інфраструктура, у якій кілька організацій спільно використовують ресурси та послуги на основі спільних операційних і нормативних вимог. Ця система є модифікованою формою приватної хмари, де потреби різних організацій і вертикалей зважуються під час розробки ідеї архітектури. Громадська хмара належить, керується та експлуатується членами спільноти, сторонніми постачальниками або обома одразу. Вона може розміщуватися в центрі обробки даних, що належить одному з орендарів, або сторонньому постачальнику хмарних послуг.

Переваги суспільної хмари:

- Відкритість і неупередженість. Громадські хмари є відкритими системами, і вони усувають залежність організацій від постачальників хмарних послуг. Організації можуть отримати багато переваг, уникаючи недоліків як публічних, так і приватних хмар.

- Гнучкість і масштабованість. Гнучкість громадської хмари забезпечується підтримкою сумісності між усіма користувачами, дозволяючи

їм змінювати властивості відповідно до індивідуальних випадків використання, можливістю компаній взаємодіяти зі своїми віддаленими співробітниками та підтримкою використання різних пристроїв. Масштабованість в різних аспектах (як апаратні ресурси, послуги, робоча сила) забезпечується наявністю спільноти. Враховується зростання попиту, а надавачу послуг необхідно лише збільшити базу користувачів.

- Висока доступність і надійність. Громадські хмари забезпечують захист інформації шляхом копіювання даних і програм у кількох безпечних місцях. Хмара має надлишкову інфраструктуру, щоб забезпечити доступність даних у будь-який час і в будь-якому місці. Висока доступність і надійність є критично важливими для будь-якого типу хмарного рішення.

- Безпека та відповідність вимогам регуляторних органів. Для уникнення порушення безпеки даних інших користувачів хмари, можливе налаштування різних рівнів безпеки для різних даних. Наприклад, є можливість заборонити користувачам редагувати та завантажувати певні набори даних.

- Зручність і контроль. Всі орендарі володіють інфраструктурою та приймають рішення спільно, тобто, присутня демократична модель поведінки користувачів, що сприяє уникненню конфліктів, пов’язаних зі зручністю та контролем.

Екологічна стійкість. У громадській хмарі організації використовують єдину платформу для всіх своїх потреб, що обмежує їх інвестування в окремі хмарні об’єкти. Це запроваджує симбіотичні відносини між розширенням і скороченням використання хмари серед клієнтів. Зі зменшенням організацій, які використовують різні хмари, ресурси використовуються ефективніше, що призводить до меншого вуглецевого сліду [7].

На рисунку 1.4 наведено архітектуру суспільної моделі розгортання хмари.

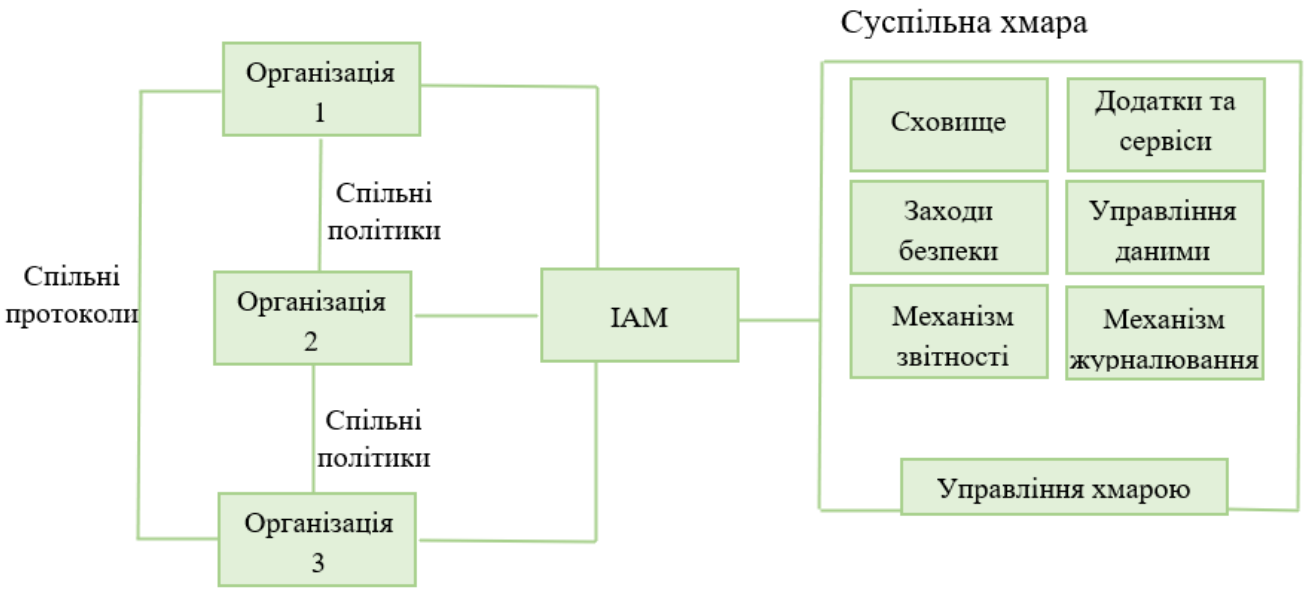

Рисунок 1.4 – Архітектура суспільної моделі розгортання хмари

1.4.4 Гібридна модель розгортання хмари

Гібридна хмара – це змішане обчислювальне середовище, у якому додатки запускаються з використанням обчислень, сховищ і служб у різних середовищах – загальнодоступних хмарах і приватних хмарах, включаючи локальні центри обробки даних або «граничні» розташування.

Гібридні хмарні рішення дозволяють переміщувати та керувати робочими навантаженнями між різними хмарними середовищами, дозволяючи створювати більш універсальні налаштування на основі конкретних бізнес-потреб. Багато організацій обирають гібридні хмарні платформи, щоб зменшити витрати, мінімізувати ризики та розширити наявні можливості для підтримки зусиль з цифрової трансформації.

Хмарна міграція часто природно призводить до реалізації гібридної хмари, оскільки організаціям часто доводиться повільно та систематично переносити додатки та дані. Гібридні хмарні середовища дозволяють продовжувати використовувати локальні служби, використовуючи переваги гнучких параметрів зберігання та доступу до даних і програм, які пропонують постачальники публічних хмар.

Подібно до інших архітектур хмарних обчислень, гібридні хмарні платформи використовують віртуалізацію, контейнеризацію та програмно визначені мережеві технології та технології зберігання для абстрагування та агрегування ресурсів. Спеціалізоване програмне забезпечення для керування дозволяє організаціям розподіляти ресурси та надавати на вимогу різні середовища.

Переваги гібридної хмари:

- Ефективне управління додатками. Гібридний підхід дозволяє вирішувати, де розміщуватиметься програма та де відбуватимуться гібридні обчислення, що може допомогти покращити конфіденційність і забезпечити відповідність регульованих програм.
- Покращена продуктивність і зменшена затримка. Іноді розподілені програми у віддалених місцях отримують переваги від гібридного хмарного рішення. Для додатків із низькими вимогами до затримки гібридні обчислення використовуються поблизу кінцевих користувачів.
- Гнучкі операції. Гібридні обчислення дають вам гнучкість для роботи в середовищі, яке найкраще підходить для вас. Наприклад, використовуючи контейнери, користувач може створювати портативні програми та легко переміщатися між приватною та публічною хмарами.
- Покращена рентабельність інвестицій. Додавши загальнодоступного хмарного постачальника до існуючої локальної інфраструктури, ви зможете розширити потужність хмарних обчислень, не збільшуючи витрати на центр обробки даних.
- Покращена продуктивність і зменшена затримка. Іноді розподілені програми у віддалених місцях отримують переваги від гібридного хмарного рішення. Для програм із низькими вимогами до затримки гібридні обчислення можуть бути ближчими до кінцевих користувачів.
- Швидші інновації. Гібридні хмарні моделі надають доступ до найновіших технологій, таких як штучний інтелект та машинне навчання, без необхідності розширювати або замінювати існуючу інфраструктуру.

Надається можливість максимізувати ресурси та підвищити продуктивність, щоб пришвидшити розробку та доставку програм [8].

На рисунку 1.5 подано схему розгортання гібридної моделі розгортання хмари.

Рисунок 1.5 – Гібридна модель розгортання хмари

2 МОДЕЛІ ЗАГРОЗ, ПОРУШНИКА ТА БЕЗПЕКИ ХМАР ТА ХМАРНИХ ОБЧИСЛЕНЬ

Загроза – сукупність факторів і умов, що можуть являти собою причину порушення цілісності, доступності та конфіденційності інформації в системі.

Ризик порушення безпеки – можливість реалізації загрози.

Вразливість – слабкість системи захисту, яка робить можливою реалізацію загрози.

Система управління ІБ – комплекс заходів, що спрямовані на забезпечення режиму інформаційної безпеки на всіх стадіях життєвого циклу інформаційної системи.

Оцінка ризиків – ідентифікація ризиків, вибір параметрів для їх опису (кількісних якісних та інших), й та отримання оцінок за цими параметрами.

Аналіз ризиків – це процес визначення вразливостей, загроз і можливого збитку безпеки корпоративної інформаційної системи. Мета аналізу ризиків полягає в тому, щоб виявити існуючі ризики і оцінити їх величину (дати їм кількісну оцінку). Ризик визначається ймовірністю заподіяння шкоди і величиною збитку, що наноситься ресурсам ІТС, в разі створення загрози безпеці. Аналіз ризиків включає в себе заходи по обстеженню безпеки ІТС, метою якого є визначення того, які ресурси і від яких загроз потрібно захищати, а також в якій мірі ті чи інші ресурси потребують захисту [9].

Важливою складовою управління ризиками безпеки є наявність моделі загроз та моделі порушника, які дозволяють сформувати перелік вимог до систем захисту інформації в середовищі хмарних обчислень.

2.1 Розподіл відповідальності

Відповідно до моделі обслуговування в хмарних сервісах існують різні рівні розподілу відповідальності.

На рисунку 2.1 подано розподіл відповідальності між користувачем та надавачем хмарних послуг при локальному забезпеченні обчислювальних ресурсів та трьох основних моделей обслуговування при використанні хмарних сервісів.

Локально	IaaS	PaaS	SaaS
Додатки	Додатки	Додатки	Додатки
Дані	Дані	Дані	Дані
Середовище виконання	Середовище виконання	Середовище виконання	Середовище виконання
Проміжне програмне забезпечення	Проміжне програмне забезпечення	Проміжне програмне забезпечення	Проміжне програмне забезпечення
Операційна система	Операційна система	Операційна система	Операційна система
Віртуалізація	Віртуалізація	Віртуалізація	Віртуалізація
Сервери	Сервери	Сервери	Сервери
Сховище	Сховище	Сховище	Сховище
Мережа	Мережа	Мережа	Мережа

– Керує користувач – Керує провайдер

Рисунок 2.1 – Розподіл відповідальності в різних моделях обслуговування

У відповідності до різних моделей обслуговування в хмарах користувачі та провайдери послуг мають різні рівні витрат і права власності (табл. 1.1).

Таблиця 1.1 – Витрати та право власності

Критерії	IaaS	PaaS	SaaS
Попередні витрати	Попередніх витрат немає. Користувачі платять лише за те, чим користуються.		Користувачі платять передплату, зазвичай за місяць або рік користування.
Права власності користувача	Користувач несе відповідальність за придбання, установку, конфігурацію та керування власним програмним забезпеченням, операційною системою, проміжним програмним забезпеченням і програмами.	Користувач несе відповідальність за розробку власних програм. Однак вони не несуть відповідальності за керування сервером чи інфраструктурою. Це дозволяє користувачеві зосередитись на програмі або робочому навантаженні, яке він запускає.	Користувачі просто використовують програмне забезпечення і не несуть відповідальності за будь-яке обслуговування чи керування цим програмним забезпеченням.

Продовження таблиці 1.1

Критерії	IaaS	PaaS	SaaS
Права власності провайдера послуг	Постачальник хмарних послуг відповідає за те, щоб базова хмарна інфраструктура (ВМ, сховище, мережа) була доступна для користувача.	Провайдер відповідає за керування операційною системою, конфігурацію мережі та послуг. Він несе відповідальність за все, окрім програми, яку запускає користувач. Постачальник забезпечує повну керовану платформу, на якій можна запускати програми.	Постачальник хмарних сервісів несе відповідальність за надання, керування та обслуговування прикладного програмного забезпечення.

2.2 Модель загроз хмар та хмарних обчислень

Моделювання загроз – це структурований підхід до ідентифікації та визначення пріоритетів потенційних загроз для системи, а також визначення цінності потенційних засобів пом’якшення для зменшення або нейтралізації цих загроз. Загрози можуть призвести до пошкодження фізичних активів, очевидних фінансових витрат та непрямих витрат.

При створенні моделі загроз необхідно задокументувати наступне:

- Шлях проходження системи даними, для визначення вразливих місць системи.
- Якнайбільшу кількість потенційних загроз для системи, для ефективної боротьби з ними.

- Засоби контролю безпеки документів, що застосовуються для зменшення ймовірності та вплив потенційних загроз.

Загрози можуть бути реалізовані шляхом використання:

- Технічних каналів (канали електромагнітного випромінювання, наводки; оптичні, віброакустичні, акустичні, акустоелектричні канали і т.д.).

- Несанкціонованого доступу (маскування в мережі під авторизованого користувача, під'єднання до ліній зв'язку чи апаратури, злам системи безпеки та інше).

- Каналів спеціального впливу (генерація сигналів для порушення цілісності інформації).

Найбільш ефективним є застосування орієнтованого на загрози підходу до кібербезпеки хмар. Одним із таких підходів являється STRIDE-LM.

STRIDE-LM – це модель загроз, яка використовується для класифікації цілей атак і застосовується на системному рівні. Назва цієї моделі загроз являє собою абревіатуру класифікацій загроз системам, а саме:

- Spoofing (спуфінг) – видання одного користувача чи компонента системи за іншого, для отримання його доступу до системи.

- Tampering (фальсифікація) – зміна системи або даних для зменшення їхньої корисності для певних користувачів.

- Repudiation (відмова) – правдоподібне заперечення дій, вжитих певним користувачем або процесом.

- Information Disclosure (витік інформації, порушення конфіденційності даних) – передача інформації неавторизованим сторонам.

- Denial of Service (відмова в обслуговуванні) – атака, яка робить систему недоступною для призначених користувачів.

- Elevation of Privilege (підвищення привілеїв) – надання користувачеві чи процесу додаткового доступу до системи без авторизації.

- Lateral Movement (латеральний рух) – розширення контролю над цільовою мережею за межі початкової точки компромісу.

Остання класифікація була додана для того, аби зробити модель більш адаптованою до використання для захисту мережі, а не для інженерних і розробних проектів. Хмарна інфраструктура і локальні обчислювальні мережі піддаються однаковим загрозам, модель загроз STRIDE-LM виявляє спільні для них загрози. Проте, такі характеристики як низька чи повна відсутність видимості операцій, відсутність контролю або нечіткі вимоги відповідності, створюють додаткові загрози при використанні хмарних обчислень [10].

Хмарна інфраструктура може створювати додаткові загрози, окрім STRIDE-LM, які необхідно враховувати будь-якій організації, зацікавленій у захисті своїх даних. Такі загрози включають:

- Зменшення конфіденційності споживачів.
- Атаки на медичні пристрої.
- Несанкціоноване використання ресурсів (наприклад, часу процесора) для виконання неавторизованих завдань.
- Зламані віртуальні машини/пристрої, які використовуються для запуску атак грубою силою на інші машини, створення спаму або сканування відкритих портів та інших пристроїв в Інтернеті.
- Проблеми з публічною інфраструктурою, що призводять до фізичного вторгнення в центр обробки даних, де розміщені властивості/об’єкти, що призводить до крадіжки незашифрованих даних клієнтів.
- Прив’язаність до постачальника послуг і портативність даних/послуг.
- Неавторизовані зміни конфігурації платежів.
- Потенційні вразливості (наприклад, помилки) у коді та ресурсах CSP, які можуть призвести до зловмисної зміни або розкриття даних клієнта.
- Потенційні недоліки безпеки віртуалізації (неналежне впровадження методів ізоляції, що призводить до атак між пристроями та між клієнтами).

- Належне та своєчасне встановлення виправлень ОС хоста, програмних бібліотек (наприклад, OpenSSL), середовищ (наприклад, Java, Apache) або програм, що використовуються в хмарному середовищі.

- Програми-вимагачі, хактивізм, атаки національних держав на пристрої критичної інфраструктури.

2.3 Модель порушника хмар та хмарних обчислень

Порушник безпеки – особа або група осіб, що здатна реалізувати певну загрозу системи. Абстрактний перелік дій порушника, що описує теоретичні і практичні можливості та знання злочинця, час та місце його дії і т. д., називається моделлю порушника.

При розробці моделі порушника безпеки варто брати до уваги наступне:

- Модель розгортання хмари;
- Власника інформації;
- Рівень контролю інформації;
- Модель надання послуг;
- Рівень контролю інфраструктури надавачем послуг та користувачем хмари.

При розробці моделі порушника необхідно враховувати хто і як мав би змогу використовувати активи компанії, в тому числі проти самої компанії. Необхідний рівень кваліфікації порушника може зростати з підвищенням складності реалізації загроз чи з необхідністю використання великої кількості ресурсів. Однак, з розвитком хмарних обчислень та поширенням програмного забезпечення для атак в Інтернеті, більшість загроз можуть легко реалізовуватись за допомогою відносно невеликих навичок і ресурсів.

Основною метою порушника безпеки може бути:

- Авторизація та заволодіння вищими правами доступу до захищених даних з подальшим володінням ними, фальсифікацією та/або видаленням, а також експлуатація обчислювальних потужностей для задоволення власних цілей.

- Нанесення матеріальних збитків шляхом вторгнення до технічних приміщень провайдерів хмарних сервісів та пошкодження їх обладнання.

- Виведення з ладу ресурсів хмарних обчислень, зміна режиму експлуатації системи.

- Генерування хибних повідомлень, зчитування сигналів з використанням фізичних засобів, наприклад, апаратних закладок.

- Зняття інформації, її модифікація з використанням програмних засобів, за допомогою генерування шкідливого програмного забезпечення, вірусів, фальсифікованих повідомлень та сигналів, для надмірного навантаження ресурсів системи і втрати їх доступності.

- Реалізація несанкціонованого доступу до обчислювальних та інформаційних ресурсів ІТС, програмного забезпечення системи, за допомогою зламу системи управління доступом.

Згідно з моделлю хмари NIST, виділяють дві категорії порушників: внутрішні (персонал або користувачі хмари, які становлять особливу загрозу) та зовнішні (інші особи). Щоб визначити зовнішніх порушників безпеки необхідно визначити всі наявні вразливості системи і канали витоку інформації. Для того, щоб встановити модель внутрішнього порушника, необхідно виявити всі можливі шляхи отримання несанкціонованого доступу до ресурсів хмари сторонніми особами, користувачами та провайдерами хмарних послуг, враховуючи при цьому реалізовану систему обмеження їх доступу.

Ці категорії порушників безпеки поділяються згідно рівню їх можливості ще на чотири підкатегорії:

- І рівень – передбачає наявність можливості запуску статичного набору програм, що втілюють заздалегідь визначені функції обробки інформації.

- ІІ рівень – забезпечується можливість розробки та виконання власних програм з додатковими функціями обробки даних.

- III рівень – надається можливість керування функціонуванням ІТС хмарної інфраструктури, що означає здатність впливати на ключове програмне забезпечення системи та конфігурацію її обладнання.

- IV рівень – визначається повним спектром дозволів для осіб, які проектують, реалізують і обслуговують апаратне устаткування ІТС хмарного середовища, з урахуванням можливості включення власних засобів з розширеними функціями обробки інформації в ІТС хмари.

Крім цього, порушників можна поділяти за рівнем обізнаності в системі:

- Звичайні користувачі хмар, які не мають компетенції в галузі програмування та обчислювальної техніки, експлуатації та проектування хмарних сервісів.

- Особи, що мають базовий чи високий рівень обізнаності в сфері програмування та обчислювальної техніки, використання та проектування хмарних сервісів, крім того мають високий рівень знань щодо систем захисту хмарної інфраструктури.

- Порушники, які мають навички користування типовими засобами та знають про характеристики функціонування інфраструктури хмари, головні особливості утворення масивів даних та потоків запитів до них.

- Спеціалісти, котрі розуміються на функціях та механізмах дії системи безпеки в хмарній інфраструктурі.

- Кваліфіковані особи, що мають досвід експлуатації та обслуговування технічних засобів хмарної інфраструктури.

Найбільш небезпечними для хмарних сервісів порушниками являються адміністратори безпеки та адміністратори хмари. Зловмисні дії можуть бути як випадковими, так і навмисними. Загрози ресурсам системи в свою чергу можуть бути пасивними та активними. Активні загрози це випадкові та навмисні дії несанкціоновані дії зловмисника, що призводять до змін стану ІТС. Пасивні загрози це вчинки порушника безпеки, які викликають несанкціоноване проникнення до системи, що не змінюють її стан.

Характер дії порушника безпеки:

- Активні дії. В такому випадку дії порушника відкриті, використовуються усі наявні заходи й засоби для порушення конфіденційності інформації в системі, яка потребує захисту.

- Пасивні дії. Здійснюються авторизованими користувачами та/або обслуговуючим персоналом хмарного сервісу, котрі порушили політику безпеки системи не виконуючи активних дій.

- Випадкові дії. Ненавмисне пошкодження засобів управління доступом до вразливих ресурсів системи користувачами або обслуговуючим персоналом хмари, виконання ними непередбачених дій, що викликали загрозу захищеності цих ресурсів.

- Віддалені дії. Використовуються методи забезпечення зовнішнього доступу до ресурсів системи (наприклад, технічні канали витоку даних, мережеве устаткування розподілених або локальних мереж, тощо) [11].

3 ОГЛЯД ВИМОГ ДО КІБЕРЗАХИСТУ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ

3.1 Цілі кіберзахисту в хмарних сервісах

Впровадження хмарних обчислень включають такі основні цілі безпеки:

1) Запобігання несанкціонованому доступу до ресурсів інфраструктури хмарних обчислень. Це включає впровадження доменів безпеки, які мають логічне розділення між обчислювальними ресурсами, наприклад, логічне розділення робочих навантажень клієнтів, що виконуються на одному сервері, за допомогою моніторів віртуальних машин (гіпервізорів) у середовищі з кількома клієнтами та використання безпечних конфігурацій за замовчуванням.

2) Управління векторами загроз гіпервізора. Серед векторів загроз атаки гіпервізора є користувачі CSP і співробітники CSP. Уразливості гіпервізора включають погані конфігурації, пропущені або затримані виправлення безпеки або несанкціоновані дії привілейованого користувача. Оскільки використання гіпервізора може призвести до катастрофічних наслідків, CMS вимагає, щоб усі рішення гіпервізора мали бути продуктами типу 1 (нативні/голі метали). Слід застосовувати найкращі галузеві практики, якщо вони доступні, або слід використовувати власні опубліковані вказівки постачальника.

3) Мінімізація спільного доступу до мережі. Більшість CSP мають деякі спільні компоненти мережевої інфраструктури між різними хмарними клієнтами; ці компоненти спільної мережевої інфраструктури становлять значний ризик, оскільки одне порушення спільного компонента може поставити під загрозу всіх користувачів послуги CSP. Таким чином, конфігурації мають відповідати найкращим практикам, а винятки мають бути добре зрозумілі, задокументовані та прийняті користувачами служби CSP.

4) Управління доступом привілейованих користувачів. Привілейованих користувачів CSP з доступом до гіпервізора слід звести до мінімуму. Постачальники послуг повинні забезпечити своєчасне скасування доступу на основі події звільнення працівника Послуги або коли доступ більше не потрібен (наприклад, переміщення роботи). Цілями CSP для керування доступом привілейованих користувачів в обох випадках має бути скасування доступу в режимі реального часу, аудиторські записи мають бути доступні для аудиторів CMS, які встановлюють, коли було зроблено запит, і фактичне скасування привілеїв.

5) Необхідно також переконатись, що відповідні заходи безпеки розгорнуті на CSP. CMS має проводити незалежні оцінки, щоб переконатися, що належні запобіжні заходи діють. Це включає традиційні заходи безпеки периметра в поєднанні з додатковими засобами захисту, необхідними для хмарних обчислень.

Визначення кордонів довіри між CSP та споживачами CMS. Вкрай важливо чітко задокументувати відповідальність за забезпечення безпеки та чітко визначити наслідки нерозгортання узгоджених заходів безпеки CSP у контрактах і SLA [12].

3.2 Проблеми дотримання вимог кіберзахисту при використанні хмарних обчислень

Незважаючи на те, що хмарні технології дають організаціям швидкість і гнучкість, які необхідні для того, щоб залишатися попереду в діловому світі, що швидко змінюється, підтримувати відповідність стандартам безпеки складно. Нижче наведено деякі ключові проблеми дотримання вимог, з якими зазвичай стикаються користувачі хмари:

1) Видимість гібридних мереж. Дотримуватись стандартів важко організаціям, які керують гібридними мережами, через проблеми з видимістю. Гібридна мережа використовує більше ніж один тип технології підключення або топології. Управління низкою технологій ускладнює отримання видимості кожного компонента мережі. Виконання вимог відповідності вимагає

належного нагляду за мережевими компонентами. Це великий виклик для компаній, які працюють на гібридних хмарних технологіях. Відстеження гібридних середовищ займає багато часу та потребує розширених можливостей через складність цих нових хмарних рішень. Проблеми видимості усуваються шляхом інтегрування спеціальних рішень для керування безпекою в хмарі, щоб забезпечити повну видимість у гібридному та багатохмарному мережевому середовищі.

2) Багатохмарні робочі процеси. Більшість компаній використовують мультихмарні рішення. Постійне ускладнення технологій викликає ускладнення робочих процесів, що в свою чергу провокує ускладнення перевірки спеціалістами відповідності робочих процесів існуючим вимогам. Робота з кількома хмарними службами та наявність співробітників, які мають доступ до даних із різних пристроїв, дуже ускладнюють дотримання інформаційної безпеки та стандартів хмарного керування. Багатохмарна архітектура дає змогу розподіляти ролі в компанії для кращої гнучкості та оперативності. Відстеження внесення змін користувачами та їх впливу на безпеку даних є трудомістким процесом і недостатній їх контроль може призвести до невідповідності вимогам.

3) Автоматизація. Невідповідність може бути результатом нездатності спеціалістів безпеки використовувати рішення автоматизації для відповідності показникам. Деякі закони чи правила безпеки вимагають ручного моніторингу хмарних інфраструктур. Стандарти безпеки набагато легше дотримуватися, коли процеси перевірки відповідності можна автоматизувати.

4) Безпека даних. Основна мета правил безпеки в хмарі полягає в забезпеченні безпеки та конфіденційності даних які потребують захисту. Оскільки хмарні середовища мають кілька точок доступу, які можуть бути скомпрометовані, зловмисники мотивовані атакувати хмарні системи. Крім того, постійно зростає кількість кібератак і загроз.

5) Підтримання стандартів відповідності. Існує багато нормативних вимог або стандартів, у тому числі вимоги щодо відповідності постачальників

хмарних послуг і галузевих стандартів відповідності (наприклад, Стандарт безпеки даних платіжних карток (PCI DSS). Після їх оновлення, компанії інвестують значні ресурси, щоб запровадити відповідні зміни, забезпечуючи при цьому оптимальну продуктивність системи безпеки [13].

3.3 Міжнародні стандарти безпеки при використанні хмарних обчислень

Основні міжнародні стандарти, що надають вимоги до кіберзахисту в хмарах:

1) ISO/IEC 27001:2022

ISO/IEC 27001 містить вимоги до ідентифікації систем управління інформаційною безпекою (СУІБ або ISMS). ISO/IEC 27001 надає компаніям будь-яких розмірів і секторів діяльності вказівки щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою.

Відповідність стандарту ISO/IEC 27001 означає, що організація або бізнес запровадили систему для управління ризиками, пов’язаними з безпекою даних, якими володіє або обробляє компанія, і що ця система відповідає всім найкращим практикам і принципам, закріпленим у цьому міжнародному стандарті.

Зі зростанням кіберзлочинності та постійною появою нових загроз може здатися складним або навіть неможливим керувати кіберризиками. ISO/IEC 27001 допомагає організаціям усвідомлювати ризики та завчасно виявляти та усувати недоліки.

ISO/IEC 27001 сприяє цілісному підходу до інформаційної безпеки: перевірка людей, політик і технологій. Система управління інформаційною безпекою, впроваджена відповідно до цього стандарту, є інструментом для управління ризиками, кіберстійкості та операційної досконалості [14].

2) ISO/IEC 27002:2022

Даний стандарт надає довідковий перелік загальних засобів контролю інформаційної безпеки та вказівки щодо їх впровадження. Цей документ призначений для використання організаціями:

- У контексті системи управління інформаційною безпекою (ISMS) на основі ISO/IEC27001;
- Для впровадження засобів контролю інформаційної безпеки на основі міжнародно визнаної найкращої практики;
- Для розробки керівних принципів управління інформаційною безпекою для конкретної організації [15].

3) ISO/IEC 27017:2015

Стандарт, призначений постачальникам хмарних сервісів і користувачам з ціллю зменшення ризику виникнення інцидентів безпеки.

ISO/IEC 27017:2015 дає настанови щодо засобів контролю інформаційної безпеки, застосовних до надання та використання хмарних послуг, забезпечуючи:

- додаткові настанови щодо впровадження відповідних засобів контролю, визначених у ISO/IEC 27002;
- додаткові елементи керування з інструкціями щодо впровадження, які стосуються саме хмарних служб.

Цей міжнародний стандарт надає засоби керування та вказівки стосовно впровадження для постачальників хмарних послуг і для клієнтів хмарних послуг [16].

4) ISO/IEC27018:2019

ISO/IEC27018 застосовується для захисту конфіденційної інформації у публічній хмарі, заснований на принципах ISO/IEC-29100 для публічних хмар.

Цей документ встановлює загальноприйняті цілі контролю, засоби контролю та вказівки стосовно впровадження заходів із захисту персональних ідентифікаційних даних, дотримуючись принципів конфіденційності, наданих в ISO/IEC 29100 для середовища публічних хмарних обчислень.

Зокрема, цей документ містить інструкції на основі ISO/IEC 27002, беручи до уваги нормативні вимоги щодо захисту ідентифікаційної інформації, які можуть бути застосовані в контексті середовищ(а) ризику інформаційної безпеки постачальника публічних хмарних послуг.

Цей документ стосується організацій усіх типів і розмірів, у тому числі державних і приватних компаній, державних установ і некомерційних організацій, які надають послуги з обробки інформації як процесори ідентифікаційної інформації через хмарні обчислення за контрактом з іншими організаціями.

Вимоги цього документі також можуть стосуватися організацій, які виконують функції контролерів ідентифікаційної інформації. Однак на контролери ідентифікаційної інформації можуть поширюватися додаткові законодавчі акти, положення та зобов'язання щодо захисту ідентифікаційної інформації, які не застосовуються до обробників ідентифікаційної інформації. Цей документ не призначений для покриття таких додаткових зобов'язань [17].

5) Загальний регламент захисту даних (GDPR)

Цей регламент встановлює правила, що стосуються захисту фізичних осіб щодо обробки персональних даних, а також правила, що стосуються вільного руху персональних даних.

GDPR захищає основні права та свободи фізичних осіб і, зокрема, їх право на захист персональних даних.

Вимоги цього документу застосовуються до обробки персональних даних повністю або частково автоматизованими засобами та до обробки персональних даних, відмінних від автоматизованих засобів, які є частиною системи зберігання даних або призначені для формування частини системи зберігання даних.

Дія цього регламент не поширюється на обробку персональних даних:

- під час діяльності, яка виходить за межі законодавства Союзу;
- фізичною особою в ході суто особистої чи домашньої діяльності;
- компетентними органами влади з метою запобігання, розслідування, виявлення або судового переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз громадській безпеці та їх запобігання [18].

6) Дотримуючись CIS AWS Foundations Benchmark, будь-яка фірма, яка використовує хмарні ресурси Amazon Web Service, може допомогти захистити конфіденційні IT-системи та дані. Тест CIS (Центр безпеки в Інтернеті) – це набір об’єктивних критеріїв конфігурації на основі консенсусу, створених аналітиками, щоб допомогти підприємствам оптимізувати інформаційну безпеку. Крім того, протоколи CIS призначені для посилення облікових записів AWS, щоб створити стабільну базу для виконання завдань на AWS. У цьому стандарті описано найкращі методи безпечного налаштування публічних хмарних ресурсів. Center of Internet Security (CIS) Benchmark працював із спільнотою, щоб опублікувати еталонний тест для різних хмарних провайдерів, таких як Alibaba, AWS, Google Cloud, IBM Cloud, Azure, Oracle Cloud та інших [19].

4 АНАЛІЗ І ДОСЛІДЖЕННЯ ВИМОГ ДО КІБЕРЗАХИСТУ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ

Кіберзахист інформації забезпечується в основному стандартами сімейства ISO/IEC 27000 та стандартом NIST SP 800-53, який використовується в найвідоміших хмарних сервісах, таких як AWS, Google Cloud Platform та Azure.

Оскільки стандарт ISO/IEC 27001:2022, відсутній у вільному доступі, дослідження засновано на доступній версії цього стандарту 2015 року. Крім того, в дослідженні використано стандарт NIST Special Publication 800-53 Revision 5.

4.1 ISO/IEC 27001:2015

Стандарт визначає вимоги щодо проектування, запровадження, функціонування, моніторингу, перегляду, постійного вдосконалення і підтримки СУІБ з урахуванням контексту діяльності організації. Система управління інформаційною безпекою гарантує збереження конфіденційності, цілісності та доступності інформаційних ресурсів завдяки впровадженню процесу управління ризиками. Крім того, зацікавленим сторонам вона надає впевненість, що управління ризиками відбувається належним чином.

Згідно з цим стандартом, організації, що застосовують хмарні обчислення, повинні визначити зовнішні та внутрішні аспекти, які важливі для її цілей та мають вплив на здатність досягти раніше запланованого результату її СУІБ.

Цей стандарт містить вимоги до кіберзахисту в хмарній інфраструктурі стосовно:

1) Політики інформаційної безпеки.
2) Організація інформаційної безпеки.
3) Безпеки дій персоналу.
4) Управління ресурсами СУІБ.

5) Контролю доступу.
6) Криптографії.
7) Фізичної безпеки та захисту від зовнішнього впливу.
8) Обладнання.
9) Безпеки експлуатації.
10) Безпеки комунікацій.
11) Придбання, розробки, підтримки інформаційних систем.
12) Взаємовідносин з постачальником.
13) Управління інцидентами інформаційної безпеки.
14) Аспектів інформаційної безпеки управління безперервністю бізнесу.
15) Відповідності [20].

4.1.1 Переваги ISO/IEC 27001

До переваг даного стандарту належать:

- Глобальне визнання. ISO/IEC 27001 це найвпливовіший та найрозповсюдженіший міжнародний стандарт безпеки інформації. Він став офіційним стандартом для багатьох галузей та організацій.

- Комплексний підхід до забезпечення безпеки інформації в системі. Стандарт надає систематичний підхід до управління інформаційною безпекою. Включає в себе визначення політики безпеки, ідентифікацію ризиків, встановлення заходів контролю та забезпечення процесу постійного вдосконалення. Такий підхід дозволяє забезпечувати повноту та надійність інформаційної безпеки системи.

- Універсальність застосування. Стандарт може застосовуватись в організаціях будь-якого розміру, галузі діяльності та юридичного статусу, а також може бути адаптованим до конкретних вимог організації та контексту її діяльності, забезпечуючи високий рівень безпеки інформаційних ресурсів.

- Підтримка у виконанні вимог законодавства. ISO/IEC 27001 враховує вимоги законодавства та регуляторних органів з питань безпеки інформації. Впровадження цього стандарту дозволяє організаціям виконувати

правові норми, пов’язані з забезпеченням безпеки інформації, що зменшує ризик порушення цих норм та допомагає уникнути відповідних наслідків [20].

4.1.2 Недоліки ISO/IEC 27001

Незважаючи на наявність великої кількості переваг, ISO/IEC 27001 має потенційні недоліки, такі як:

- Складність впровадження. Це високо структурований та деталізований стандарт, тому його впровадження може вимагати значних зусиль та ресурсів. Для розуміння, адаптації та реалізації всіх вимог стандарту організаціям необхідна консультація фахівця.
- Високі витрати на впровадження. Проведення аудитів, навчання персоналу, впровадження технологічних засобів провокує значні фінансові витрати організацій.
- Потреба в оновленні. Під впливом постійних змін загроз та технологій, ISO/IEC 27001 зазнає оновлень. Організації, які прагнуть зберегти сертифікацію даного стандарту, повинні систематично оновлювати системи та процеси до нових його версій.
- Висока залежність від людського фактору. Ефективне впровадження та дотримання вимог цього стандарту потребує активної участі та свідомого дотримання персоналом організації [20].

4.2 NIST Special Publication 800-53 Revision 5

Стандарт під назвою «Контроль безпеки та конфіденційності для інформаційних систем і організацій», виданий Національним інститутом стандартів і технологій у США. Даний стандарт надає опис повного набору засобів контролю безпеки та конфіденційності для інформаційних систем і організацій.

Основна мета SP 800-53 Revision 5 це стандартизація впровадження ефективних програм безпеки та конфіденційності для захисту інформації та інформаційних систем. Він містить каталог елементів керування безпекою та конфіденційністю, а також відповідні вказівки щодо вибору та впровадження цих елементів керування.

Редакція 5 SP 800-53 містить оновлення та вдосконалення каталогу засобів керування, включаючи інтеграцію елементів керування конфіденційністю та додавання нових елементів керування для вирішення нових технологій і загроз. Видання також підкреслює важливість управління ризиками та налаштування засобів контролю на основі оцінки організаційних ризиків.

SP 800-53 Revision 5 широко визнаний і використовується як довідник організаціями в різних секторах, включаючи державні установи, приватні компанії та інші організації, які займаються інформаційною безпекою та конфіденційністю. Цей стандарт забезпечує структуру для проектування, впровадження та керування засобами контролю безпеки та конфіденційності для захисту конфіденційної інформації та забезпечення стійкості інформаційних систем.

NIST SP 800-53 охоплює наступні аспекти хмарної безпеки та конфіденційності:

1) Управління доступом;
2) Навчання та підвищення обізнаності;
3) Аудит та звітність;
4) Оцінювання, авторизація та моніторинг;
5) Керування конфігурацією;
6) Врегулювання непередбачуваних ситуацій;
7) Ідентифікація та аутентифікація;
8) Реагування на інциденти;
9) Обслуговування;
10) Захист медіа;
11) Захист фізичного середовища;
12) Планування;
13) Програмне управління;
14) Кадрова безпека;
15) Обробка персональної ідентифікуючої інформації та прозорість;

16) Оцінка ризиків;
17) Закупівля систем та послуг;
18) Захист систем та зв’язку;
19) Цілісність системи та інформації;
20) Управління ризиками ланцюга постачання [21].

4.2.1 Переваги NIST Special Publication 800-53 Revision 5

До переваг даного стандарту відносяться:

- Комплексність і повнота. NIST SP 800-53 надає широкий спектр рекомендацій щодо забезпечення безпеки інформаційних систем і охоплює такі аспекти як: управління ризиками, фізична безпека, контроль доступу, криптографія, забезпечення безпеки програмного забезпечення та інші, що дозволяє створювати комплексні та цілісні плани безпеки інформаційних систем.

- Актуальність та відповідність. Даний стандарт постійно переглядається та оновлюється з урахуванням змін у використовуваних технологіях, наявних загрозах та регуляторному середовищі. Вимоги NIST SP 800-53 відповідають більшості регуляторних стандартів.

- Гнучкість й адаптованість. Надається гнучка архітектура контролю інформаційної безпеки, яка дозволяє організаціям вибирати та налаштовувати необхідні заходи контролю залежно від потреб та вимог організації. Його вимоги дозволяють забезпечити належний рівень безпеки для різноманітних сценаріїв за рахунок розгляду різних рівнів ризику, типів систем та контексту роботи організації.

- Застосування в широкому спектрі галузей. Велика кількість організацій, що працює в таких галузях як промисловість, фінанси, охорона здоров’я та інші, застосовує ці вимоги як стандарт забезпечення інформаційної безпеки системи.

- Загальноприйнятість та сумісність. NIST SP 800-53 являється одним з найбільш визнаних та широко прийнятих наборів рекомендацій із

забезпечення інформаційної безпеки системи. Він сумісний з багатьма стандартами безпеки, в тому числі з ISO/IEC 27001 та іншими [21].

4.2.2 Недоліки NIST Special Publication 800-53 Revision 5

Окрім переваг, NIST SP 800-53 має наступні недоліки:

- Складність та обсяг. Цей стандарт є обширним і докладним документом, що надає широкий спектр вимог та заходів контролю інформаційної безпеки.
- Брак конкретизації. В документі надаються загальні рекомендації і заходи контролю безпеки, без конкретизації деталізованих методів або технічних рішень для їх впровадження.
- Відсутність міжнародного статусу. NIST SP 800-53 розроблений для федерального сектору США і не має офіційного статусу міжнародного стандарту, що може призводити до відсутності всесвітнього визнання та прийняття в міжнародному контексті.
- Вимоги до ресурсів. Розробка, впровадження та підтримка системи безпеки організації на основі вимог даного стандарту вимагає використання значного обсягу ресурсів [21].

4.3 Порівняння ISO/IEC 27001 та NIST Special Publication 800-53 Revision 5

NIST SP 800-53 та ISO/IEC 27001 – це два різні стандарти, які визначають, як організації можуть найкращим чином захистити свої системи та дані від кібератак та інших форм загроз інформаційній безпеці. Для забезпечення найвищого рівня безпеки даних, організації повинні розуміти відмінності між двома стандартами та способи їх спільного використання. Ці елементи керування є частиною NIST Cyber Security Framework, яка є уніфікованим набором стандартів, інструкцій і найкращих практик, які надають організаціям комплексний підхід до управління ризиками та покращення рівня безпеки.

Незважаючи на те, що NIST SP 800-53 й ISO/IEC 27001 є різними стандартами, їх варто використовувати разом для забезпечення комплексної

системи безпеки. NIST SP 800-53 надає детальні вказівки щодо того, як запроваджувати засоби контролю безпеки, тоді як ISO/IEC 27001 надає структуру того, як слід організовувати та впроваджувати засоби керування. Використовуючи два стандарти разом, організації можуть створити комплексну програму безпеки, яка захищає їхні дані та системи від різноманітних загроз безпеці.

Порівняння викладення вимог, описаних у цих стандартах надано в таблиці 4.1 [21].

Таблиця 4.1 – Викладення вимог ISO/IEC 27001 та NIST SP 800-53

Група вимог	NIST SP 800-53	ISO/IEC 27001
Управління доступом	Контроль доступу до інформації та інформаційних систем, включно з ідентифікацією та автентифікацією користувачів, керування привілеями, контролем доступу та моніторингом.	Контроль доступу до інформації, контроль змін до інформації та управління інцидентами інформаційної безпеки.
Аудит та звітність	Записи аудиту, перевірка аудиту та звітність, скорочення аудиту.	Проведення моніторингу, реєстрація подій безпеки, реагування на події безпеки та звітування про них керівництву.

Продовження таблиці 4.1

Група вимог	NIST SP 800-53	ISO/IEC 27001
Підвищення обізнаності та навчання	Вимоги до обізнаності та навчання з питань безпеки, включаючи безпеку персоналу, підвищення обізнаності та навчання з питань безпеки.	Вимоги до безпеки персоналу. Контроль доступу. Перевірка досвіду та кваліфікації персоналу, навчання співробітників.
Управління конфігурацією	Вимоги щодо планування керування конфігурацією. Контроль зміни конфігурації та облік стану конфігурації.	Вимоги до керування конфігурацією, включаючи контроль змін, ідентифікацію та аудит конфігурації.
Планування дій в разі виникнення непередбачуваних ситуацій	Розробка та документування політики та процедур планування на випадок надзвичайних ситуацій. Координація планування на такий випадок. Тестування та відпрацювання планування дій в разі кризових ситуацій.	Оцінка ризику, обробка ризиків. Розробка та впровадження заходів для забезпечення неперервної діяльності системи.

Продовження таблиці 4.1

Група вимог	NIST SP 800-53	ISO/IEC 27001
Ідентифікація та аутентифікація	Ідентифікація та аутентифікація користувача. Контроль доступу користувачів.	Керування ідентифікацією та доступом, включно з реєстрацією користувачів та перевірку ідентифікації. Методи автентифікації та контроль доступу.
Реагування на інциденти безпеки	Заходи реагування на інциденти, в тому числі планування реагування на інциденти, їх виявлення, аналіз, локалізація та ліквідація.	Планування реагування на інциденти. Виявлення та аналіз інцидентів, стримування та відновлення системи.
Технічне обслуговування	Планування технічного обслуговування. Контроль технічного обслуговування. Огляд і аудит технічного обслуговування.	Підтримка інформаційної безпеки шляхом контролю змін, перевірки продуктивності системи та обслуговування системи.
Захист медіа	Маркування та використання носіїв інформації. Зберігання, транспортування й утилізація носіїв інформації.	
Кадрова безпека	Відбір і наймання кваліфікованого персоналу. Допуск персоналу до захищених ресурсів організації. Звільнення персоналу.	

Продовження таблиці 4.1

Група вимог	NIST SP 800-53	ISO/IEC 27001
Захист фізичного середовища	Фізичний контроль доступу до інформації. Моніторинг навколишнього середовища та обслуговування обладнання.	Контроль доступу, моніторинг навколишнього середовища та управління активами.
Планування	Придбання, впровадження та розвиток системи і послуг.	Розробка політики інформаційної безпеки. Її підтримка та періодичний перегляд.
Програмне управління	Планування та вимоги до програмного управління. Звітність, моніторинг, огляд та аудит програмного управління.	Організація інформаційної безпеки, відповідальність за управління та комунікацію.
Оцінка ризиків	Планування та координація оцінки ризиків. Заходи з оцінки ризику та звітність про оцінку ризиків.	
Оцінка захищеності та авторизація	Планування та координація оцінки безпеки, заходи з оцінки безпеки та звітність щодо оцінки безпеки.	
Захист систем і комунікацій	Планування, моніторинг та впровадження заходів захисту системи та комунікацій.	Впровадження та моніторинг комунікацій.

Продовження таблиці 4.1

Група вимог	NIST SP 800-53	ISO/IEC 27001
Цілісність системи та інформації	Планування, впровадження та моніторинг цілісності системи й інформації	
Закупівля систем та послуг	Планування, реалізація та моніторинг придбання систем і послуг	Планування придбання систем, планування розвитку та обслуговування систем. Придбання, розробка та моніторинг підтримки системи.

4.4 Аналіз рівня захищеності системи при дотриманні вимог стандартів NIST SP 800-53 та ISO/IEC 27001

При одночасній реалізації вимог цих двох стандартів для захисту інформації при використанні хмарних обчислень забезпечується високий рівень захисту ресурсів системи віл різних типів атак і загроз. Основні типи атак, захист від яких забезпечується дотриманням вимог стандартів NIST SP 800-53 та ISO/IEC 27001:

- Атаки на конфіденційність даних. Вимоги стандартів покликані забезпечити захист інформації від несанкціонованого доступу, розголошення та перехоплення даних, витоку інформації, шпигунства та інших атак на конфіденційність. Для цього застосовується шифрування даних, захист мережевого зв’язку, криптографічні алгоритми та забезпечення безпеки фізичного середовища функціонування системи.
- Атаки на цілісність даних. Дотримання вимог цих нормативних актів запобігає неправомірній модифікації та втраті даних, включаючи віруси, зловмисний код, підміну даних при обміні або при зберіганні інформації. Забезпечується контроль цілісності інформації, моніторинг і виявлення некоректних змін, резервне копіювання і відновлення даних.
- Атаки на доступність даних. Завдяки реалізації рекомендацій цих стандартів встановлюється захист від атак, спрямованих на обмеження доступності інформаційних ресурсів, наприклад, DDoS-атак. Забезпечення доступності системи відбувається за допомогою використання резервних каналів зв’язку, забезпечення надійності мережевої інфраструктури та інших вимог.
- Атаки на автентифікацію. Використання даних стандартів дозволяє захистити процес аутентифікації, враховуючи можливість використання неправомірних автентифікаційних даних, підробку автентифікаційних механізмів, тощо. До вимог цих стандартів, що допомагають забезпечити захист від атак на аутентифікацію, відносяться вимоги використання сильних

паролів, двофакторної автентифікації, управління автентифікаційними механізмами та інші.

- Атаки на доступ. Одночасне використання стандартів NIST SP 800-53 та ISO/IEC 27001 дозволяє виключити можливість НСД до систем, маніпулювання автентифікацією та контролем доступу, підбір паролів, використання слабких автентифікаційних методів. В стандартах надаються рекомендації щодо контролю доступу, автентифікації, авторизації та ідентифікації.

NIST SP 800-53 та ISO/IEC 27001 надають вимоги щодо впровадження заходів забезпечення інформаційної безпеки, що дозволяють зменшити ризики для систем і успішність проведення різних типів атак. Проте, навіть повна відповідність всім описаним в цих документах вимогам, не може гарантувати повного захисту від всіх можливих атак, оскільки кіберзлочинці постійно вдосконалюють власні методи та використовують нові вразливості інформаційних систем. Основні типи атак, від яких не може убезпечити дотримання вимог цих стандартів:

- Атаки нульового дня. Такий тип атак, для якого використовуються раніше не відомі вразливості системи, для пошкодження або викрадення даних системи, ураженої цією вразливістю.

- Внутрішні атаки. Не дивлячись на те, що стандарти включають заходи забезпечення внутрішньої безпеки системи, вони не можуть гарантувати відсутність ризику недобросовісних чи некоректних дій з боку персоналу організації.

- Соціально-інженерні атаки. Наявність навчання та підвищення обізнаності серед користувачів не повністю гарантує невразливість до фішингу, фармінгу, соціального інжинірингу та інших атак, що залежать від маніпуляцій людьми.

4.5 Варіанти покращення наявних вимог стандартів NIST SP 800-53 та ISO/IEC 27001

В результаті проведеного аналізу вимог до кіберзахисту, наданих в NIST SP 800-53 та ISO/IEC 27001, можна зробити висновок що при спільному їх використанні забезпечується комплексна система захисту інформації. Проте, зважаючи на постійний розвиток інформаційних технологій та появу нових атак, варто постійно переглядати та покращувати вимоги щодо кіберзахисту. Можливими варіантами покращення цих вимог можуть бути:

- Для запобігання атакам нульового дня варто проводити ретельний моніторинг активності та аналіз журналів, використовувати захисні системи (брандмауери, системи виявлення вторгнень, антивіруси, системи контролю доступу та інші).
- Для мінімізації ризику виникнення внутрішніх атак, спричинених несанкціонованими діями персоналу організації, рекомендується проводити регулярний моніторинг задоволеності персоналу умовами праці. Це дозволить нівелювати вигоду від злочинних дій співробітників організації.
- Вірогідність виникнення соціально-інженерних атак може знизитись за рахунок використання спеціальних заходів забезпечення інформаційної безпеки. Таких як, система на основі штучного інтелекту, яка проводить аналіз всіх надісланих в мережі повідомлень і виявляє серед них підозрілу активність.

ВИСНОВКИ

У ході виконання даної кваліфікаційної роботи було проведено аналіз та дослідження вимог до кіберзахисту при використанні хмарних обчислень. Хмарні обчислення є перспективним напрямком в інформаційних технологіях, але збільшення обсягів даних, що зберігаються в хмарних системах, а також зростання кількості кібератак, призвело до зростання вимог до кіберзахисту.

Проведено аналіз підходів до забезпечення кібербезпеки в хмарних обчисленнях, зокрема, управління доступом, захист даних та мережева безпека. Виявлено, що проблеми кібербезпеки в хмарних обчисленнях є складними і потребують поєднання технічних, організаційних та правових заходів для забезпечення надійного захисту.

Результати дослідження вказують на необхідність розробки нових методів та інструментів забезпечення кібербезпеки в хмарних обчисленнях. Однак, на даний момент, ще існує прогалина в знаннях та практичних розробках, які можуть забезпечити повноцінний захист даних в хмарних системах.

У світі проблема кібербезпеки в хмарних обчисленнях є актуальною і вирішується провідними спеціалістами у даній галузі. Однак, ще більше зусиль потрібно зробити, щоб забезпечити надійний кіберзахист у хмарних обчисленнях.

Отже, результати цієї кваліфікаційної роботи є актуальними та важливими для подальшого розвитку хмарних технологій та забезпечення кібербезпеки. Результати дослідження можуть бути використані для розробки більш ефективних технічних засобів кіберзахисту в хмарних сервісах та формування національної політики в галузі кібербезпеки. Також, можливими галузями використання результатів роботи є розробка нових технологій та засобів кіберзахисту для хмарних сервісів, а також вдосконалення існуючих методів та технологій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Про хмарні послуги. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 06.05.2023).

2 Cloud Security Requirements. [Електронний ресурс]. URL: https://www.cms.gov/tra/Content/Infrastructure_Services/IS_0100_Cloud_Security_Requirements.htm?TocPath=Infrastructure%20Services|Cloud%20IaaS%20and%20PaaS%20Infrastructure|_____5 (дата звернення: 06.05.2023).

3 Модель системи захисту інформації для хмарної СКБД. URL: https://ela.kpi.ua/bitstream/123456789/27195/1/Mazurenko_magistr.pdf (дата звернення: 06.05.2023).

4 Переваги та недоліки хмарних сервісів .: Ресурсний центр ГУРТ. Ресурсний центр ГУРТ. URL: https://gurt.org.ua/articles/38359/ (дата звернення: 10.04.2023).

5 What is Public Cloud | IBM. [Електронний ресурс]. URL: https://www.ibm.com/topics/public-cloud (дата звернення: 06.05.2023).

6 What is Private Cloud? | IBM. [Електронний ресурс]. URL: https://www.ibm.com/topics/private-cloud (дата звернення: 06.05.2023).

7 What Is Community Cloud? Definition, Architecture, Examples, and Best Practices - Spiceworks. [Електронний ресурс]. URL: https://www.spiceworks.com/tech/cloud/articles/what-is-community-cloud/ (дата звернення: 06.05.2023).

8 What is a Hybrid Cloud? | Google Cloud. [Електронний ресурс]. URL: https://cloud.google.com/learn/what-is-hybrid-cloud (дата звернення: 06.05.2023).

9 Каталоги | Національна бібліотека України імені В. І. Вернадського. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Uprv_2014_4_6.pdf (дата звернення: 30.05.2023).

10 STRIDE-LM Threat Model. URL: https://csf.tools/reference/stride-lm/ (дата звернення: 30.05.2023).

11 Аулов І. Ф. - Дослідження моделі загроз ключових систем хмари та пропозиції захисту від них (2015). Національна бібліотека України імені В. І. Вернадського. URL: http://nbuv.gov.ua/UJRN/Vejpte_2015_5(2)__2 (дата звернення: 30.05.2023).

12 Cloud Security Requirements. [Електронний ресурс]. URL: https://www.cms.gov/tra/Content/Infrastructure_Services/IS_0100_Cloud_Security_Requirements.htm?TocPath=Infrastructure%20Services|Cloud%20IaaS%20and%20PaaS%20Infrastructure|_____5 (дата звернення: 06.05.2023).

13 Cloud Security Compliance: Requirements & Standards | AlgoSec. [Електронний ресурс]. URL: https://www.algosec.com/resources/cloud-compliance/ (дата звернення: 06.05.2023).

14 ISO/IEC 27001 Standard – Information Security Management Systems. [Електронний ресурс]. URL: https://www.iso.org/standard/27001 (дата звернення: 06.05.2023).

15 ISO/IEC 27002:2022. [Електронний ресурс]. URL: https://www.iso.org/standard/75652.html (дата звернення: 06.05.2023).

16 ISO/IEC 27017:2015. [Електронний ресурс]. URL: https://www.iso.org/standard/43757.html (дата звернення: 06.05.2023).

17 ISO/IEC 27018:2019. [Електронний ресурс]. URL: https://www.iso.org/standard/76559.html (дата звернення: 06.05.2023).

18 Загальний регламент про захист даних (GDPR) - GDPR-Text.com. [Електронний ресурс]. URL: https://gdpr-text.com/uk/ (дата звернення: 06.05.2023)/

19 Cloud Custodian Policies for CIS AWS Foundations Benchmark (Part 1). [Електронний ресурс]. URL: https://ismsguy.medium.com/cloud-custodian-policies-for-cis-aws-foundations-benchmark-part-1-43d711effa4b (дата звернення: 07.05.2023)/

20 ISO/IEC 27001. Information technology – Security techniques – Information security management systems – Requirements. Чинний від 2013-01-01. Вид. офіц.

21 NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. Вид. офіц.

ДОДАТОК А

АНАЛІЗ ТА ДОСЛІДЖЕННЯ ВИМОГ ДО КІБЕРЗАХИСТУ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ

Сніжана НОВОСЬОЛОВА[a], Юрій ГОРБЕНКО[b]

[a] *Харківський національний університет імені В. Н. Каразіна, майдан Свободи 4, Харків, Україна*
[b] *АТ «Інститут Інформаційних технологій», вул. Коломенська 15, Харків, Україна*

Анотація. *У цій роботі наведено вимоги до кіберзахисту при використання хмарних технологій та огляд міжнародних стандартів, присвячених цьому.*
Ключові слова. *Хмарні сервіси, хмарні обчислення, стандартизація*

1. Вступ

Вимоги до кіберзахисту стають все більш актуальними в контексті зростаючої залежності сучасного суспільства від інформаційних технологій, зокрема, хмарних сервісів. Щоб підвищити безпеку та зменшити ризики, існує багато нормативних вимог та стандартів. У зв'язку із актуальністю даної теми, у даній роботі буде розглянуто цілі кіберзахисту в хмарних сервісах, основні проблеми, що можуть виникнути, та наведено перелік міжнародних стандартів, які регулюють вимоги.

2. Цілі кіберзахисту

Виділяють наступні цілі кіберзахисту [1]:

- Запобігання несанкціонованому доступу до ресурсів інфраструктури хмарних обчислень;
- Управління векторами загроз гіпервізора;
- Мінімізація спільного доступу до мережі;
- Управління доступом привілейованих користувачів;
- Застосування відповідних заходів безпеки на CSP;
- Визначення кордонів довіри між CSP та споживачами CMS.

3. Проблеми дотримання вимог

Нижче наведено деякі ключові проблеми дотримання вимог, з якими зазвичай стикаються користувачі хмари [2]:

- Дотримуватись стандартів важко організаціям, які керують гібридними мережами, через проблеми з видимістю. Гібридна мережа використовує більше, ніж один тип технології підключення або топології. Це ускладнює отримання видимості кожного компонента мережі.
- Більшість компаній використовують багатохмарні рішення. Робота з кількома хмарними службами та наявність співробітників, які мають доступ до даних із різних пристроїв, ускладнюють дотримання інформаційної безпеки та стандартів хмарного керування.
- Закони чи правила безпеки вимагають ручного моніторингу хмарних інфраструктур. Цей підхід займає багато часу. Стандартів безпеки набагато легше дотримуватися, коли процеси перевірки відповідності можна автоматизувати.
- Зростає кількість кібератак, і кіберзлочинці стають більш досвідченими, ніж раніше. Оскільки хмарні середовища мають кілька точок доступу, які можуть бути скомпрометовані, зловмисники мотивовані атакувати хмарні системи.

4. Міжнародні стандарти

Існують різноманітні міжнародні стандарти безпеки хмарних сервісів. Далі наведено огляд деяких міжнародних стандартів хмарної безпеки.

1. ISO 27001 / ISO 27002 [3, 4]

Стандарт ISO 27001 містить вимоги до ідентифікації систем управління інформаційною безпекою (ISMS), а також оцінку та управління ризиками для процесів, що стосуються обробки інформації. Це корисно, наприклад, коли проект знаходиться на початковій стадії. ISO 27002

містить довідковий набір загальних засобів контролю інформаційної безпеки, включаючи вказівки щодо впровадження.

2. ISO 27017 [5]

ISO 27017 – це стандарт безпеки, створений для постачальників хмарних послуг і споживачів з метою зниження ризику інциденту безпеки в хмарі. Крім того, це також стандарт для хмарних організацій, який допомагає контролювати рекомендації та впровадження. Це стосується організацій, які зберігають дані в хмарі, і компаній, які надають хмарні послуги іншим компаніям, які можуть мати конфіденційні дані.

3. ISO 27018 [6]

ISO 27018 використовується для захисту ідентифікаційної інформації у публічній хмарі. Він дотримується всіх принципів ISO/IEC 29100 для публічних хмарних обчислювальних середовищ. Крім того, ISO 27018 також можна застосовувати до організацій будь-якого типу та розміру: державних чи приватних, державних або неприбуткових організацій.

4. Загальний регламент захисту даних (GDPR) [7]

Умова GDPR поширюється на кожного члена Європейського Союзу. Його мета полягає в тому, щоб побудувати безперервний захист даних споживачів у всіх членах Європейського Союзу. Важливо враховувати, що будь-яка компанія, яка співпрацює з ЄС, підпорядкована його правилам. З цієї причини ЄС має вплив на захист даних у всьому світі.

5. Основи CIS AWS v1.2 [8]

Дотримуючись CIS AWS Foundations Benchmark, будь-яка фірма, яка використовує хмарні ресурси Amazon Web Service, може захистити конфіденційні IT-системи та дані.

CIS (Центр безпеки в Інтернеті) – це набір об'єктивних критеріїв конфігурації на основі консенсусу, створених аналітиками, щоб допомогти підприємствам оптимізувати інформаційну безпеку. Крім того, протоколи CIS призначені для посилення облікових записів AWS, щоб створити стабільну базу для виконання завдань на AWS.

5. Висновки

Отже, вимоги до кіберзахисту в контексті хмарних обчислень є актуальним питанням, оскільки ці технології набувають все більшої популярності. Забезпечення безпеки даних та інфраструктури, виявлення та запобігання загрозам, та забезпечення надійності та доступності сервісів є важливими завданнями кіберзахисту у контексті хмарних обчислень.

Для найкращого досягнення цих завдань необхідно забезпечити відповідність вимогам, що визначені в міжнародних стандартах, які були розглянуті в даній роботі, а саме: ISO 27001, ISO 27017, ISO 27018 та інші.

6. Список літератури

[1] Cloud Security Requirements. Home - Centers for Medicare & Medicaid Services | CMS. URL: https://www.cms.gov/tra/Content/Infrastructure_Services/IS_0100_Cloud_Security_Requirements.htm?TocPath=Infrastructure%20Services|Cloud%20IaaS%20and%20PaaS%20Infrastructure|_____5 (дата звернення: 06.05.2023).

[2] Cloud Security Compliance: Requirements & Standards | AlgoSec. algosec. URL: https://www.algosec.com/resources/cloud-compliance/ (дата звернення: 06.05.2023).

[3] ISO/IEC 27001 Standard – Information Security Management Systems. ISO. URL: https://www.iso.org/standard/27001 (дата звернення: 06.05.2023).

[4] ISO/IEC 27002:2022. ISO. URL: https://www.iso.org/standard/75652.html (дата звернення: 06.05.2023).

[5] ISO/IEC 27017:2015. ISO. URL: https://www.iso.org/standard/43757.html (дата звернення: 06.05.2023).

[6] ISO/IEC 27018:2019. ISO. URL: https://www.iso.org/standard/76559.html (дата звернення: 06.05.2023).

[7] Загальний регламент про захист даних (GDPR) - GDPR-Text.com. GDPR-Text.com – GDPR Text, Translation and Commentary. URL: https://gdpr-text.com/uk/ (дата звернення: 06.05.2023).

[8] Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0 – AWS Security Hub. URL: https://docs.aws.amazon.com/securityhub/latest/userguide/cis-aws-foundations-benchmark.html (дата звернення: 06.05.2023).