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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження моделей обслуговуваня та властивостей хмарних веб-сервісів

Виконав: студент VI курсу, групи СНм-61
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

(підпис) Залужець О.Т. (прізвище та ініціали)

Керівник (підпис) Козбур Г.В. (прізвище та ініціали)

Нормоконтроль (підпис) Мацюк О.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Боднарчук І.О. (прізвище та ініціали)

Рецензент (підпис) Петрик М.Р. (прізвище та ініціали)

Тернопіль
2021

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

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра комп'ютерних наук

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«17» грудня 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня **Магістр**
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

студенту Залужцю Остапу Тарасовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження моделей обслуговування та властивостей хмарних веб-сервісів

Керівник роботи Козбур Галина Володимирівна, к.т.н., доц.кафедри КН

Затверджені наказом ректора від «28» 10 2021 року № 4/7-908.
2. Термін подання студентом завершеної роботи
3. Вихідні дані до роботи Наукові публікації про моделі обслуговування та властивості Хмарних веб-сервісів

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Опис хмарних веб-сервісів. 2 Основні загрози та меоди їх усунення.
3 Дослідження властивостей хмарних веб-сервісів.
4 Охорона праці та безпеки в надзвичайних ситуаціях. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сорінка. 2 Мета роботи. 3 Актуальність теми. 4 Об'єкт та прадмет дослідження.
5 Опис хмарних веб-сервісів. 6 Хмарні сервіси. 7 Обов'язкові характеристики.
8 Універсальний доступ до мережі. 9 Моделі розгортання хмарних систем.
10 Об'єднання ресурсів. 11 Публічна хмара. 12 Гібридна хмара. 13 Моделі обслуговування.
14 IaaS. 15 PaaS. 16 SaaS. 17 Хмарні сервіси у період пандемії. 18 Методи захисту інформації
19 Ринок хмарних послуг. 20 Amazon. 21 Хмарні сервіси для зберігання даних.
22 Хмарні сервіси для колективних проектів 23 Висновки. 24 Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Дмитроца Л.П., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М.		

7. Дата видачі завдання 21 вересня 2021

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	28.10.2021	*Виконано*
2.	Підбір наукових джерел про моделі обслуговування	29.10.2021-2.11.2021	*Виконано*
3.	Переклад та опрацювання наукових джерел про	3.11.2021-5.11.2021	*Виконано*
4.	Виконання дослідження моделей обслуговування	5.11.2021-6.11.2021	*Виконано*
5.	Оформлення розділу «Опис хмарних вебсервісів»	6.11.2021-8.11.2021	*Виконано*
6.	Оформлення розділу «Дослідження властивостей	8.11.2021-9.11.2021	*Виконано*
	хмарних-веб сервісів»		
7.	Виконання завдання до підрозділу «Охорона праці»	14.11.2021-16.11.2021	*Виконано*
8.	Виконання завдання до підрозділу «Безпека в	17.11.2021-18.11.2021	*Виконано*
	надзвичайних ситуаціях»		
9.	Оформлення кваліфікаційної роботи	19.11.2021-23.11.2021	*Виконано*
10.	Нормоконтроль	24.11.2021-25.11.2021	*Виконано*
11.	Перевірка на плагіат	29.11.2021	*Виконано*
12.	Попередній захист кваліфікаційної роботи	10.12.2021	*Виконано*
13.	Захист кваліфікаційної роботи	17.12.2021	

Студент _____ Залужець О.Т.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козбур Г.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження моделей обслуговування та властивостей хмарних веб-сервісів // Кваліфікаційна робота освітнього рівня «Магістр» // Залужець Остап Тарасович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНм-61 // Тернопіль, 2021 // С. 58, табл. – 3, бібліогр. – 51.

Ключові слова: моделі хмарних сервісів, хмарні веб-сервіси.

Кваліфікаційна робота присвячена дослідженню моделей обслуговування та властивостей хмарних веб-сервісів.

В першому розділі кваліфікаційної роботи досліджено хмарні веб-сервіси.

В другому розділі кваліфікаційної роботи досліджено основні загрози втрати і витоку даних та метои їх усунення.

В третьому розділі кваліфікаційної роботи досліджено основні властивості хмарних веб-сервісів.

Об'єкт дослідження: хмарні веб-сервіси.

Предмет дослідження: властивості та моделі хмарних веб-сервісів.

ANNOTATION

Research of service models and properties of cloud web services // Qualification work of educational level "Master" // Zaluzhets Ostap Tarasovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, group SNm-61 // Ternopil, 2021 // C. 58, table. - 3, bibliogr. - 51.

Keywords: cloud service models, cloud web services.

Qualification work is devoted to the study of service models and properties of cloud web services.

The first section of the qualification work explores cloud web services.

The second section of the qualification work examines the main threats of data loss and leakage and methods of their elimination.

The third section of the qualification work explores the main properties of cloud web services.

Object of research: cloud web services.

Subject of research: properties and models of cloud web services.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ – інформаційні технології.

ПЗ – програмне забезпечення.

PaaS (англ. Platform as a Service) – модель надання хмарних обчислень, при якій споживач отримує доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, зв'язного програмного забезпечення, засобів розробки і тестування розміщених у хмарних провайдерах.

SaaS (англ. Software as a Service) – модель поширення програм споживачам, при якій постачальник розробляє веб-програму, розміщує її й управляє нею (самостійно або через третіх осіб) з метою використання її замовниками через Інтернет.

CaaS (англ. Communications as a Service) – побудоване в хмарі комунікаційне рішення для підприємства, яке забезпечує передачу мовного сигналу по мережі Інтернет або по будь-яким іншим IP-мереж (VoIP) , обмін миттєвими повідомленнями (IM) , відеоконференції.

MaaS (англ. Monitoring as a Service) – забезпечує в хмарі моніторинг та безпеку, насамперед на бізнес платформах.

IaaS (англ. Infrastructure as a Service) – це надання комп'ютерної інфраструктури (як правило у формі віртуалізації) як послуги на основі концепції хмарних обчислень.

RAM (англ. Random Access Memory) – швидкодіюча пам'ять, призначена для запису, зберігання та читання інформації у процесі її обробки.

API (англ. Application Programming Interface) – набір визначень взаємодії різнотипного програмного забезпечення.

CPU (англ. Central Processing Unit) – функціональна частина комп'ютера, що призначена для інтерпретації команд.

ЗМІСТ

ВСТУП

Актуальність теми. Інформація – одна із найважливіших ресурсів не лише для конкуруючих за вплив над ринком компаній, але й цілих держав. При цьому обробка та зберігання інформації потребує значної кількості потужності обчислювальних машин. Тому вимоги до них збільшуються з разючою швидкістю. А водночас змінюється і вартість.

Великі обсяги обчислювальної потужності потрібні як для торгових промислових підприємств, так і у галузях освіти та розваг. Тому все гостріше постає питання про необхідність створення економічних та ефективних систем обробки даних.

У зв'язку зі стрімким розвитком технологій бездротового доступу відпала необхідність розташування комплексу засобів обробки та зберігання інформації безпосередньо на території організації та стала можливою віддалена робота з даними. Це дало перший поштовх виникнення хмарних сервісів.

На сьогоднішній день хмарні обчислення є одним з найперспективніших напрямів розвитку інформаційних технологій, і розглядаються як альтернатива традиційним способам роботи з інформацією. Використання структури хмарних обчислень дозволяє реалізувати можливість віддаленої роботи з інформацією та забезпечує досягнення високих показників доступності та відмовостійкості.

Минулого року загальний обсяг світового ринку у сфері хмарних технологій зайняв близько $40 млрд. Більшість експертів прогнозують, що до 2022 року це значення досягне $240 млрд.

Мета роботи. Метою магістерської роботи є дослідження властивостей та моделей хмарних веб-сервісів. Для досягнення поставленої мети потрбно було виконати завдання:

– дослідити основні принципи та напрямки використання моделей обслуговування,

– розглянути деякі веб-сервіси, що надаються концепцією хмарних сервісів,

– проаналізувати основні поняття хмарних сервісів; визначити можливості використання типових моделей послуг/представлення сервісів та розгортання хмар для організації хмарних сервісів,

– зробити висновок про переваги та недоліки хмарних сервісів.

Об’єкт дослідження: хмарні веб сервіси.

Предмет дослідження: властивості та моделі хмарних веб сервісів.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у виявленні специфіки використання моделей хмарних сервісів за умов збільшення попиту під час пандемії.

Практичне значення одержаних результатів. Виконаний в роботі глибиний аналіз існуючих моделей хмарних сервісів, особливостей їх використання в період пандемії дозволить розробити рекомендації для їх використання підприємствами малого та середнього бізнесу.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на міжнародній науково-практичній конференції «Актуальні проблеми науки, освіти та технологій: теорія та практика» (м. Полтава, 2021 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції.

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 51 найменувань. Загальний обсяг кваліфікаційної роботи складає 58 сторінки, з них 47 сторінки основного тексту, який містить 3 таблиці.

1 ОПИС ХМАРНИХ ВЕБ-СЕРВІСІВ

1.1 Характеристики хмарних сервісів

Хмарні обчислення (від англ. cloud computing, також використовується термін «хмарна обробка даних») – це інноваційний спосіб представлення інфраструктури в інформаційних технологіях, який дозволяє користувачам отримувати дистанційний доступ до даних. Цей комплекс складається із сукупності апаратних та мережевих ресурсів, а також програмного забезпечення, що базується на віддалених DATA центрах постачальників. Таким чином, споживачеві можуть бути швидко надані масштабовані обчислювальні ресурси та програмне забезпечення у вигляді послуги, а обов'язки щодо вибору комп'ютерів, що обробляють запити, та операційної системи, що управляє, покладаються на постачальника хмарних послуг. Основною складовою хмари є технологія віртуалізації, яка дозволяє користувачам використовувати обчислювальні ресурси на будь-якій платформі незалежно від апаратної реалізації та допомагає розподіляти обчислювальну потужність, необхідну клієнтам, на кілька серверів, можливо навіть територіально віддалених один від одного [1]. При цьому всі обчислювальні процеси будуть логічно ізольовані один від одного.

Поява концепції хмарних обчислень є результатом розвитку інформаційних технологій за останні кілька десятиліть та стрімким зростанням глобалізації. Термін же з'явився завдяки буквальному словесному опису картинок з книг, в яких робоча станція користувача з'єднувалася з мережею, яка схематично зображується у вигляді хмари.

Вперше ідея про те, що комп'ютерна технологія поділу часу може призвести до майбутнього, в якому комп'ютерна міць і навіть певні програми можуть продаватися з використанням бізнес-моделі «сфери послуг», було висловлено 1961 року американським інформатиком Джоном Маккарті [2]. Поява універсальної комп'ютерної системи IBM System/360 у 1964 році дала

початок мейнфреймам, з якими часто порівнюють хмарні сервіси. Але між ними існує дві принципові відмінності. По-перше, теоретично обчислювальна потужність хмарної системи не має обмежень за дотримання необхідних умов експлуатації. По-друге, термінали для роботи з мейнфреймами призначені безпосередньо для діалогового зв'язку користувача з завданням, що обробляється. А в хмарних системах термінал спочатку є повноцінним засобом роботи, здатним не тільки зберігати інформацію в буфері, ай безпосередньо здійснювати управління глобальним комплексом обчислювальних ресурсів.

З 1990 року стали широко використовуватися grid-обчислення. Цей спосіб обробки даних передбачає систему оренди обчислювальної потужності вільних ресурсів процесорів. На даний момент ця форма розподілених обчислень все ще застосовується для вирішення наукових завдань, де потрібні значні обчислювальні ресурси. І незважаючи на те, що хмарні системи та Grid-обчислення схожі в принципах побудови та експлуатації, перші вважаються найбільш перспективними завдяки більш розвиненим функціям віддаленої роботи.

Новий етап розвитку технологій обробки даних розпочався з настанням 21 століття, коли програмні та апаратні засоби здійснили значний прорив уперед. У 2006 році Amazon представила свою інфраструктуру веб-сервісів під назвою Elastic Computecloud (EC2) , що надає не лише послуги з розміщення інформації та додатків користувачів на сервері, але й можливість їхньої віддаленої обробки [2]. З того часу ідеологія хмарних обчислень щороку набирає популярності завдяки швидкому розвитку каналів зв'язку і потребам користувачів, що стрімко зростають.

На сьогоднішній день хмарні сервіси налічують тисячі серверів, розміщених у центрах обробки даних (ЦОД) , і забезпечують ресурсами десятки тисяч додатків, які одночасно використовують мільйони користувачів.

Щоб система обчислень могла вважатися хмарною, вона повинна відповідати п'яти обов'язковим характеристикам, встановленим Національним інститутом стандартів і технологій США [3].

1) Самообслуговування на вимогу — споживач при необхідності може сам вибирати і змінювати певні параметри системи, такі як серверний час, обробки даних та швидкість доступу, обсяг даних, що зберігаються без взаємодії з представником постачальника послуг;

2) Універсальний доступ по мережі — послуги, що запитуються, доступні споживачам по мережі передачі даних у будь-якій точці світу незалежно від термінального пристрою, що використовується;

3) Об'єднання ресурсів — постачальник послуг об'єднує ресурси обслуговування великої кількості споживачів на єдиний пул для динамічного перерозподілу потужностей між споживачами за умов постійного зміни попиту потужності; при цьому споживачі контролюють лише основні параметри послуги;

4) Еластичність — область послуг може бути розширена або звужена в будь-який момент часу в автоматичному режимі;

5) Облік споживання —автоматично постачальник оцінює обсяг наданих споживачам послуг (наприклад, обсяг даних, що зберігаються, пропускна спроможність, кількість користувачів, кількість транзакцій) , і на основі цих даних розраховує вартість використання.

Для споживача дотримання цих характеристик дає гарантію того, що їм будуть надані автоматично масштабовані послуги з найвищем рівнем доступності та низьким ризиком непрацездатності без необхідності створення, обслуговування та модернізації власної апаратної інфраструктури. ніверсальний та зручний доступ, забеспечує доступність послуг та підтримка різного класу термінальних пристроїв (персональних комп'ютерів, мобільних телефонів, планшетів) .

У той же час для постачальників хмарних обчислень з'являється можливість проектування нової бізнес-моделі надання серверного обладнання, що дозволяє зекономити на масштабах, використовуючи менші ресурси, ніж були б потрібні при виділених апаратних потужностях для кожного споживача завдяки об'єднанню ресурсів та непостійному характеру споживання з боку

споживачів . А за допомогою автоматизацій процедур можна знизити витрати на абонентське обслуговування [4].

Використання хмарних сервісів або відмову від них залежить виключно від потреб користувачів. Якщо компанія або приватний клієнт впевнені в необхідності використання даної моделі надання послуг, першим кроком створення хмарної системи для них буде вибір моделі розгортання.

1.2 Моделі розгортання хмарних систем

На даний момент виділяють основні три моделі розгортання хмарних систем. Вони поділяються на приватні, публічні та гібридні.

Приватна хмара – це внутрішньокорпоративна хмарна інфраструктура, призначена для обслуговування конкретного підприємства та його філій. Приватна хмара може безпосередньо керуватись замовником або бути доручена зовнішньому підряднику. Від цього залежить розміщення апаратної інфраструктури, яка може бути розташована на території клієнта, так і у зовнішнього оператора. Також можливий варіант поділу, коли частина апаратних засобів знаходиться у замовника, а частина у оператора. Ідеальний варіант приватної хмари - хмара, яка є розгорнутою на території організації, що обслуговується та контролюється її співробітниками.

Перевагою моделі приватної хмари перед іншими є можливість здійснення більш детального контролю над ресурсами і розширені можливості їх конфігурації. Крім того, приватні хмари є ідеальним рішенням у разі роботи з конфіденційною інформацією [5]. Але, водночас це може вважатися основним недоліком, оскільки підприємство має можливість самостійно встановити і підтримувати хмарні сервіси. У цьому випадку витрати, пов'язані зі створенням та експлуатацією, лягають на компанію і можуть перевищувати цінність інформації, що обробляється.

Приватним випадком такої інфраструктури можна вважати хмару спільноти (Community cloud) , призначену для спільного використання

обчислювальної потужності приватної хмари кількома організаціями або особами, які поділяють одні інтереси та вимоги до політики безпеки та керівних документів [6].

Публічна хмара – це хмарна інфраструктура, яка знаходиться у повному розпорядженні постачальника послуг та призначена для вільного використання широкою публікою. Вся відповідальність за встановлення, обслуговування та підтримання працездатності покладається на провайдера. Клієнти, що використовують можливості даного типу інфраструктури, не мають доступу до управління та конфігурування системи та фактично оплачують лише використовувані ресурси у вигляді обчислювальної потужності та абонентського доступу. Абонентом цього типу сервісів може стати як компанія, так і індивідуальний користувач.

Основними перевагами публічних хмар є можливість масштабування сервісами і доступність вартості для рядового користувача, з допомогою оплати лише споживаних ресурсів [7].

При цьому головним недоліком даної інфраструктури є найменша можливість конфігурування системи з боку клієнтів, так як дані функції зазвичай є стандартизованими і ґрунтуються на випадках, що часто запитуються користувачами випадках. Також не варто забувати про те, що оскільки споживачі не мають можливості управління інфраструктурою, інформація, яка потребує підвищених вимог безпеки та нормативного контролю, не може перебувати в загальнодоступній хмарі через обмежену відповідальність постачальника в цьому питанні.

Гібридна хмара - це інфраструктура, що є поєднанням загальнодоступних і приватних моделей хмар. У цьому типі систем обов'язки з управління розподіляються між провайдером та клієнтом. Даний сервіс надає послуги, що стосуються як приватних, так і публічних хмар [8]. Найбільшу популярність цей тип сервісу має в організацій, де підвищений рівень активності у певні періоди часу. Завдяки ньому компанії можуть відправляти частину інформації, що не має цінності, на публічну хмару під час ресурсозатратної обробки

важливих відомостей, а також надавати через неї доступ користувачам до ресурсів підприємства, що знаходяться в приватній хмарі. Чудово розрахована хмара даного типу дозволяє обробляти інформацію, що має підвищені вимоги до безпеки, так і більш незначну.

При цьому головним недоліком даної інфраструктури є найменша можливість конфігурування системи з боку клієнтів, так як дані функції зазвичай є стандартизованими і ґрунтуються на випадках, що часто запитуються користувачами. Також не варто забувати про те, що оскільки споживачі не мають можливості управління інфраструктурою, інформація, яка потребує підвищених вимог безпеки та нормативного контролю, не може перебувати в загальнодоступній хмарі через обмежену відповідальність постачальника в цьому питанні.

Так як подібна концепція є новим рішенням у сфері хмарних обчислень, фундаментальним недоліком гібридних хмар є складність створення оптимального рішення щодо реалізації цієї інфраструктури. Втілення у життя ускладнюється як зміною взаємодії між приватним і загальнодоступним компонентами, і налаштуванням отримання послуг із різних джерел та об'єднанням їх у єдиний блок [9].

Після розгляду переваг та недоліків трьох існуючих моделей розгортання хмарної інфраструктури можна виділити модель приватної хмари, як найбільш безпечну та яка забезпечує більше можливостей для конфігурації системи.

Наступним кроком реалізації хмарного сервісу є вибір моделі обслуговування, яку надає провайдер хмарних послуг.

1.3 Моделі обслуговування

На сьогоднішній день є кілька моделей обслуговування із боку постачальника [9]. Їх прийнято розділяти на три групи залежно від типу послуг (Таблиця 1). Подібні моделі іноді називають шарами хмари, хоча вважається, що вони відображають будову інформаційних технологій загалом.

Таблиця 1.1 – Моделі обслуговування

IaaS	PaaS	SaaS
Програми	Програми	Програми
Середовище виконання	Середовище виконання	Середовище виконання
СУБД	СУБД	СУБД
Безпека	Безпека	Безпека
Сервер	Сервер	Сервер
Зберігання данних	Зберігання данних	Зберігання данних
ЦОД	ЦОД	ЦОД
ОС	ОС	ОС

Інфраструктура як послуга (Infrastructure as a Service – IaaS) – це модель надання клієнтам набору фізичних ресурсів обробки даних, таких як сервери, мережеве обладнання та пристрої зберігання. При цьому споживач не може контролювати хмарну інфраструктуру, проте може керувати операційними системами, системами зберігання, розгорнутими програмами та деякими мережевими компонентами. У цьому випадку захист платформ і програм клієнт забезпечує самостійно, а на провайдера покладається організація захисту.

Приватним випадком інфраструктури як послуги є апаратне забезпечення послуги (Hardware as a Service – HaaS), де користувач отримує обладнання, на основі якого розгортає власну інфраструктуру з використанням найбільш відповідного програмного забезпечення.

Ця модель часто має на увазі використання методів віртуалізації, тому її основною перевагою можна вважати зниження інвестицій в обладнання. А до недоліків відноситься бізнес-ефективність та продуктивність яка значною мірою залежить від можливостей постачальника. Також є ймовірність, що будуть потрібні потенційно великі довгострокові витрати та додаткові заходи щодо забезпечення безпеки.

Платформа як послуга (Platform as a Service – PaaS) – це модель надання користувачеві інфраструктури для розміщення створених або придбаних додатків, таких як програмне забезпечення, месенджер, сховище даних без можливості керування інфраструктурою в цілому. В даному випадку клієнт не може конфігурувати базову структуру хмарного сервісу, але йому дається доступ до налаштування параметрів хостингу і встановлених програм. Забезпечення безпеки інформації, що зберігається та обробляється, також покладається на користувача.

Надані програми можуть функціонувати як у центрах обробки даних компанії, так і безпосередньо у хмарі завдяки технології віртуалізації. Окремими випадками PaaS є такі послуги як:

1) Робоче місце як послуга (Workplace as a Service - WaaS) - модель надання компаніям стандартизованого програмного забезпечення, доступного для всіх співробітників незалежно від апаратної частини, що використовується.

2) Дані як послуга (Data as a Service - DaaS) - модель надання користувачеві дискового простору, який може бути використаний для зберігання особистої інформації або збереження резервних копій системи та додатків.

3) Безпека як послуга (Security as a Service – SaaS) – модель надання користувачеві можливості розгортання системи безпеки підприємства, пов'язаної з використанням веб-сервісів.

Основними перевагами даної моделі є відсутність необхідності переплачувати провайдерам за ресурси, що не використовуються, а також плавність розгортання додатків і набір засобів для створення, тестування та виконання програмного забезпечення. Недоліки полягають у відсутності контролю та управління фізичною та віртуальною інфраструктурою хмари та забезпечення безпеки з боку постачальників.

Додаток як послуга (Software as a Service – SaaS) – це модель надання користувачеві програмного забезпечення, розгорнутого на віддалених серверах постачальника, доступ до якого здійснюється за допомогою Інтернету.

Програмне забезпечення в цьому випадку оплачується за фактом використання або надається на безоплатній основі, але з умовою можливості отримання прибутку від реклами.

Надані програми можуть бути доступні за допомогою різних клієнтських пристроїв, всесвітньої павутини або мобільних додатків. Відповідальність клієнта полягає лише у збереженні параметрів доступу та виконанні рекомендацій провайдера щодо безпечних налаштувань додатків.

Перевагою даної послуги є зручний доступ до роботи через інтернет або мобільний додаток, а недоліки – неможливість управління інфраструктурою хмари, низька швидкість обробки даних у реальному часі та заборона на обробку даних на сторонніх сервісах.

Тенденції розвитку технологій говорять про те, можливо незабаром подібний поділ не матиме сенсу, оскільки з'являться постачальники, що надають і програмну та апаратну частину, а також функції управління інфраструктурними та платформними елементами, зібрані від різних постачальників, але об'єднані в єдину хмарну систему.

1.4 Хмарні сервіси у період пандемії

Хмарні сервіси довели свою ефективність під час пандемії, коли компанії швидко переводили свою діяльність у дистанційний режим. Винесені уроки вплинули на формування IT-стратегії на 2021 рік, відмічається в дослідженні Gartner. Попри невелике скорочення загальних витрат на IT компанії продовжать інвестувати кошти в хмарні сервіси.

В результаті пандемії припинилися суперечки, чи є публічна хмара операційною моделлю для бізнесу, наголошують у Gartner. Тож аналітики прогнозують, що використання хмар розширюватиметься. У 2024 році на хмарні сервіси буде припадати 14,2% світових корпоративних витрат на IT. Для порівняння: зараз цей показник складає лише 9,1%. За прогнозом аналітиків Gartner найбільший ріст у 2021 році припаде на IaaS (інфраструктура як сервіс)

– 26,6%. При цьому SaaS (ПЗ як сервіс) з об’ємом витрат у $117,7 млрд залишиться найбільшим сегментом ринку хмарних сервісів. Послуги PaaS набиратимуть все більшої популярності, адже межі між різними хмарними сервісами продовжать розмиватися, компанії стануть частіше пропонувати свої продукти у вигляді пакетів.

Багато задач, які мігрують у хмару, переписуються та стають нативно-хмарними. Тоді як раніше вони переносилися у незмінному вигляді. Нині компанії використовують такі технології, як контейнери, штучний інтелект та машинне навчання у якості елементів DevOps, створюють конвеєри безперервної інтеграції/доставки ПЗ (CI/CD).

Навіть у разі ефективності вакцини і завершення пандемії хмари будуть надалі посилювати та трансформувати IT. Значна частина працівників у різних компаніях хочуть мати можливість і надалі працювати віддалено, адже компанії переконалися, що це можливо. Це стимулюватиме подальший розвиток відповідних сервісів, покликаних забезпечити надійну, стабільну та безперебійну роботу у дистанційному режимі.

Спроби працювати виключно на власних майданчиках залишитися в минулому. Ідея створення масштабних власних ЦОДів починає відходити в минуле.

1.5 Висновки до першого розділу

Хмарні обчислення і “хмари” тісно увійшли у життя і щоденне використання комп'ютера, підключеного до мережі Інтернет не обходиться без них. Нові технології принесли багато нового, зокрема, зміни на IT-ринку та поява нових послуг, сервісів та платформ, які є основними для нових бізнес-моделей. Розвиток глобальної мережі, а також зростання споживання контенту, пов'язане також із бурхливим зростанням мобільної техніки зажадав від виробників створення нових масштабованих і гнучких систем, які б дозволили найкраще підлаштовуватися під зростаючі запити, а також надали нові шляхи

доставки контенту та побудови інфраструктур. Основні переваги "хмар", такі як масштабованість, мультитенантність, еластичність, а також, що дуже важливо, оплата за використання висувають їх на перший план. Це саме те, що потрібно ринку і як каже аналітика, попит на них буде зростати. Сьогодні на ринку "хмар" представлено досить багато гравців, які пропонують свої платформи. З них є і вільні (відкриті), які можна розвивати самостійно, у разі потреби розробки унікальної архітектури для розгортання інфраструктури. Деякі компанії використовують готові рішення, інші – розвивають свої. Боротьба за частку ринку буде посилюватися і в залежності від спектру пропонованих послуг він буде поділений між найбільшими гравцями. однак кожна з них має зробити вибір. Багато хто хоче отримати все і одночасно, "під ключ", а саме, готову інфраструктуру, без необхідності розробки та перенесення. Це означає, що ті компанії, які пропонують готові послуги, будуть мати більше клієнтів. Хмарні обчислення є найбільш швидким трендом світового ринку.

Кожна хмарна модель пропонує певні функції та можливості. Коли бізнес має набір конкретних завдань і розуміння переваг різних типів хмарних сервісів, простіше вибрати відповідний.

Підкреслимо плюси кожної з моделей:

Рішення IaaS дають практично повний контроль за готовою інфраструктурою, що дозволяє організації створити стек технологій, повністю адаптований до потреб бізнесу.

Підприємства, які вже мають деякі ресурси та IT-відділ, можуть вибрати сервіси PaaS: готова платформа допоможе компаніям розробляти індивідуальні рішення, які легше інтегрувати з існуючими робочими процесами.

Послуги SaaS дозволяють підприємствам економити гроші: клієнтам не потрібно самостійно займатися розробкою та підтримкою програмного забезпечення. Хоча, на перший погляд, ці моделі схожі, SaaS, PaaS та IaaS надають різні рівні послуг. Однак у будь-якому випадку, хмарні рішення знімають роботу з клієнтів та допомагають економити час.

2 ОСНОВНІ ЗАГРОЗИ ТА МЕТОДИ ЇХ УСУНЕННЯ

2.1 Загрози

Наразі хмарні обчислення є прогресивним методом оптимізації IT інфраструктури. Але, незважаючи на всі позитивні моменти, це тягне за собою низку проблем, пов'язаних як із труднощами збереження конфіденційності оброблюваних даних, так і з областю відповідальності провайдерів. В інтересах підтримки своєї репутації провайдери багато уваги приділяють забезпеченню безпеки даних від можливого проникнення ззовні. Але не завжди така ж увага приділяється юридичним аспектам використання даних самим постачальником. А в окремих випадках (наприклад, у загальнодоступних сервісах хмарного зберігання, таких як Google тощо) , навіть безпосередньо вказується той факт, що постачальник має право використовувати будь-яку отриману від користувача інформацію так, як вважатиме це за потрібне.

За основу забезпечення фізичної безпеки береться суворий контроль фізичного доступу до серверів та інфраструктури мережі. На відміну від фізичної безпеки, мережна безпека в першу чергу являє собою побудову надійної моделі загроз, що включає захист від вторгнень і брандмауер.

В даний час не один хмарний провайдер не може гарантувати, що всі ресурси хмарного сервісу, що їм надається, і в ньому немає неконтрольованих віртуальних машин, не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари. Тому важливо знати, з якими небезпеками може зіткнутися користувач під час використання хмарних систем.

2.1.1 Загроза віртуалізації

Як згадувалося раніше, хмарні середовища можна розділити на три категорії відповідно до трьох моделей розгортання. Але у всіх найважливіша роль відводиться технології віртуалізації. Вимоги до безпеки хмарних систем мало відрізняються від вимог, що висуваються до роботи звичайних центрів

обробки даних. Однак перехід до віртуалізації може спричинити виникнення нових типів загроз. Тому розглянемо основні можливі загрози у системі хмарних обчислень [10].

В даний час ця обчислювальна платформа має такі потенційно слабкі сторони:

— Обміни даних між різними віртуальними машинами або між віртуальною машиною та хостом із застосування спільних використовуваних дисків, комутаторів або віртуальних локальних мереж (VLAN) та спільно використовуваної підсистеми вводу-виводу або кешу.

— Стандартних драйверів, які емулюють апаратні засоби.

— Уразливосьті в гіпервізора, що дозволяє виконувати довільний код на хості з привілеями гіпервізора, що дає зловмиснику можливісті керувати усіма віртуальними машинами та самим хостом.

— Руткіти, що дозволяють отримати управління системою та вносити зміни в роботу гіпервізора з метою впровадження та виконання шкідливого коду.

— «Втеча з віртуальної машини» – вразливість, що надає програмі вихід із віртуальної машини та можливість взаємодії з операційною системою, а також безмежний доступ до хоста завдяки ресурсам, що спільно використовуються.

— Атаки типу «відмова в обслуговуванні», які полягають у виведенні з ладу однієї віртуальної машини, якою надалі відбувається напад інші машини, запущені з неї на одному хості.

Першим кроком до заходів захисту щодо цих загроз є розуміння робочого середовища. Якщо дані мають бути захищені відповідно до законів, стандартів або галузевих норм, то до забезпечення безпеки повинен бути застосований відповідний підхід. І в цьому випадку найбільш популярним є рішення, засноване на моделі приватного або гібридного хмарного сервісу, в якому всі дані, що потребують безпеки, розташовуються на території підконтрольного відомства, і знаходяться безпосередньо під охороною організації-

правовласника.

Наступним етапом є перевірка постачальника хмарних послуг на предмет надійності та з'ясування заходів, що вживаються для захисту найбільш уразливих місць у системі, особливо щодо гіпервізора.

Гіпервізор є одним із головних елементів віртуальних системи. Його основна функція полягає у розподілі ресурсів між віртуальними машинами, забезпечуючи тим самим роботу кількох операційних систем та ізолюючи їх один від одного. І виведення гіпервізора з ладу може призвести до того, що одному користувачеві будуть доступні не тільки фізичні ресурси та пам'ять іншого, а й можливість перехоплення мережного трафіку.

2.1.2 Втрата та витік даних

З моменту появи даних у хмарі, кошти компанії із запобігання витоку даних вважаються недійсними, оскільки вже не можуть допомогти у захисті конфіденційності цих даних. При цьому, в більшості випадків, компанія навіть не має можливості прямого контролю за збереженням безпеки своїх даних не тільки в загальнодоступній хмарі, але і в таких моделях надання послуг як програмне забезпечення як сервіс (SaaS) і платформа як сервіс (PaaS) » [11].

Для запобігання витоку інформації в хмарних сервісах існує безліч рішень та готових продуктів, але вони в основному спрямовані на забезпечення цілісності та доступності даних та не підходять для реалізації захисту. Крім того, ці рішення не підходять для середовищ, де користувач не має доступу до управління інфраструктурою.

Тим часом основою запобігання витоку інформації є застосування довірених систем зберігання та транспортування даних. Насамперед, від постачальника потрібно використання високонадійного шифрування як під час зберігання, і під час передачі матеріалу. Також необхідно мати завірену угоду, в якій будуть чітко визначені ролі провайдера та споживача у забезпеченні безпеки даних та умови надання сервісу. Крім цього, контракт повинен містити вимогу до постачальника послуг хмари про знищення даних, що зберігаються

на постійних носіях, перед визволенням до пул. У той же час згідно з вимогами стандарту PCI DSS, необхідною є належним чином налаштований міжмережевий екран Web-додатків для захисту останніх від різноманітних атак, а також проведення випробування проникненням, щоб перевірити захист від небажаного доступу всіх додатків, що використовуються компанією.

Зрештою, на боці організації потрібна наявність відповідних політик безпеки. Компанії, що побоюються витоку інформації, повинні мати чинні політики класифікації даних та встановлення стандартів щодо порядку поводження з даними різного рівня конфіденційності, які можуть бути абсолютно не призначеними для зберігання у хмарі.

2.1.3 Незахищені інтерфейси API

Для того, щоб клієнтам було зручно взаємодіяти з хмарними сервісами, постачальники послуг часто надають інтерфейси прикладного програмування (API) , які можуть бути застосовні для керування та моніторингу хмари. Тому більшою мірою безпека використання хмарних послуг залежить від того, як якісно захищені дані інтерфейси API.

Серйозними загрозами безпеці в цьому випадку є функції здійснення анонімного доступу, відкриті способи автентифікації та багаторазове використання паролів, а також застарілі засоби контролю доступу та авторизації [12].

Крім того, інтерфейси API, розроблені сторонніми організаціями для надання клієнтам додаткових можливостей використання хмарних сервісів, не завжди відповідають вимогам безпеки та піддаються детальному аналізу, або навіть можуть містити прихованіфункції передачі даних сторонній особі. А це підвищує рівень ризику порушення конфіденційності.

Щоб запобігти подібним проблемам, слід використовувати лише програми, надані або перевірені постачальником хмарних послуг, а також переконатися, що провайдер робить все необхідне для захисту таких інтерфейсів API. Крім того, організація повинна провести ретельну перевірку

засобів аутентифікації та доступу, щоб бути впевненою в наявності шифрування даних при передачі. А також переконатися, що використовуються лише заявлені у договорі інтерфейси програмування.

2.1.4 Викрадення та несанкціоноване використання облікових записів

До цього часу були розглянуті лише вразливості, боротьба з якими покладається на плечі постачальника послуг хмар. Але забезпечення безпеки облікових записів користувачів у рівній частці залежить від провайдера хмарних систем і від споживача. Тому що вразливість програмного забезпечення, що уможливлює перехоплення облікової інформації користувача, не є найпоширенішим способом крадіжки аутентифікаційних даних.

У більшості випадків, щоб оволодіти обліковою інформацією користувачів, зловмисники використовують атаки фішингу, шкідливе програмне забезпечення та соціальну інженерію. Оскільки люди часто використовують одні й ті ж ім'я користувача і пароль для отримання різних послуг, лише полегшують хакерам пошук автентифікаційної інформації. З моменту отримання зловмисником облікових даних користувача, під загрозу ставиться не тільки цілісність та конфіденційність даних, що зберігаються у хмарі, а й репутація компанії, оскільки правопорушники можуть використати отриману інформацію для атак на інші організації [13].

Тому від організації потрібне не тільки розуміння політик безпеки постачальника хмари, а й здійснення запобіжного моніторингу користування хмарними сервісами.

Також застосування політик з сторони компаній, що передбачають використання унікальних облікових даних для входу у систему та надійності паролю, допомагає запобігти вразливості, пов'язані з багаторазовим користанням інформацією користувачем. Зменшити ймовірність атак такого типу допомагають методи двофакторної аутентифікації.

2.1.5 Загрози з боку інсайдерів

Як правило, компанії витрачають дуже багато коштів на встановлення систем захисту із розмежуванням доступу користувачам та перевірку благонадійності співробітників. Але коли йдеться про дії персоналу з боку постачальника хмарних послуг та про те, як регламентовані їхні дії, прозорість процесів та процедур, є недостатньою.

Передача управління послугами постачальнику хмарних послуг означає відсутність у клієнта ставлення до тому, хто має доступ (фізичний і віртуальний) до ресурсів організації. Інформація про контроль співробітників, аналіз та дотримання політик безпеки, так чи інакше, не є доступною для користувачів. А в той же час можливість роботи із засекреченою інформацією є дуже привабливою для хакерів та корпоративних шпигунів, оскільки отримання контролю над хмарним сервісом пропонує зловмиснику такі конфіденційні дані, як обсяг продажів та прибуток компанії, які можуть бути продані їм з незначною часткою ризику виявлення або взагалі без такого.

Основним заходом захисту від діяльності з боку постачальника послуг є поінформованість про те, які заходи контролю співробітників здійснюються провайдером, а також які дії будуть вжиті у разі порушення захисту та витоку інформації. Якщо терміни або процес оповіщення є неприйнятними, слід шукати іншого постачальника послуг.

2.2 Методи захисту

Після розгляду існуючих загроз у сфері хмарних обчислень можна виділити кілька найбільш поширених рішень проблем, що виникають. Проаналізувавши опубліковану з цього питання інформацію та спираючись на методи захисту, обрані організацією Cloud Security Alliance (CSA), було виділено чотири методи забезпечення безпеки інформації в середовищі хмарних технологій: шифрування, захист даних під час передачі, автентифікація, ізоляція користувачів.

2.2.1 Захист даних під час передачі

Основною відмінністю хмарних сервісів від звичайних центрів обробки даних є зручність доступу користувача до ресурсів програми у будь-який момент, з будь-якого місця та з будь-якого пристрою, що має доступ до Інтернету. Але, крім окремих користувачів, до хмарної системи можуть підключати свою локальну інфраструктуру цілі компанії. При цьому і ті, й інші повинні бути абсолютно впевнені у безпечній доставці своїх даних до сервісу хмар. Тому розглянемо можливі способи та варіанти безпечного доступу з двох сторін.

Підключення кінцевих користувачів до хмарних сервісів

Для підключення окремих користувачів в даний час є кілька варіантів підключення до хмарних сервісів, що відрізняються один від одного не лише настроюванням та встановленням, але й зручністю використання. Це підключення за допомогою RDP-клієнта, RemoteApp, Веб-доступу, Remote access VPN, VPN site-to-site, DirectAccess та VDI [14].

1) Підключення за допомогою віддаленого робочого столу (RDP-клієнт)

Віддалений робочий стіл – це інструмент віддаленого доступу до робочого місця, створений на основі пропрієтарного протоколу прикладного рівня RDP (Remote Desktop Protocol) . На даний момент існує безліч клієнтів для найбільш популярних операційних систем, за допомогою яких користувач підключається до віддаленого робочого стола і може запускати розгорнуті на сервері терміналів програми, а також може конфігурувати параметри доступу та системи. Крім того, RDP клієнт підтримує функцію обміну даними між локальним комп'ютером і віддаленим робочим столом.

1) Віддалені програми служб терміналів (RemoteApp)

Це рішення є різновидом розглянутого вище варіанта. Принципова відмінність полягає тільки в тому, що при доступі до віддаленого робочого столу користувач має доступ до цілої операційної системи та встановлених на ній програм, а RemoteApp призначений для доступу до конкретного додатку,

інтегрованого з робочою станцією користувача, але фактично знаходиться на віддаленому сервері. Засобами RemoteApp відбувається підключення до цього сервера, авторизація та запуск програми, створюючи видимість локально встановленої програми.

2) Веб-доступ до служб терміналів

Цей спосіб допомагає здійснити доступ як до віддаленого робочого столу, так і до окремої програми за допомогою браузера. Для цього необхідно авторизуватися на веб-сторінці постачальника послуги.

3) Підключення за VPN

VPN – це віртуальна приватна мережа, що дозволяє забезпечити кілька надійних інтернет-з'єднань, використовуючи різні засоби криптографії.

Існує два типи VPN-тунелів:

a. Remote access VPN – це захищений тунель, організований між додатком на комп'ютері клієнта та будь-яким пристроєм (наприклад, маршрутизатором) , розташованому у хмарі хостинг-провайдера. Для реалізації цього типу доступу користувачеві необхідно запустити ярлик VPN на своїй робочій станції та ввести свої вірчі дані. При успішній авторизації користувач потрапляє в мережу віртуального віддаленого офісу в хмарі і може використовувати ресурси так, якби він знаходився безпосередньо в офісі компанії.

b. Site-to-site VPN – це захищений тунель, організований між двома пристроями користувачів, розташованими в одній локальній мережі. Тому не потрібно встановлювати на комп'ютерах будь-яке спеціальне програмне забезпечення. Даний тип тунель застосовується, якщо кількість користувачів компанії, яким необхідний доступ до ресурсів файлового сервера, досить велика. У цьому випадку необхідно безпосередньо в офісі компанії додатково розгорнути VPN-сервер та реалізувати підключення Site-to-Site VPN на рівні VPN-сервера в хмарі та VPN-сервера в офісі компанії.

4) DirectAccess

Крім стандартних реалізацій VPN, існує технологія DirectAccess,

заснована на базі Microsoft. Вона дозволяє реалізувати можливість віддаленого доступу до ресурсів, розгортаючи тунель до сервера DirectAccess і завдяки ньому отримуючи доступ до всієї мережі. При цьому користувачеві не потрібно робити жодних додаткових дій. Навіть якщо зв'язок з Інтернетом буде втрачено на якийсь час, тунель самостійно відновиться.

5) VDI (віртуалізація робочих столів)

На сьогоднішній день віртуальна інфраструктура робочих столів (VDI, Virtual Desktop Infrastructure) реалізована на багатьох хмарних майданчиках корпоративних IaaS-провайдерів та дозволяє централізувати робочі станції користувачів на серверах віртуалізації, створивши при цьому єдину точку управління, розгортання та обслуговування. Для реалізації цієї технології з боку клієнта потрібна наявність інтернет-з'єднання та робочої станції. На практиці виділяється сервер у хмарі IaaS-провайдера, на який встановлюється гіпервізор, а на ньому розгортаються окремі віртуальні машини. На кінцевому пристрої користувача запускається програма-клієнт та відбувається підключення до інфраструктури.

Найчастіше багато дрібних і навіть середніх компаній не мають своєї локальної IT-інфраструктури, воліючи при цьому розгортання всіх необхідних для бізнесу рішень і сервісів у хмарі IaaS-провайдера. Такий підхід економічно виправданий, вигідний та зручний.

Існує кілька можливих варіантів підключення локальної інфраструктури компанії до IaaS-інфраструктури у хмарі:

— оренда виділеного каналу та підключення до хмари;

— прокидання свого кабелю до ЦОД;

— використання точок обміну трафіком.

Розглянемо кожен із варіантів докладніше.

1) Оренда виділеного каналу та підключення до ЦОД для доступу до хмари

В даний час дуже популярним є варіант з'єднання внутрішньої мережі замовника з мережею в хмарі IaaS-провайдера. Такий сценарій часто називають

гібридною хмарою, оскільки замовник має власні ресурси, а майданчик IaaS-провайдер надає тільки додаткову обчислювальну потужність. Фізично це рішення являє собою використання двох виділених каналів провайдера, що працюють в режимі автоматичного перемикання у разі падіння одного з них. Як правило, такий канал зв'язку надається на основі власної оптоволоконної мережі провайдера з можливістю підписання угоди про рівень обслуговування, що регламентує гарантії дотримання технічних характеристик каналу. Безперечним плюсом даного методу є його відносна дешевизна порівняно з варіантом, коли замовник прокидав би свій власний кабель. При цьому провайдер, як правило, дає гарантію високої щільності покриття, а також безпеки та надійності каналів, що орендуються, включаючи можливість резерву ємності при зростанні каналу.

2) Прокидання свого кабелю до ЦОД

Внутрішня мережа замовника та мережа у хмарі IaaS-провайдера також можуть бути з'єднані прокидом власного кабелю клієнта до необхідного центру обробки даних. Такий метод є менш економічним порівняно з попереднім. Тому компанії, які потребують високошвидкісних телекомунікаційних каналів, у більшості випадків віддали б перевагу раніше розглянутому нами варіанту: оренді каналів або викупу оптичних волокон у вже прокладеній лінії зв'язку. Однак організації, які пред'являють підвищені вимоги до безпеки та експлуатаційних показників каналу зв'язку, змушені зробити вибір на користь прокладання власної оптичної лінії.

3) Використання точок обміну трафіком

Цей спосіб прокладання каналу від організації до IaaS-провайдер є здешевленою версією методу, розглянутого раніше. Його суть полягає в тому, що кабель прокладається не до центру обробки даних хмарного провайдера безпосередньо, а до комутаційного обладнання, розміщеного IaaS-провайдером на майданчиках, де розміщуються точки обміну трафіком. Точка обміну трафіком – це місце, де здійснюється прямий обмін трафіком між інтернет-операторами, минаючи мережі сторонніх провайдерів. Усі її учасники мають

можливість побудувати з'єднання один з одним, задіявши лише один порт. Завдяки прямим пірингам, через точку обміну можна зменшити завантаження зовнішніх каналів і скоротити час передачі даних між учасниками. Для безпечної обробки даних обов'язковою умовою є їх передача, що шифрується. З метою захисту даних у публічній хмарі використовується тунель віртуальної приватної мережі (VPN), яка зв'язує клієнта та сервер для отримання публічних хмарних послуг. Як засіб передачі даних у публічних хмарах VPN – з'єднання використовує загальнодоступні ресурси, такі як Інтернет. Процес заснований на режимах доступу із шифруванням за допомогою двох ключів на базі протоколу Secure Sockets Layer (SSL).

Протоколи SSL і VPN як опція підтримують використання цифрових сертифікатів для аутентифікації, з допомогою них перевіряють ідентифікаційна інформація іншої сторонни, ще до початку передачі даних. Такі цифрові сертифікати зберігаються на віртуальних жорстких дисках у зашифрованому вигляді, і використовуються вони лише після того, як сервери керування ключами перевірить ідентифікаційну інформацію та цілісність системи. Отже, такий взаємозалежність дозволить передавати дані лише тим хмарним серверам, що пройшли попередню перевірку [15].

Зашифровані дані під час передачі повинні бути доступні лише після аутентифікації. Дані не вдасться прочитати або внести зміни до них, навіть у разі доступу через ненадійні вузли. Такі технології досить відомі, алгоритми та надійні протоколи AES, TLS, IPsec давно використовуються провайдерами.

2.2.2 Аутентифікація

Вирішення проблеми безпеки користувача у хмарних обчисленнях часто залежить від вибраних механізмів автентифікації. Найпопулярнішим методом вирішення досі є пароль. Більшість клієнтів вибирають для пароля слова, які легше запам'ятати, імена та номери телефонів. Для отримання подібного пароля зловмиснику достатньо зробити перебір за словником.

Альтернативою цього методу захисту вважається двофакторна

автентифікація. На даний момент найбільш поширена технологія двофакторної аутентифікації, яка використовує одноразові паролі (One Time password) . Саме такий тип паролів можуть генеруватися або по спеціальних програмах, додатковими пристроями, або сервісами, з пересилкою користувачеві SMS і діють протягом обмеженого часу. Суть цього методу – пароль дійсний лише для одного входу до системи, при кожному наступному запиті доступу потрібен новий пароль. Нині є кілька реалізацій технології одноразових паролів. Для її використання можуть застосовуватись такі засоби, як:

c. Віртуальні токени (Mobile-OTP) ;

d. Апаратні токени (Aladdin eToken PASS) ;

e. Аутентифікація через SMS (RSA Mobile) ;

f. Автентифікація One Time Matrix (OTM) .

Розглянемо докладніше кожен із способів реалізації технології одноразових паролів.

1) Принцип роботи віртуальних токенів.

На пристрій користувача встановлюється спеціальна програма – програмний токен. Працює на принципі двофакторної автентифікації. Після інсталяції програми, користувачеві потрібно пройти процес реєстрації свого пристрою на сервері організації, до ресурсів якої потрібно здійснити доступ. Наступний крок для генерування одноразового пароля користувач вводить PIN-код у додатку на своєму пристрої. Отриманий одноразовий пароль, користувач може використовувати для входу в систему.

2) Принцип роботи апаратних токенів.

Як правило, апаратний токен являє собою компактний пристрій, призначений для ідентифікації його власника і спрощення аутентифікації. Для генерування одноразового пароля має існувати синхронізація між токеном клієнта та сервером автентифікації. Основними недоліками токенів цього типу є обмежений термін служби, можливість розсинхронізації та втрати.

3) Принцип роботи технології аутентифікації через SMS.

Основна відмінність хмарної інфраструктури полягає в тому, що доступ

користувача до системи не повинен бути територіально обмеженим. Саме тому на перший план виходить використання мобільних пристроїв для отримання одноразових паролів, які сьогодні є практично у кожного. У найпростішому випадку одноразовий пароль буде згенеровано спеціальним сервером аутентифікації та надіслано в SMS на мобільний телефон користувача після введення правильного статичного пароля на сторінку доступу до хмарного сервісу. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації також рекомендується використовувати протокол LDAP (Lightweight Directory Access Protocol) та мову програмування SAML (Security Assertion Markup Language) .

4) Принцип роботи технології аутентифікації One Time Matrix.

Одноразова матриця (One-Time Matrix, OTM) — це різновид технології одноразових паролів, яка не потребує додаткових пристроїв для використання. В основі технології доступу OTM лежить використання одноразового пароля, який формується шляхом розпізнавання заданого шаблону (матриці) та послідовного зчитування цифр, що відображаються в осередках шаблону. Під шаблоном розуміється послідовність довільно обраних користувачем осередків одноразової матриці, яку користувач повинен зберегти в системі, і використовується як еталонний автентифікатор. Набір цифр у комірках матриці генерується випадковим чином при кожній спробі автентифікації, що виключає можливість повторного використання одного й того ж коду доступу.

Найбільш перспективною зараз є технологія біометричної аутентифікації. Це форма аутентифікації, у якій фізіологічні риси людини використовуються для ідентифікації або автентифікації користувача. На даний момент біометрична автентифікація ще не набула належного поширення у зв'язку з технологічною складністю системи.

2.2.3 Шифрування

Шифрування – це один з найефективніших способів захисту даних. Провайдер, що надає доступ до даних, повинен шифрувати інформацію

користувача, що зберігся в центрах обробки даних, а також у разі відсутності необхідності безповоротно видаляти. При шифруванні даних найважливішим питанням є розташування ключів. Їх зберігання на хмарному сервері є безглуздим, оскільки кожен, хто має доступ до хмарних серверів або шаблонів, може отримати доступ до ключа та розшифрувати дані. Фізичне введення ключа замінюється запитом, який надсилає хмарний сервер зовнішньому джерелу — серверу управління ключами (Key Management Server, KMS). Хорошою альтернативою є встановлення сервера KMS у локальному ЦОД або як зовнішню послугу в іншого сервіс-провайдера [16].

2.2.4 Ізоляція користувачів

При використанні хмарних обчислень периметр мережі компанії може розмитися або зовсім зникнути. Це призводить до того, що захист кожного користувача визначає загальний рівень захищеності. Але важливо не лише надати користувачам безпечний спосіб обробки даних, а й захистити інформацію. У тому числі і від інсайдерів. Корпоративний firewall — основна властивість для впровадження політики IT безпеки та розмежування сегментів мережі, що не можуть вплинути на сервери, розміщений у хмарних середовищах. Тому важливо, щоб віртуальні мережі були розгорнуті із застосуванням таких технологій, як VPN (Virtual Private Network) , VLAN (Virtual Local Area Network) та VPLS (Virtual Private LAN Service) [17].

Також провайдери можуть ізолювати дані користувачів один від одного за рахунок зміни коду в єдиному програмному середовищі. Саме той цуй підхід має ризики, пов'язані з певною небезпекою знайти дірку в нестандартному коді, що допомагає отримати доступ до даних. У разіпомилки у коді,користувач отримає доступ до інформації іншого користувача.

Безпека не завжди забезпечується лише захистом. Вона може бути досягнута також певними організаційними правилами поведінки та взаємодії об'єктів та професійнальної підготовки персоналу. Конфіденційність інформації – це принцип аудиту, у тому, що аудитори зобов'язані забезпечувати

збереження документів, одержуваних чи складених ними під час аудиторської діяльності, і немає права передавати ці документи чи його копії яким би то не було третім особам, або розголошувати усно, які у них відомості без згоди власника економічного суб'єкта. За винятком випадків, передбачених законодавчими актами.

2.3 Висновки до другого розділу

У цій роботі проведено аналіз основних загроз інформаційній безпеки та існуючих методів захисту від їх у хмарних системах. На основі проведеного аналізу показано, що найбільш небезпечними є атаки на віртуальну структуру хмарної системи. Також наведено класифікацію, на підставі якої можливе подання аналізу методів захисту із описом їх використання.

У ході роботи було розібрано такі поняття як,втрата та витік даних, методи захисту, та інформаційна безпека. У нашому випадку, під «інформаційною безпекою» ми розумітимемо ступінь захисту інформації та інфраструктури, що її забезпечують існування, від небажаного (випадкового та спеціального) впливу, яке надалі здатне завдати неприйнятної шкоди учасникам інформаційних відносин.

Виділено такі типи загроз для інформації:

— Штучні:

• ненавмисні загрози,

• навмисні небезпеки.

— Природні:

• неправильне зберігання,

• крадіжка комп'ютерів та носіїв,

• форс-мажорні обставини,

• пожежі, повені, урагани, удари блискавок та інші стихійні лиха та явища, що не залежать від людини.

Для забезпечення інформаційної безпеки використовують три основні

методи:

— правові,

— організаційно-технічні

— економічні.

Також,можна виділити основні методи захисту забезпечення безпеки інформації в середовищі хмарних технологій:

— шифрування

— захист даних під час передачі,

— автентифікація, ізоляція користувачів.

Формування нових стандартів, серед яких надання захисту хмарних технологій, зараз вважається пріоритетною місією, а подальше формування хмарних рішень буде реалізовуватися спільно з появою нових, найбільш надійних методів захисту інформації.

3 ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ХМАРНИХ ВЕБ-СЕРВІСІВ

3.1 Постачальники хмарних сервісів та методи захисту

На сьогоднішній день головними постачальниками «хмари» є Amazon, Google і Microsoft.

Google Drive – хмарне сховище від компанії Google, яке дозволяє зберігати свої дані на серверах і ділитися ними в Інтернеті. Усі користувачі Google Drive отримують не більше 15 Гбайт вільної пам'яті. Google самостійно може вирішити, скільки виділити місця під пошту і під важливі файли. Робота з файлами Google Drive відбувається прямо в браузері.

Google Docs –хмарний пакет, що включає в себе текстовий, табличний і редакційну службу для створення презентацій. Сервіс можна використовувати без встановлення на комп'ютер. Таблиці і документи, які створюються користувачем, зберігаються на комп'ютер користувача або на сервера Google. Це одна з основних переваг програми, тому що, доступ до даних, які вводяться може здійснюватися з пристрою, під'єднаного до інтернету. Особисті документи користувача захищені паролями.

Google App Engine – це сервіс для хостингу сайтів та web-додатків які зберігаються на серверах Google. Користувачу надається: 1 Гб дискового простору, 10 Гб трафіку і 2000 операцій надсилання електронної пошти. Додатки, які працюють на базі App Engine написані на Python, Java або Go. Користувачу надається можливість вибрати набір API для сервісів сховища datastore API (BigTable) акаунтів Google, а також набір API для завантаження даних по URL, електронної пошти і т.д.

Конкурентом платформи Google є аналогічні сервіси від Amazon, у яких є можливість розміщувати веб-програми і файли, використовуючи свою інфраструткру. На відміну від багатьох звичайних розміщень програм на віртуальних машинах, платформа App Engine тісно інтегрована з додатками і накладає на розробників деякі обмеження. Amazon Storage Service – це сервіс

зберігання об'єктів, що пропонує найкращі в галузі показники продуктивності, масштабованості, доступності та безпеки даних. Клієнти будь-якої величини та з будь-якої промислової галузі можуть зберігати та захищати необхідний обсяг даних для практично будь-якого прикладу використання. Вигідні класи сховища та прості у використанні інструменти адміністрування дозволяють оптимізувати витрати, організувати дані та точно налаштувати обмеження доступу відповідно до потреб бізнесу чи законодавчих вимог.

У березні 2012 року компанія Nasuni провела досвід, протягом якого по черзі передавала масивний об'єм даних (12 Тб) з одного хмарного сервісу в інший. В експерименті брали участь найбільш рейтингові хмари: Amazon S3, Windows Azure і Rackspace. На подив дослідників, швидкість передачі даних сильно відрізнялася в 43 залежності від того, яка хмара приймала дані. Найкращий показник швидкості запису даних виявився у Amazon S3, передача даних з двох інших сервісів займала всього 4-5 годин, в той час як передача даних в Rackspace зайняла трохи менше тижня, а в Windows Azure – 40 годин.

Amazon Elastic Compute Cloud (Amazon EC2) – веб-сервіс, що надає обчислювальні потужності в хмарі. Він дає користувачам повний контроль над обчислювальними ресурсами, а також доступне середовище для роботи. Amazon EC2 дозволяє користувачам створити Amazon Machine Image (AMI), який буде містити їх застосування, бібліотеки, дані і пов'язані з ними конфігураційні параметри, або використовувати заздалегідь налаштовані шаблони образів для роботи Amazon S3. Amazon EC2 надає інструменти для зберігання AMI. Amazon S3 надає безпечне, надійне і швидке сховище для зберігання образів.

Microsoft SkyDrive – інтернет-сервіс зберігання файлів з функціями файлообміну, створений і керований компанією Microsoft. Сервіс SkyDrive дозволяє зберігати до 7 ГБ інформації (або 25 ГБ для користувачів, які мають право на безкоштовне оновлення) у вигляді стандартних папок. Користувачі можуть переглядати, завантажувати, створювати, редагувати і обмінюватися документами Microsoft Office (Word, Excel, PowerPoint і OneNote)

безпосередньо в веб-браузері. Присутній віддалений доступ до комп'ютера, який працює під управлінням Windows. Windows Azure – платформа хмарних сервісів, розроблена Microsoft. Реалізує моделі PaaS і IaaS. Платформа надає можливість розробки і виконання програм і зберігання даних на серверах, розташованих в розподілених центрах даних. Windows Azure Compute – компонент, який реалізує обчислення на платформі Windows Azure, надає середовище виконання на основі рольової моделі. Windows Azure Storage – компонент сховища, що надає сховище з можливістю масштабування. Не має можливості використовувати реляційну 44 модель і є альтернативою (або доповнює рішенням) SQL Databases (SQL Azure) – масштабованою «хмарною» версією SQL Server. Windows Azure Fabric – за своїм призначенням є контролером і ядром платформи, виконуючи функції моніторингу в реальному часі, забезпечення відмовостійкості, виділення потужностей, розгортання серверів, віртуальних машин і додатків, балансування навантаження і управління обладнанням. Майже всі (приблизно 90%) із постачальників хмарних сервісів надають користувачам наступні послуги безкоштовно:

1. Безкоштовний обсяг сховища – 2 і більше ГБ.

2. Автоматична синхронізація даних, котрі зберігаються між кожним пристроєм, які мають підключення до хмарного сервісу. Відпадає необхідність у використанні зовнішнього пристрою (CD / DVD-накопичувачі, Flash-диск) для того, щоб перенести дані на інший пристрій (планшет, 49 смартфон, ПК, ноутбук і т.д.) . При підключенні пристрою до мережі Інтернет, актуальна версія даних буде автоматично завантажена на. Завдяки цій функції користувач економить багато часу – можна швидко продовжити роботу над поточним завданням, змінивши місце знаходження та обладнання.

3. Забезпечується безпека даних, що зберігаються у "хмарі". Весь трафік що йде між клієнтом і "хмарою" піддається шифруванню (використовується, як мінімум, протокол SSL, а в деяких випадках RSA + AES) , що дуже сильно ускладнює перегляд інформації, що передається сторонніми особами. Тому рівень безпеки роботи з даними вище, ніж, наприклад, при використанні

звичайного листа по електронній пошті. Деякі сервіси хмарного зберігання (SpiderOak, Wuala) надають шифрування даних не лише при передачі, але і при зберіганні в "хмарі".

4. Надання можливості публічного доступу через Інтернет до матеріалів, що зберігаються в хмарі, для будь-якої людини. Досить відправити колезі посилання на потрібний файл, щоб він зміг ознайомитися, наприклад, з результатами вчорашньої наради або новими матеріалами поточного проекту.

5. Надійність даних що зберігаються. Постачальники хмарних рішень при зберіганні даних на своїх сервісах використовують надмірність, що саме по собі гарантує надійність. Додатково до цього, на будь-якому з пристроїв, що підключені до "хмари", зберігається, як мінімум одна актуальна копія даних.

3.2 Порівняння хмарних сервісів для зберігання даних

Як було відзначено раніше, існує достатня кількість онлайн-сервісів зберігання даних. Для зручності вибору характеристики найпопулярніших з цих сервісів зведені в табл. 3.1.

Критерієм вибору тих сервісів, які потрапили в порівняльну таблицю, була в тому числі мінімізація вартості ліцензії, тому що це є важливим фактором при виборі хмарних послуг в економічному суспільстві. Тому в табл.3.1 включені дані тільки про безкоштовні сервіси тих чи інших постачальників послуг.

Таблиця 3.1 – Характеристики хмарних сервісів

Назва	Безкоштовний об`єм, ГБ	Шифрування даних	Операційні системи які підтримуються	Загальний доступ	Колективна робота	Постачальник послуги
Drop box	2	SSL, AES256	Windows, Mac OS, Linux, Android, iOS	Так	Ні	Dropbox Inc
Spider Oak	2	RSA2048, AES256	Windows, Mac OS, Linux, Android, iOS	Так	Ні	SpiderOak Inc
One Drive	5	SSL, AES128	Windows, Mac OS, And	Так	Так	Microsoft
Box	10	SSL, AES256	Windows, Android, BlackBerry, iOS, WebOS, Phone	Так	Так	Box

Підводячи підсумки короткого порівняння "хмарних" сервісів зберігання даних, можна зробити наступні висновки:

– будь-які сучасні онлайн-сервіси пропонують достатню кількість дискового простору для зберігання документів і матеріалів користувача;

– майже всі сервіси підтримують сучасні алгоритми шифрування при передачі даних;

– якщо необхідна конфіденційність зберігання даних, то найвищий рівень захисту при передачі і зберіганні інформації в хмарі забезпечує SpiderOak (шифрування даних відбувається на клієнтському пристрої) ;

– для спільної роботи над документами і електронними таблицями прекрасно підійде сервіс Box.

3.3 Порівняння хмарних сервісів для колективних проектів

Хмарні сервіси для управління проєктами допомагають відслідковувати роботу учасників команди, розподіляти завдання між ними, визначати їхню пріоритетність тощо. До цієї категорії сервісів відносять Microsoft Teams, Asana, Trello, Jira та інші.

Хмарні сервіси для колективної розробки програмних продуктів дають змогу користувачам спільно працювати над кодом, керувати версіями тощо. До таких сервісів відносять: GitHub, Bitbucked, GitLab, Phabricator, Beanstalk та ін.

Обираючи хмарні сервіси для управління проєктами, необхідно врахувати можливість формування груп, постановки завдань учасникам команди, пріоритезації задач, комунікації між учасниками команди, організації відеозв’язку та організації спільної роботи в реальному часі, планування та збереження результатів командної роботи, вбудовування додаткових сервісів (див.табл.3.3).

Одним із важливих різновидів проєктів у ході підготовки ІТ-фахівців є проєкти з колективної розробки програмних продуктів, саме тому ще зі студентської лави важливо готувати студентів до виконання таких проєктів, розвивати в них необхідні для цього професійні та особистісні навички. Обираючи хмарні сервіси для колективної розробки програмних продуктів, необхідно звертати увагу на можливість спільної роботи над кодом, відстеження помилок, обговорення коду з іншими учасниками команди, управління версіями коду та інтеграції додаткових сервісів, наявність репозиторію, вікі та редактора коду тощо. Для того, щоб хмарні сервіси колективної розробки програмних продуктів допомагали керувати проєктами, в них необхідно інтегрувати додаткові сервіси. Саме тому можливість такої інтеграції є одним з основних критеріїв, за яким здійснюється порівняльна характеристика хмарних сервісів для колективної розробки програмних продуктів.

Таблиця 3.2 – Критерії хмарних сервісів для колективної роботи

Критерій	GitHub	Bitbucket	DeployBot	Phabricator
Можливість спільної роботи над кодом	+	+	+	+
Можливість відстеження помилок	+	+	-	+
Наявність стрічки активності	-	+	-	+
Наявність репозиторію	+	+	-	+
Можливість управління версіями коду	+	+	+	-
Наявність редактора коду	+	+	+	+
Можливість обговорення коду	+	-	-	+
Наявність вікі	+	+	+	+
Можливість інтеграції додаткових сервісів	+	+	+	+

3.4 Висновки до третього розділу

Таким чином, виходячи з перерахованого вище, можна зробити висновок про те, що хмарні системи та хмарні обчислення слід розглядати як новий підхід, який дасть потужний імпульс подальшому розвитку інформаційних технологій та обчислювальних наук. Багато в чому полегшилося життя всіх людей: від пересічного користувачі мережі “Інтернет” до найбільших компаній, що базують свою роботу на зберіганні та обробці інформації. Від звільнення пам'яті пристрою, шляхом синхронізації даних із хмарою, до обробки великих обсягів даних та заробляння на цьому грошей.

Порівняння різних хмарних систем, їх переваги та недоліки наочно показало прагнення IT-компаній удосконалювати свої продукти та бути конкурентоспроможними.

На сьогоднішній день хмарні системи є багатофункціональними помічниками у житті. Тенденції розвитку хмарних систем та великих центрів даних говорять про швидкий перехід до нової ери інформаційних технологій. Інформація стає ще доступнішою; її пошук та обробка стають ще швидше.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИУАЦІЯХ

4.1 Облаштування і безпека серверних приміщень

Використання хмарних веб-сервісів на сьогоднішній день несе в собі як позитивні, так і негативні моменти. З одного боку, використання хмарних сервісів здатне надати неабияку кількість обчислювальних ресурсів для компанії, а з іншого змушує облаштувати серверне приміщення. Для продуктивної і безпечної роботи серверних приміщень існує ряд вимог, також, це стосується і операторів які працюють на цьому робочому місці.

Приміщення, де розміщені робочі місця операторів, потрібно оснастити вогнегасниками. Виняток становлять ті, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер). Приміщення, де розміщені робочі місця операторів сервера загального призначення, варто обладнати системою автоматичної пожежної сигналізації та засобами пожежогасіння (пп. 1.15, 1.16 п. 1 розд. III Правил № 65).

Щоб запобігти витоку інформації у серверних приміщеннях через побічні випромінювання і наводи, а також порушенню її цілісності через вплив зовнішніх електромагнітних полів, слід використовувати екрановані шафи, сейфи (клас опору до злому не нижче II), кабіни. Можна використовувати екрановані шафи (сейфи) для розміщення серверів баз даних, прикладних задач тощо. Екрановані шафи (сейфи) повинні мати сертифікат відповідності, виданий Державною службою спеціального зв’язку та захисту інформації України.

Серверні приміщення рекомендовано обладнати у приміщеннях без вікон. Це не поширюється на старі приміщення, які реконструюють, та на неекрановані приміщення, у яких установлені екрановані шафи (сейфи). Щоб запобігти несанкціонованому доступу до серверних приміщень, обладнайте їх двері автоматизованою системою доступу або кодовим замком. А також не менше ніж двома рубежами охоронної сигналізації, кожний із яких

підключений окремими кодами до приймально-контрольних приладів, установлених на посту охорони банку та/або охорони банку.

Серверні приміщення слід обладнати системою оповіщення під час пожежі та автоматичною системою газового пожежогасіння. Внутрішні поверхні цих приміщень облицюйте пожежобезпечними матеріалами, що відповідають санітарно-гігієнічним вимогам. Через повітропроводи системи вентиляції та канали для введення кабелів і комунікацій до серверних приміщень можуть проникнути сторонні речовини, щоб цього не допустити, обладнайте їх вогнетривкими пробками чи вогнетривкими аварійними заслінками. Також обладнайте централізованою або окремими системами припливно-витяжної вентиляції та автоматичного кондиціювання повітря з очищенням від пилу. Вони мають забезпечувати у приміщенні температуру повітря 18-24 ºС і відносну вологість не більше ніж 60% у будь-яку пору року.

Серверні приміщення та приміщення електронних архівів розміщуйте у віддалених один від одного кінцях будівлі. Якщо є змога, ці приміщення розміщуйте у внутрішній частині будівлі або з боку внутрішнього двору.

У кожному серверному приміщенні забезпечте ведення журналу на паперових носіях. У ньому зазначають:

- дату та час відчинення і зачинення кімнати;
- прізвища працівників, які відвідували кімнату;
- опис проведених робіт.

Фахівці, що забезпечують технічне обслуговування електротехнічних пристроїв серверного приміщення, є електротехнічним персоналом. Вони повинні мати ІІІ кваліфікаційну групу з електробезпеки. Присвоювати кваліфікаційну групу з електробезпеки особам, які працюють тільки з програмним забезпеченням, немає потреби. Адже ці особи є звичайними користувачами комп’ютерної техніки.

На підприємстві, де експлуатують електронно-обчислювальну техніку, мають розробляти інструкцію з охорони праці (відповідно до Положення про розробку інструкцій з охорони праці, затвердженого наказом

Держнаглядохоронпраці від 29.01.1998 № 9; НПАОП 0.00-4.15-98; п. 1.8 розд. I Правил № 65). Постає запитання: чи мають розробляти на підприємстві інструкцію з охорони праці для оператора (користувача) комп'ютерної техніки?

Відповісти однозначно не можна. Є відомчі інструкції, пов'язані з використанням ЕОМ на виробництві: наприклад, була Інструкція щодо користування персональним комп'ютером (затверджена наказом Державної судової адміністрації України від 10.01.2004 № 1/04) та чинна Примірна інструкція з охорони праці під час експлуатації електронно-обчислювальних машин (затверджена наказом Міністерства доходів і зборів України від 05.09.2013 № 443).

ДСТУ не передбачають наявність для користувача комп'ютера інструкції з охорони праці під час роботи з ЕОМ. Вони передбачають інструкцію з експлуатування (користування) цією технікою.

Користувачі ЕОМ мають використовувати інструкцію з експлуатування, а для апаратури з під'єднанням з'єднувачем та призначеної для встановлення користувачем – інструкцію із встановлення (монтажу; п. 1.7.2 ДСТУ 4467-1:2005). Інструкція з охорони праці під час роботи з комп'ютером (комп'ютерною технікою) може бути як однією з інструкцій за видом робіт, якої має дотримуватися обслуговуючий персонал (обслуга) (прим. 3 до п. 1.7.2 ДСТУ 4467-1:2005).

Отже, інструкція з охорони праці для комп'ютерної техніки недоцільна з таких міркувань:

1. Сучасна ЕОМ є електротехнічним пристроєм загального призначення. Під час експлуатації ЕОМ найважливішим є питання електробезпеки. Тому інструкцією з охорони праці (поряд із інструкцією з пожежної безпеки та інструкцією з надання домедичної допомоги) має бути інструкція з електробезпеки. До неї варто включити вимоги електробезпеки під час експлуатації ЕОМ.

2. Робота на ЕОМ загального призначення не є роботою з підвищеною небезпекою. Програмне забезпечення не стосується теми охорони праці. Немає

потреби визначати в інструкції з охорони праці вимоги щодо улаштування робочого місця користувача ЕОМ. Адже організувати робоче місце користувача ЕОМ зобов'язаний роботодавець. Він має інформувати працівника про умови праці, небезпечні і шкідливі виробничі фактори на його робочому місці, які ще не усунуто, можливі наслідки їх впливу на здоров'я та про права працівника на пільги і компенсації за роботу в таких умовах. Також роботодавець має провести відповідний інструктаж та навчання з питань охорони праці.

4.2 Пожежна безпека в навчальних закладах

Відповідно до Правил пожежної безпеки України, затверджених постановою Міністерства освіти і науки від 15.08, та правил пожежної безпеки навчальних закладів України забезпечується пожежна безпека організацій і підприємств системи освіти України. 2016 № 974, зареєстрований в Міністерстві юстиції України 8 вересня 2016 року за номером 1229/29359.

Забезпечення пожежної безпеки в організаціях, на підприємствах системи освіти України здійснюється згідно з Відповідно з Правилами пожежної безпеки в Україні та Правилами пожежної безпеки для навчальних закладів та установ системи освіти України, затверджених наказом Міністерства освіти і науки України 15.08.2016 № 974, зареєстрованих в Міністерстві юстиції України 08.09.2016 за № 1229/29359, відбувається забезпечення пожежної безпеки в організаціях [47].

Основним завданням пожежної безпеки в навчальних закладах є захист і порятунок персоналу (дітей) від небезпечних пожежних факторів, які супроводжуються неконтрольованим горінням. При виникненні пожежі дії працівників, залучених до гасіння пожежі, повинні бути спрямовані на забезпечення безпеки особового складу, особливо дітей, а також їх евакуацію та рятування.

Усі заклади та установи перед початком навчального року мають бути затверджені відповідною комісією, у тому числі представниками органів

державного нагляду у сфері пожежної безпеки.

Діти у будинках дитячих дошкільних закладів повинні розміщуватися з таким розрахунком, щоб молодші розташовувалися на нижчих поверхах [48].

У багатоповерхових навчальних корпусах та школах-інтернатах класи повинні розміщуватися на нижніх поверхах. У кімнатах з дітьми підлога повинна бути прикріплена до кріплення (за винятком дитячих садків), мати помірну здатність до димоутворення. У дитячих закладах, які працюють цілодобово, літні дитячі дачі повинні бути оснащені чергуванням персоналу нічної служби. Зал очікування повинен забезпечувати телефонний зв'язок. Черговий повинен забезпечити: особовий склад на пожежі засобами індивідуального захисту органів дихання, комплектом ключів від евакуаційних дверей, переносним ліхтарем, а також знати кількість дітей, які ночують, їх місцезнаходження та зателефонувати до найближчого пожежно-рятувальної частини для передачі інформації.

У загальноосвітніх навчальних закладах (крім закладів для дітей з розумовими і фізичними вадами) можуть створюватися дружини молодих пожежників-рятувальників. У закладах та установах, де учні/першокласники проживають цілодобово, необхідно встановити обов'язки персоналу нічної служби, яка не має права спати під час зміни. Зал очікування повинен забезпечуватися телефонним зв'язком. Черговий персонал повинен окремо оснастити фільтруючими пристроями усіх дітей та обслуговуючий персонал на випадок пожежі, комплектом ключів від евакуаційних виходів і воріт, а також автомобільних під'їздів і установ для в'їзду на територію установи [49]. Не допускається в будівлях установ і в місцях:

- розміщувати людей на горищі та на поверсі (будівлі), не передбачаючи двох евакуаційних виходів;
- перепланувати ділянку без урахування будівельних норм і правил;
- установлювати ґрати та пристрої на вікнах приміщень де перебувають учасники навчально-виховного процесу, а саме: сходових клітках, у коридорах, холах та вестибюлях Якщо ґрати все таки встановлені (кабінет

інформатики, інші приміщення з обладнанням, що має матеріальну цінність), вони повинні розсуватися, зніматися або розкриватися, під час перебування в цих приміщеннях вони мають бути відчиненими;

- знімати дверні полотна в отворах, що з'єднують коридори зі сходовими клітками, та двері евакуаційних виходів;
- використовувати для опалення нестандартні (саморобні) нагрівальні пристрої;
- користування прилади для приготування їжі, крім спеціально обладнаних приміщень;
- захаращувати шляхи евакуації;
- встановлення дзеркал та встановлення фальш-дверей на шлях евакуації;
- встановлювати перешкоди на шляху евакуації; пороги, виступи, поворотні двері, розсувні двері, підйомні двері та інші пристрої для евакуації;
- при наявності людей у будівлі проводити електрозварювання та інші види пожежонебезпечних робіт;
- використовувати для освітлення свічки та гасові лампи та ліхтарі;
- використовувати відкритий вогонь для нагрівання труб систем опалення, водопостачання, каналізації тощо (для цього використовується гаряча вода, пару або гарячий пісок);
- зберігати використані обтиральні матеріали на робочому місці, в шафах, зберігати їх у кишенях робочого одягу;
- підключати до джерела живлення електроприлади без нагляду [50].

При належному виконанні всіх вимог ризик пожежі набагато зменшується. Навіть в випадку виникнення пожежі виконання вимог дозволяє набагато легше проводити евакуацію та мінімізувати наслідки пожежі.

4.3 Висновки до четвертого розділу

Було проаналізовано та розглянуто облаштування і норми безпеки в серверних приміщеннях. Також було розглянуто пожежну безпеку, та заборонені дії в навчальних закладах які можуть призвести до пожежі.

ВИСНОВКИ

В даний час хмарні засоби обчислення набули активного поширення як серед організацій, що потребують додаткової обчислювальної потужності, так і серед простих людей, які бажають спростити процес обробки та зберігання даних. Але разом із зростанням користувачів збільшилася і кількість виявлених уразливостей цього методу обробки даних. Як і будь-які інші засоби обробки даних, хмарні послуги мають свої переваги та недоліки.

Виділяють кілька переваг, пов'язаних із використанням хмарних технологій:

— Доступність.

Доступ до інформації, що зберігається в хмарному сервісі, може отримати будь-яка людина, яка має у своєму розпорядженні комп'ютер, планшет або будь-який мобільний пристрій, підключений до Інтернету.

— Мобільність.

Користувач не має постійної прихильності до одного робочого місця. Обробка інформації може проводитися з будь-якої точки світу зі швидкістю, що дорівнює швидкості інтернет-з'єднання користувача.

— Економічність.

Однією з важливих переваг є знижена витратність використання хмарних сервісів у порівнянні зі стандартними центрами обробки даних, оскільки в даному випадку у користувача немає необхідності купувати дорогі комп'ютери та програмне забезпечення, а також він звільняється від необхідності наймати спеціаліста з обслуговування локальних IT-технологій.

— Оренда.

Користувач має право отримувати лише необхідні пакети послуг із фактичною оплатою споживаної потужності та не переплачувати за непотрібні функції.

— Гнучкість.

Усі необхідні ресурси надаються провайдером автоматично.

— Висока технологічність.

Провайдери прагнуть надати клієнтам все більші обчислювальні потужності, які можна використовувати для зберігання, аналізу та обробки даних. Тому ця галузь активно розвивається нині.

— Надійність.

Надійність, яку забезпечують сучасні хмарні обчислення, набагато вища, ніж надійність локальних ресурсів, бо лише невелика кількість підприємств здатна дозволити собі повноцінний центр обробки даних та забезпечити йому належний утримання та безпеку.

Незважаючи на всі позитивні відгуки, існує й низка недоліків хмарних технологій. Згідно з дослідженнями аналітичної фірми IDC, багато компаній, в першу чергу, пов'язують з «хмарними» сервісами великі проблеми щодо безпеки. А незалежна дослідницька організація Portio Research лише підтвердила це, вказавши конкретні цифри: 68% опитаних керівників європейських IT-компаній, з метою безпеки, відмовляються використовувати хмарні технології. Це пов'язано з тим, що надійність, своєчасність отримання та доступність даних, розташованих у хмарному сховищі, дуже залежить від багатьох проміжних параметрів, таких як: канали передачі даних на шляху від клієнта до платформи, якість роботи інтернет-провайдера клієнта, доступність хмарного сервісу даний час. Але, незалежно від цього, більшість експертів дотримуються думки, що переваги даної технології переважують її недоліки.

Залежно від потреб клієнтів, надаються кілька моделей реалізації хмарних технологій. Найбезпечнішою з них є модель приватної хмари, а найбільш уразливою – модель публічної хмари. Також хмари поділяються за моделями обслуговування. Кожна з них має свої переваги і недоліки і вибирається користувачем виходячи з цілей, що переслідуються. Серед індивідуальних клієнтів найбільшого поширення набула модель обслуговування SaaS. Зараз все більше компаній пропонують свої додатки на основі даної моделі. Але водночас ця послуга з обробки інформації є найменш безпечною.

Відповідно до поставлених завдань у цій роботі були розглянуті існуючі

моделі загроз у хмарних обчисленнях та протестовані можливі заходи щодо підвищення безпеки файлів користувача. Методи автентифікації та розмежування доступу не були розглянуті через те, що вони не є доступними для пересічного користувача.

Через стрімкий розвиток хмарної інфраструктури варто очікувати появи незабаром універсальних методів забезпечення безпеки даних. Але на сьогоднішній день виділення найбільш оптимального методу захисту не є можливим, тому що до кожного типу послуги повинен бути застосований індивідуальний підхід відповідно до переслідуваних цілей замовників хмарних сервісів.

ПЕРЕЛІК ДЖЕРЕЛ

1. Arif Mohamed. A history of cloud computing. http://www.computerweekly.com/feature/A-history-of-cloud-computing
2. Peter M. Mell, Timothy Grance NIST Definition of Cloud Computing https://www.nist.gov/node/568586
3. SoCC 10: Процедури 1st ACM симпозіум на Cloud computing / Hellerstein, Joseph M. - NY: ACM, 2019. - ISBN 978-1-4503-0036-0.
4. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. - L.: Springer, 2019. - 379 p.
5. Гребньов Є. Хмарні послуги. – М.: CNews, 2021. – 282с.
6. Глазунов С. Бізнес у хмарах. Чим корисні технології для підприємця. https://kontur.ru/articles/225.
7. Іванніков В.П. Звіт ІСПРАН «Хмарні обчислення в освіті, науці та держсекторі»/ІНІОН РАН. М., 2020
8. Бузов Г.А., Калінін СВ., Кондратьєв А.В. Захист від витоку інформації з технічних каналів: Навчальний посібник. - М. - Гаряча лінія - Телеком. - 2018.-416 с.
9. Лебідь С. Ст, Міжмережеве екранування: Теорія та практика захисту зовнішнього периметра, Видавництво Московського технічного університету ім. Баумана, 2020 р, 304 с.
10. Панасенко С.П. Алгоритми шифрування. Спеціальний довідник BHV-Санкт-Петербург, 2019. - 576с.
11. Туманов Ю.М. Захист серед хмарних обчислень шляхом верифікації програмного забезпечення на наявність деструктивних властивостей // Автореф. канд. дис., М: Вид-во НІЯУ «МІФІ», 2018. 20 с.
12. Грейс Вокер, «Основи хмарних обчислень», Довідник IBM, 2019р.
13. Іванніков В.П. Звіт ІСПРАН «Хмарні обчислення в освіті, науці та держсекторі»/ІНІОН РАН. М., 2020
14. Савченко О.П. Корпоративна база знань як ядро системи управління та

інформаційне забезпечення національного стратегічного проектування, інноваційного та технологічного розвитку ІНІОН РАН, 2020. С. 297-300

15. Розумніков С.В. Інтегральна модель оцінки ефективності та ризиків хмарних IT-сервісів для впровадження на підприємство // Фундаментальні дослідження. - 2019. - № 2-24. - С. 5362-5366.
16. Петренко С. Захищена віртуальна приватна мережа: сучасний погляд захисту конфіденційних даних / Світ Internet. - М.: № 2, 2001.
17. Бердник А. В. Порівняльний аналіз рішень з безпеки SaaS сервісу від компанії IBM та КРОК // Безпека інформаційного простору: збірник статей. Тюмень, 2021. С. 245-253.
18. Віхорєв З., Кобцев Р. Як визначити джерела угроз.//Открытые системи. - 2019. - №07-08.С.43.
19. Краковський Ю.М.: Інформаційна безпека та захист інформації. –М.; Ростов н/Д: Березень, 2020
20. 8 кроків до безпечних хмарних систем // Журнал «Information Security/Інформаційна безпека» № 1, 2019. – С. 28-29
21. Іванов М.А. Криптографічні методи захисту інформації в комп'ютерних системах та мережах. - М.: КУДИЦЬ-ОБРАЗ, 2020, - 368 с.
22. Панасенко С.П. Алгоритми шифрування. Спеціальний довідник BHV-Санкт-Петербург, 2021. - 576с.
23. Рябко Б. Я., Фіонов О.М. Основи сучасної криптографії для спеціалістів в інформаційних технологіях. - М: Науковий світ, 2020.
24. «Гігієнічні вимоги до персональних електронно-обчислювальних машин та організації роботи» (СанПіН 2.2.2/2.4.1340-03) ;
25. «Типова інструкція з охорони праці під час роботи на персональному комп'ютері» (ТОІ Р-45-084-01).
26. Бурлак Г.М. Безпека роботи на комп'ютері. Організація праці на підприємствах інформаційного обслуговування. - Навч. посібник. - М.: Фінанси та статистика, 2018. - 144 с.

27. C. Camara, P. Peris-Lopez, J.E. Tapiador, Security and privacy issues in implantable medical devices: a comprehensive survey, J. Biomed. Inform. 55 (2015) 272–289.
28. R. RlTawy, A.M. Youssef, Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices, IEEE Access 4 (2016) 959–979.
29. M. A. Rahman, A. T. Asyhari, S. Azad, M. M. Hasan, C. P. Munaiseche, M. Krisnanda, A cyber-enabled mission-critical system for post-flood re33 Journal Pre-proof sponse: Exploiting tv white space as network backhaul links, IEEE Access 7 (2019) 100318–100331.
30. Javaid, Mohd, and Ibrahim Haleem Khan. "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic." Journal of Oral Biology and Craniofacial Research 11.2 (2021): 209-214.
31. Otoom, Mwaffaq, et al. "An IoT-based framework for early identification and monitoring of COVID-19 cases." Biomedical Signal Processing and Control 62 (2020): 102149.
32. Guth, J.; Breitenbucher, U.; Falkenthal, M.; Fremantle, P.; Kopp, O.; Leymann, F.; Reinfurt, L. A detailed analysis of IoT platform architectures: Concepts, similarities, and differences. In Internet of Everything; Springer: Berlin/Heidelberg, Germany, 2018; pp. 81-101.
33. Uddin, M.Z.; Hassan, M.M.; Alsanad, A.; Savaglio, C. A body sensor data fusion and deep recurrent neural network-based behavior recognition approach for robust healthcare. Inf. Fusion 2020, 55,105-115.
34. Yang, Y.; Nan, F.; Yang, P.; Meng, Q.; Xie, Y.; Zhang, D.; Muhammad, K. GAN-based semi-supervised learning approach for clinical decision support in health-IoT platform. IEEE Access 2019, 7, 8048-8057.
35. Rubi, J.N.S.; Gondim, P.R.D.L. Interoperable Internet of Medical Things platform for e-Health applications. Int. J. Distrib. Sens. Netw. 2020,16,1550147719889591.

36. Nasajpour, M.; Pouriyeh, S.; Parizi, R.M.; Dorodchi, M.; Valero, M.; Arabnia, H.R. Internet of Things for current COVID-19 and future pandemics: An exploratory study. J. Healthc. Inform. Res. 2020, 4, 325-364.
37. Ting, D.S.W.; Carin, L.; Dzau, V.; Wong, T.Y. Digital technology and COVID-19. Nat. Med. 2020, 26, 459-461.
38. Ndiaye, M.; Oyewobi, S.S.; Abu-Mahfouz, A.M.; Hancke, G.P.; Kurien, A.M.; Djouani, K. IoT in the wake of COVID-19: A survey on contributions, challenges and evolution. IEEE Access 2020, 8,186821-186839.
39. Terroso-Saenz, F.; Gonzalez-Vidal, A.; Ramallo-Gonzalez, A.P.; Skarmeta, A.F. An open IoT platform for the management and analysis of energy data. Future Gener. Comput. Syst. 2019, 92,1066-1079.
40. Benammar, M.; Abdaoui, A.; Ahmad, S.H.; Touati, F.; Kadri, A. A modular IoT platform for real-time indoor air quality monitoring. Sensors 2018,18,581.
41. Mineraud, J.; Mazhelis, O.; Su, X.; Tarkoma, S. A gap analysis of Internet-of-Things platforms. Comput. Commun. 2016, 89, 5-16.
42. Das, S. A Machine Learning Model for Detecting Respiratory Problems using Voice Recognition. In Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 29-31 March 2019; pp. 1-3.
43. Cho, Y.; Bianchi-Berthouze, N.; Julier, S.J. DeepBreath: Deep learning of breathing patterns for automatic stress recognition using low-cost thermal imaging in unconstrained settings. In Proceedings of the 2017 Seventh International Conference on Affective Computing and Intelligent Interaction (ACII), San Antonio, TX, USA, 23-26 October 2017; pp. 456-463.
44. Subirana, B.; Hueto, F.; Rajasekaran, P.; Laguarta, J.; Puig, S.; Malvehy, J.; Mitja, O.; Trilla, A.; Moreno, C.I.; Valle, J.F.M.; et al. Hi Sigma, do I have the Coronavirus?: Call for a New Artificial Intelligence Approach to Support Health Care Professionals Dealing With The COVID-19 Pandemic. arXiv 2020, arXiv:2004.06510.
45. Anthes, E. Alexa, do I have COVID-19? Nature 2020, 586, 22-25.

46. SM, U.S.; Ganesan, R.; Katiravan, J.; Ramakrishnan, M.; Ruhin Kouser, R. Mobile application based speech and voice analysis for COVID-19 detection using computational audit techniques. Int. J. Pervasive Comput. Commun. 2020.
47. Deshpande, G.; Schuller, B. An Overview on Audio, Signal, Speech, & Language Processing for COVID-19. arXiv 2020, arXiv:2005.08579.
48. Rahman, Md Arafatur, et al. "Data-driven dynamic clustering framework for mitigating the adverse economic impact of Covid-19 lockdown practices." Sustainable Cities and Society 62 (2020): 102372.
49. M.A. Alzubaidi, M. Otoom, N. Otoum, Y. Etoom, R. Banihani, A Novel Computational Method for Assigning Weights of Importance to Symptoms of COVID-19 Patients, 2020. Under Review.
50. J. Medina, M. Espinilla, A.L. García-Fer´ nandez, L. Martínez, Intelligent multi-dose´ medication controller for fever: from wearable devices to remote dispensers, Comput. Electrical Eng. 65 (2018) 400–412.
51. Y. Umayahara, Z. Soh, K. Sekikawa, T. Kawae, A. Otsuka, T. Tsuji, A mobile cough strength evaluation device using cough sounds, Sensors 18 (2018) 3810.

ДОДАТКИ