

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут інформатики та радіоелектроніки
Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, назва факультету)

Кафедра захисту інформації
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти (освітній ступінь))

на тему "Дослідження та аналіз сучасних методів та засобів захисту
хмарних обчислень"

Виконав: студент 6 курсу, групи РТ-813м
спеціальності (напряму підготовки)

125 – Кібербезпека

(безпека інформаційних і комунікаційних
систем)

(код і назва напряму підготовки, спеціальності)

Хвостенко А.І

(прізвище та ініціали)

Керівник Романенко С.М.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

м.Запоріжжя
2018 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет
 (повне найменування вищого навчального закладу)

Інститут, факультет ІРЕ, ФРЕТ
 Кафедра захисту інформації
 Ступінь вищої освіти (освітній ступінь) магістр
 Спеціальність 125 Кібербезпека
(код і назва)
 Напрямок підготовки Безпека інформаційних і комунікаційних систем
(код і назва)

ЗАТВЕРДЖУЮ
 Завідувач кафедри захисту інформації,
проф., д.т.н., Карпуков Л.М.
 “ ” 2018 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Хвостенку Андрію Івановичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) дослідження та аналіз сучасних методів та засобів захисту хмарних обчислень

керівник проекту (роботи) Романенко Сергій Миколайович, канд. фіз.-мат. наук, доцент кафедри захисту інформації

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “7” листопада 2018 року №328

2. Строк подання студентом проекту (роботи) 5 грудня 2018

3. Вихідні дані до проекту (роботи). Перелік та опис хмарних обчислень. Основні загроз хмарам.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Дослідження послуг, переваг та недоліків хмарних технологій. Загрози хмарним технологіям та рішення по захисту від них. Ефективність захисту хмарних сервісів.

5. Перелік графічного матеріалу (зточним зазначенням обов'язкових креслень) Мультимедійна презентація до доповіді.

РЕФЕРАТ

ПЗ: 82 сторінок, 12 рисунків, 3 таблиць, 2 формул.

Об'єкт дослідження – сучасні хмарні сервіси.

Предмет дослідження – наявні вразливості та методи захисту хмарних обчислень.

Метою роботи є дослідження та аналіз сучасних методів та засобів що використовуються для забезпечення захисту в хмарних технологіях.

Одним з ключових факторів у розвитку нових технологій є забезпечення безпеки та надійної роботи система. Чим більш технологічна та функціональна система, тим більше вона містить вразливостей у собі. При недостатньому рівні захисту всіх компонентів сервісу, подальший розвиток та підвищення якості неможливі. Лише ретельний аналіз усіх можливих загроз та розробка ефективних засобів протидії атакам, може забезпечити конкурентоспроможність і подальший розвиток продукту на ІТ-ринку.

Проведена робота з дослідження вразливостей і можливих атак складових хмарних технологій. Розглянуто способи захисту хмарних сервісів, що використовують різні компанії. Запропоновано оптимальні хмарні сервіси для різних потреб користувача.

ЦОД, ХМАРНІ ТЕХНОЛОГІЇ, ПО, БЕЗПЕКА, ВРАЗЛИВОСТІ, АТАКА, ПРОТОКОЛ, ІНФРАСТРУКТУРА, РЕСУРСИ, СЕРВІС.

СПИСОК СКОРОЧЕНЬ

IT – Information Technology
ЦОД – центр обробки даних
ПО – програмне забезпечення
ПК – персональний комп'ютер
SaaS – Software as a Service
PaaS – Platform as a Service
IaaS – Infrastructure as a Service
DDoS – Distributed Denial of Service
DoS – Denial of service
DB – database
SDLC – software development lifecycle
SSL – Secure Sockets Layer
AES – Advanced Encryption Standard
TLS – transport layer security
IPsec – Internet Protocol Security
VPN – Virtual Private Network
VLAN – Virtual Local Area Network
VPLC – Virtual Private Local Service
API – application programming interface
URL – Uniform Resource Locator
AMI – Alternate Mark Inversion
SQL – structured query language
REST – Representational State Transfer
HTTP – Hyper Text Transfer Protocol
HTTPS – Hyper Text Transfer Protocol Secure
XML – Extensible Markup Language
NIST – National Institute of Standards and Technology
RSA – аббревіатура від прізвищ Rivest, Shamir и Adleman

CD – Compact Disc

DVD – Digital Video Disc

IoT – Internet of Things

ERM – Enterprise Resource Management

CRM – Customer Relationship Management

BPaaS – business process as a service

ГОСТ – ГОсударственный СТандарт

ПУЕ – Правила улаштування електроустановок

ССБТ – Система стандартів безпеки праці

НПАОП – нормативно-правові акти із охорони праці

ПБЕЕС – Правила безпечної експлуатації електроустановок

споживачів

ДСТУ – Державний стандарт України

ISO – International Organization for Standardization

ВДТ – Відеотермінал

КПО – коефіцієнт природної освітленості

ДБН – державні будівельні норми

ДСН – державні санітарні норми

URL – Uniform Resource Locator

DLP – Data Leak Prevention

ЗМІСТ

Вступ.....	9
1 Дослідження послуг, переваг та недоліків хмарних технологій	11
1.1 Історія і ключові фактори розвитку	11
1.2 Переваги хмарних обчислень.....	13
1.3 Недоліки хмарних обчислень.....	15
1.4 Види послуг що надаються хмарними системами.....	16
1.5 Класифікація хмарних сервіс	18
1.6. Розвиток хмарних технологій	21
2 Загрози хмарним технологіям та рішення по захисту від них.....	28
2.1 Загрози безпеки в публічній хмарі	28
2.2 Загрози хмарних обчислень і методи їх захисту	31
2.3 Атаки на хмари і рішення по захисту від них	35
2.4 Рішення щодо захисту від загроз безпеки	37
2.5 Майбутнє хмарних обчислень	38
3 Ефективність захисту хмарних сервісів.....	40
3.1 Постачальники хмарних сервісів та методи захисту які вони використовують.....	40
3.2 Порівняння хмарних сервісів для зберігання даних	48
3.3 Підвищення ефективності захисту хмарних сервісів	50
4 Економічна частина	53
4.1 Оцінка ефективності капіталовкладень в захист хмарних обчислень в умовах розвитку цифровізації економіки	53
4.2 Подвоєння числа гіпермасштабних ЦОД	54
4.3 Дані розвитку ринку хмарних технологій звіту IDC	55
4.4 Дослідження світового ринку публічних хмар компанією Gartner та IDC.....	57
4.5 Економічні ефекти використання хмарних технологій.....	62
5 Охорона праці та безпека у надзвичайних ситуаціях.....	64
5.1 Аналіз потенційних небезпек.....	64
5.2 Заходи щодо забезпечення безпеки.....	65
5.3 Заходи щодо виробничої санітарії та гігієни праці.....	68

5.4 Заходи з пожежної безпеки	71
5.5 Заходи безпеки у надзвичайних ситуаціях	73
Висновки	78
Список використаної літератури	80

ВСТУП

Актуальність теми досліджень. У сфері ІТ-технологій набуває все більшого поширення концепція використання віддалених (хмарних) ресурсів, які можуть замовляти і отримувати користувачі на вимогу (за передплатою). Рішення дозволяє економити кошти, так як ресурси оплачуються по факту їх фактичного споживання. У разі необхідності клієнт може отримати додаткові ресурси, запускаючи віртуальні машини і / або додатки, розташовані в хмарі або, навпаки, відмовитися від частини чи від усіх ресурсів, коли необхідність в їх використанні зникла. Для роботи з хмарею користувачеві не потрібно дорогого обладнання, так як комп'ютер користувача фактично використовується в якості терміналу, а всі ресурсомісткі обчислення проводяться на комп'ютерах що входять в хмарну інфраструктуру. Забезпечення цілісності даних їх конфіденційності та надання цілодобового доступу до них, є актуальними для великої кількості людей. Беручи до уваги високі темпи розвитку хмарних сервісів, постійне розширення ринку послуг та стабільно високого попиту на них, потреба в забезпеченні всебічної захищеності цього сегменту ІТ-технологій не втрачатиме своєї актуальності ще довгий час.

Для роботи з хмарею користувачам не потрібні високопродуктивні комп'ютери, однак підвищені вимоги пред'являються до технологій, що забезпечують передачу інформації від користувача до хмарних ресурсів і назад. Якість зв'язку має бути постійною і не змінюватися в часі більше, ніж на величину, що допускається користувачем і прописану в договорі на обслуговування.

З метою встановлення найбільш безпечних хмарних сервісів що пропонують більш вигідні умовами використання, було досліджено та проаналізовано сучасні хмарні сервіси і їх методи забезпечення безпеки.

Метою роботи є дослідження та аналіз сучасних методів та засобів що використовуються для забезпечення захисту в хмарних технологіях.

Об'єкт дослідження є рівень захисту сучасних хмарних сервісів.

Предмет дослідження є наявні вразливості та методи захисту хмарних обчислень.

Метою роботи є ознайомлення з темою дослідження та постановка задачі, вибір літератури, вивчення вразливостей сучасних хмарних сервісів, аналіз можливих загроз, шляхів їх реалізації то способів захисту від імовірних атак, знаходження оптимального сервісу шляхом порівняння.

У якості результату роботи буде надано порівняльна характеристика сучасних хмарних сервісів з вказаними методами захисту, що використовуються в них та запропоновано оптимальні рішення для користувача зважаючи на його поточні потреби.

Також будуть запропоновані рішення для підвищення ефективності захисту хмарних сервісів.

1 ДОСЛІДЖЕННЯ ПОСЛУГ, ПЕРЕВАГ ТА НЕДОЛІКІВ ХМАРНИХ ТЕХНОЛОГІЙ

1.1 Історія і ключові фактори розвитку

Вперше ідею того, що ми сьогодні називаємо хмарними обчисленнями була озвучена J.C.R. Licklider, в 1970 році. В ці роки він був відповідальним за створення ARPANET (Advanced Research Projects Agency Network). Його ідея полягала в тому, що кожна людина на землі може біти підключена до мережі, з якої вона буде отримувати не тільки дані але і програми. Інший вчений John McCarthy висунув ідею про те, що обчислювальні потужності будуть надаватися користувачам у вигляді послуги (сервісу). На цьому етапі, розвиток хмарних технологій було призупинено до 90-х років, після чого їх розвитку посприяв ряд факторів.

Розширення пропускної здатності Інтернету, в 90-ті роки не дозволило отримати значний стрибок у розвитку в хмарних технологіях, так як практично жодна компанія і технології того часу не були готові до цього. Однак сам факт прискорення Інтернету дав поштовх швидкому розвитку хмарних обчислень.

Однією з найбільш значущих подій в даній області була поява Salesforce.com в 1999 році. Дана компанія стала першою компанією що надала доступ до свого додатку через сайт, по суті ця компанія першою надала своє програмне забезпечення за принципом - програмне забезпечення як сервіс (SaaS).

Наступним кроком стала розробка хмарного веб-сервісу компанією Amazon в 2002 році. Даний сервіс дозволяв зберігати, інформацію і робити обчислення.

У 2006, Amazon запустила сервіс під назвою Elastic Compute cloud, як веб-сервіс який дозволяв його користувачам запускати свої власні додатки.

Сервіси Amazon EC2 і Amazon S3 стали першими доступними сервісами хмарних обчислень.

Інша віха в розвитку хмарних обчислень сталася після того, як компанія Google створила платформу Google Apps для веб-додатків в бізнес секторі.

Значну роль у розвитку хмарних технологій зіграли технології віртуалізації, зокрема програмне забезпечення, що дозволяє створювати віртуальну інфраструктуру.

Розвиток апаратного забезпечення сприяв не стільки швидкому зростанню хмарних технологій, а й доступності даної технології для малого бізнесу і індивідуальних осіб. Що стосується технічного прогресу, то значну роль в цьому зіграло створення багатоядерних процесорів і збільшення ємності накопичувачів інформації.

Хмарні обчислення (англ. Cloud computing) - технологія розподіленої обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс. Надання користувачеві послуг як Інтернет-сервіс є ключовим. Однак під Інтернет-сервісом не варто розуміти доступ до сервісу тільки через Інтернет, він може здійснюватися також і через звичайну локальну мережу з використанням веб-технологій.

З визначення та історії видно, що основою для створення і швидкого розвитку хмарних обчислювальних систем послужили великі інтернет сервіси, такі як Google, Amazon та ін, та технічний прогрес, що по суті говорить про те, що поява хмарних обчислень було всього лише справою часу. Розглянемо яким же чином розвиток перерахованих вище напрямків дозволив хмарним системам стати доступнішими.

Розвиток багатоядерних процесорів призвів до:

- збільшення продуктивності, при тих же розмірах обладнання;
- зниження вартості обладнання, як наслідок експлуатаційних витрат;

- зниження енергоспоживання хмарної системи, для більшості ЦОД це дійсно проблема при нарощуванні потужностей ЦОД.

Збільшення ємностей носіїв інформації, зниження вартості зберігання 1 Мб інформації дозволило безмежно (принаймні так позиціонують себе більшість «хмар») збільшити обсяги інформації, що зберігається і знизити вартість обслуговування сховищ інформації, значно збільшивши обсяги даних.

Розвиток технологій віртуалізації призвів до:

- створення програмного забезпечення що дозволяє створювати віртуальну інфраструктуру не залежно від кількості наданих апаратних ресурсів;
- легкого масштабування, нарощування систем;
- зменшення витрат на адміністрування хмарних систем;
- доступності віртуальної інфраструктури через мережу Інтернет.

Збільшення пропускної спроможності призвело до:

- збільшення швидкості роботи з хмарними системами зокрема віртуальний графічний інтерфейс і робота з віртуальними носіями інформації;
- зниження вартості Інтернет трафіку для роботи з великими обсягами інформації;
- проникнення хмарних обчислень в маси.

Всі перераховані вище фактори призвели до підвищення конкурентоспроможності хмарних обчислень в ІТ сфері.

1.2 Переваги хмарних обчислень

Доступність - хмари доступні всім, з будь-якої точки, де є Інтернет, з будь-якого комп'ютера, де є браузер. Це дозволяє користувачам (підприємствам) економити на закупівлі високопродуктивних, дорогих комп'ютерів. Також співробітники компаній стають більш мобільними так, як

можуть отримати доступ до свого робочого місця з будь-якої точки земної кулі, використовуючи ноутбук, нетбук, планшетник або смартфон. Немає необхідності в купівлі ліцензійного ПО, його налаштування і оновлення, ви просто заходите на сервіс і користуєтеся його послугами заплативши за фактичне використання.

Низька вартість - основні чинники що знизили вартість використання хмар:

- зниження витрат на обслуговування віртуальної інфраструктури, викликане розвитком технологій віртуалізації, за рахунок чого потрібен менший штат для обслуговування всієї ІТ інфраструктури підприємства;
- оплата фактичного використання ресурсів, користувач хмари платить за фактичне використання обчислювальних потужностей хмари, що дозволяє йому ефективно розподіляти свої грошові кошти. Це дозволяє користувачам (підприємствам) економити на покупці ліцензій до ПО;
- використання хмари на правах оренди дозволяє користувачам знизити витрати на закупівлю дорогого устаткування, і зробити акцент на вкладення грошових коштів у наладку бізнес процесів підприємства, що в свою чергу дозволяє легко почати бізнес;
- розвиток апаратної частини обчислювальних систем, в зв'язку з чим зниження вартості обладнання.

Гнучкість - необмеженість обчислювальних ресурсів (пам'ять, процесор, диски), за рахунок використання систем віртуалізації, процес масштабування і адміністрування "хмар" стає досить легким завданням, так як «хмара» самостійно може надати вам ресурси, які вам необхідні, а ви платите тільки за фактичне їх використання.

Надійність - надійність «хмар», особливо що знаходяться в спеціально обладнаних ЦОД, дуже висока так, як такі ЦОД мають резервні джерела живлення, охорону, професійних працівників, регулярне резервування даних, високу пропускну здатність Інтернет каналу, високу стійкість до DDOS атак.

Безпека - «хмарні» сервіси мають досить високу безпеку при належному її забезпеченні, однак при недбалому ставленні ефект може бути повністю протилежним.

Великі обчислювальні потужності - ви як користувач «хмарної» системи можете використовувати всі її обчислювальні можливості, заплативши тільки за фактичний час використання. Підприємства можуть використовувати цю можливість для аналізу великих обсягів даних.

1.3 Недоліки хмарних обчислень

Постійне підключення до мережі - для отримання доступу до послуг «хмари» необхідно постійне з'єднання з мережею Інтернет. Однак у наш час це не такий і великий недолік особливо з приходом технологій стільникового зв'язку 3G і 4G.

Програмне забезпечення та його кастомізація - є обмеження по ПО яке можна розгортати на «хмарах» і надавати його користувачеві. Користувач має обмеження в використовуваному ПО і іноді не має можливості налаштувати його під свої власні цілі.

Конфіденційність - конфіденційність даних, що зберігаються на публічних «хмарах» в даний час викликає багато суперечок, але в більшості випадків експерти сходяться в тому, що не рекомендується зберігати найбільш цінні для компанії документи на публічній "хмарі", так як в даний час немає технології яка б гарантувала 100% конфіденційність даних, що зберігаються.

Надійність - що стосується надійності інформації, що зберігається, то з упевненістю можна сказати, що якщо ви втратили інформацію збережену в "хмарі", то ви її втратили назавжди.

Безпека - "хмара" сама по собі є досить надійною системою, однак при проникненні на нього зловмисник отримує доступ до величезного сховища даних. Ще один мінус це використання систем віртуалізації, в яких у якості

гіпервізора використовуються ядра стандартних ОС такі, як Linux, Windows і ін., Що дозволяє використовувати віруси.

Вартість обладнання - для побудови власної хмари компанії необхідно виділити значні матеріальні ресурси, що не вигідно щойно створеним і малим компаніям.

1.4 Види послуг що надаються хмарними системами

Що стосується послуг, які надаються, то в даний час концепція хмарних обчислень передбачає надання наступних типів послуг своїм користувачам. Що стосується послуг, які надаються, то в даний час концепція хмарних обчислень передбачає надання наступних типів послуг своїм користувачам.

Все як послуга (Everything as a Service). При такому виді сервісу користувачеві буде надано все, від програмно апаратної частини і до управління бізнес процесами, включаючи взаємодію між користувачами, від користувача вимагається тільки наявність доступу в мережу Інтернет. На мій погляд, даний вид сервісу це більш загальне поняття по відношенню до нижченаведених послуг, які є більш приватними випадками.

Інфраструктура як послуга (Infrastructure as a service). Користувачеві надається комп'ютерна інфраструктура, зазвичай віртуальні платформи (комп'ютери) пов'язані в мережу. Які він самостійно налаштовує під власні цілі (рис1.1).



Рисунок 1.1– Інфраструктура як послуга.

Платформа як послуга (Platform as a service). Користувачеві надається комп'ютерна платформа, зі встановленою операційною системою можливо і з програмними засобами (рис 1.2).



Рисунок 1.2 – Платформа як послуга

Програмне забезпечення як послуга (Software as a service). Даний вид послуги зазвичай позиціонується як «програмне забезпечення на вимогу», це програмне забезпечення розгорнуте на віддалених серверах і користувач може отримувати до нього доступ за допомогою Інтернету, причому всі питання оновлення та ліцензій на дане програмне забезпечення регулюється

постачальником даної послуги. Оплата в даному випадку проводиться за фактичне використання програмного забезпечення (рис.1.3).



Рисунок 1.3 – Програмне забезпечення як послуга

Апаратне забезпечення як послуга (Hardware as a Service). В даному випадку користувачеві послуги надається обладнання, на правах оренди яке він може використовувати для власних цілей. Даний варіант дозволяє економити на обслуговуванні даного обладнання, хоча за своєю суттю мало чим відрізняється від виду послуги «Інфраструктура як сервіс» за винятком того що ви маєте голе обладнання на основі якого розгортаєте свою власну інфраструктуру з використанням найбільш підходящого програмного забезпечення.

Робоче місце як послуга (Workplace as a Service). В даному випадку компанія використовує хмарні обчислення для організації робочих місць своїх співробітників, налаштувавши і встановивши все необхідне програмне забезпечення, необхідне для роботи персоналу.

Дані як послуга (Data as a Service). Основна ідея даного виду послуги полягає в тому, що користувачеві надається дисковий простір, яке він може використовувати для зберігання великих обсягів інформації.

Безпека як сервіс (Security as a Service). Даний вид послуги надає можливість користувачам швидко розгорнути, продукти що дозволяють

забезпечити безпечне використання веб-технологій, безпеку електронного листування, а також безпеку локальної системи, що дозволяє користувачам даного сервісу економити на розгортанні та підтримці своєї власної системи безпеки.

1.5 Класифікація хмарних сервіс

В даний час виділяють три категорії «хмар»: публічні, приватні та гібридні.

Публічна хмара - це ІТ-інфраструктура що використовується одночасно безліччю компаній і сервісів. Користувачі даних хмар не мають можливості управляти і обслуговувати хмару, всю відповідальність з цих питань покладено на власника даної хмари (рис.1.4). Абонентом пропонуванних сервісів може стати будь-яка компанія і індивідуальний користувач.



Рисунок 1.4 – Інфраструктура публічної хмари.

Вони пропонують легкий і доступний за ціною спосіб розгортання веб-сайтів або бізнес-систем, з великими можливостями масштабування, які в

інших рішеннях були б недоступні. Приклади: онлайн сервіси Amazon EC2 і Simple Storage Service (S3), Google Apps / Docs, Salesforce.com, Microsoft Office Web.

Приватна хмара - це безпечна IT-інфраструктура, контрольована і експлуатована в інтересах однієї-єдиної організації. Організація може керувати приватною хмарою самостійно або доручити це завдання зовнішньому підряднику. Інфраструктура може розміщуватися або в приміщеннях замовника, або у зовнішнього оператора, або частково у замовника і частково у оператора (рис.1.5).



Рисунок 1.5 – Інфраструктура приватних хмар.

Ідеальний варіант приватної хмари це хмара розгорнута на території організації, що обслуговується і перебуває під контролем її співробітників.

Гібридна хмара - це IT-інфраструктура що використовує кращі якості публічної і приватної хмари, при вирішенні поставленого завдання (рис.1.6)

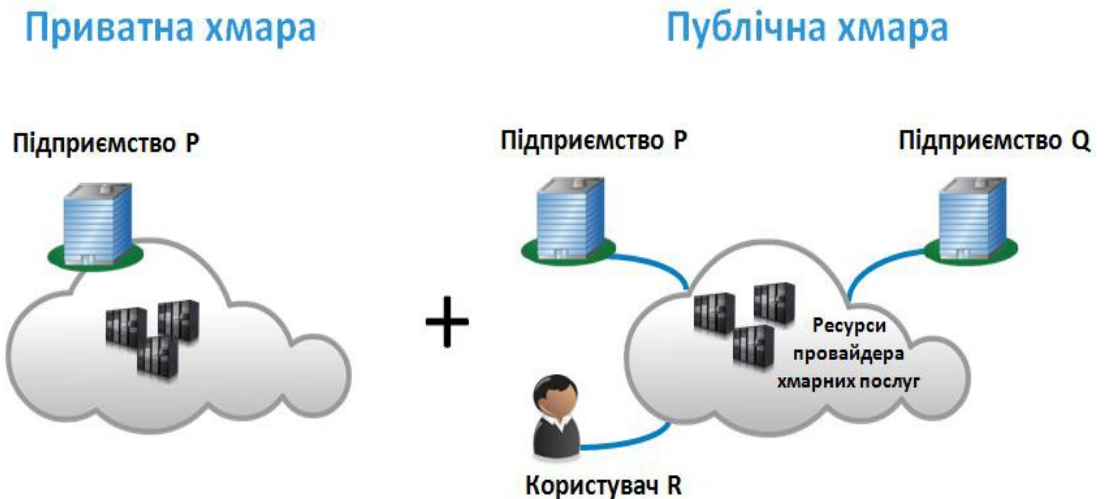


Рисунок 1.6 – Інфраструктура гібридної хмари.

. Часто такий тип хмар використовується, коли організація має сезонні періоди активності, іншими словами, як тільки внутрішня ІТ-інфраструктура не справляється з поточними завданнями, частина потужностей перекидається на публічну хмару (наприклад великі обсяги статистичної інформації, які в необробленому вигляді не являють цінності для підприємства), а також для надання доступу користувачам до ресурсів підприємства (до приватної хмари) через публічну хмару.

1.6. Розвиток хмарних технологій

За оцінками експертів потенціал хмарних обчислень дуже високий. На високому темпі розвитку хмарних технологій можна заробити працюючи в наступних напрямках:

- надання послуг хмарних обчислень - дана можливість доступна не всім компаніям, оскільки потрібні значні вкладення в побудову і розробку ЦОД.
- розробка ПО для побудови віртуальної інфраструктури - не слід забувати і про тих хто буде впроваджувати і налаштовувати це ПО, отже будуть потрібні фахівці в цій галузі.

- адміністрування хмар - будуть потрібні фахівці з адміністрування і консультування в сфері хмарних обчислень.
- апаратне забезпечення - компанії що займаються розробкою і проектуванням апаратного забезпечення для створення «хмар».
- проектування - дана сфера охоплює практично всі перераховані вище сфери починаючи від проектування ЦОД і закінчуючи проектуванням програмного забезпечення.

Раніше, щоб розгорнути який-небудь додаток, доводилося купувати і налаштовувати власні фізичні сервери. Такий підхід мав велику кількість недоліків, наприклад, якщо для нормальної роботи програми йому досить «півтора сервера», платити все одно доводилося за два - витрати на утримання і обслуговування інфраструктури виявлялися невиправдано високими.

Сьогодні у нас є такі сервіси, які дозволяють налаштувати віртуальний сервер і сховище даних під власні потреби. У цьому випадку витрати залежать від необхідної кількості обчислювальних (і інших) ресурсів - ви платите тільки за те, що використовуєте.

Коріння хмарних обчислень сягають високопродуктивних обчислень. У гонці країн з нарощування обчислювальної потужності взяли участь навіть такі великі компанії, як IBM і HP. «Однак інженери і дослідники швидко зрозуміли, що такий підхід погано масштабується, - говорить Прадіп Падала (Pradeep Padala), засновник ContainerX. - Тому почалися пошуки альтернативних способів проведення обчислень: почали розроблятися розподілені системи, що поєднують в собі потужності величезної кількості комп'ютерів».

З'явилися такі академічні проекти, як Condor - це розподілена мережа комп'ютерів, розгорнута в університеті Вісконсіна в Мадісоні. На сьогоднішній день там встановлено 350 настільних UNIX-станцій, які надають доступ для роботи користувачам з усього світу. Були й інші проекти, наприклад distributed.net і SETI @ home - на той момент ця ідея була

інноваційною, та й займатися пошуком позаземних цивілізацій теж досить цікаво.

Потім в моду увійшли грід-обчислення. Визначення грід-обчислень дуже близьке до того, що ми називаємо «обчислення як послуга».

Грід-обчислення (англ. Grid - решітка, мережа) - це форма розподілених обчислень, в якій «віртуальний суперкомп'ютер» представлений у вигляді кластерів, з'єднаних за допомогою мережі комп'ютерів, що працюють разом для виконання величезної кількості завдань (операцій, робіт). Ця технологія застосовується для вирішення наукових, математичних задач, що вимагають значних обчислювальних ресурсів. Грід-обчислення використовуються також в комерційній інфраструктурі для вирішення таких трудомістких завдань, як економічне прогнозування, сейсмоаналіз, розробка та вивчення властивостей нових ліків.

Грід з точки зору мережевої організації являє собою узгоджену, відкриту і стандартизовану середу, яка забезпечує гнучкий, безпечний, скоординований розподіл обчислювальних ресурсів і ресурсів зберігання інформації, які є частиною цього середовища, в рамках однієї віртуальної організації. Як приклад можна привести Globus Toolkit.

Одночасно з усім цим, в технічній індустрії, VMware і Xen займалися популяризацією віртуалізації, яка дозволяла запускати відразу декілька віртуальних машин на одній фізичній машині. Це дало новий поштовх для розвитку ІТ-індустрії, а простота використання привернула увагу стартапів, яким було складно купувати і утримувати своє власне обладнання.

Нижче зображена класична модель комп'ютерних обчислень (рис.1.7). Доступ до серверів, додатків і сервісів здійснюється по мережі.

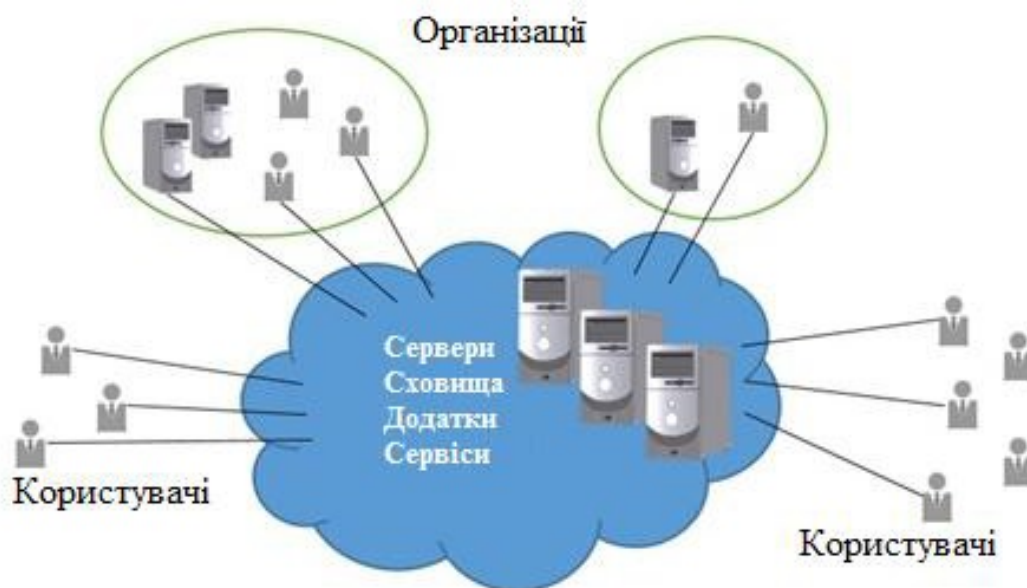


Рисунок 1.7 – Класична модель комп'ютерних обчислень

Звернувшись до хмарних обчислень, організація отримує можливість налаштовувати інфраструктуру на свій розсуд, витрачаючи на це меншу кількість коштів і зусиль. Іншими словами, ця модель спрямована на підвищення доступності обчислювальних ресурсів і поєднує в собі п'ять характеристик: самообслуговування на вимогу, широка доступність через Інтернет, об'єднання ресурсів в пул, здатність до швидкої адаптації і вимірювання показників.

Самообслуговування означає, що споживачі повинні мати можливість без ускладнень і за власним бажанням задіяти (або навпаки відключити) додаткові обчислювальні потужності, не контактуючи з персоналом і технікою на стороні постачальника послуг.

Широка доступність означає, що всі можливості, пропоновані постачальником доступні через мережу. Робота з ними здійснюється на основі стандартних механізмів - це дає можливість використовувати різні клієнтські платформи, наприклад мобільні телефони, планшетні і персональні комп'ютери.

Свої обчислювальні ресурси постачальник об'єднує в пул, щоб їх можна було динамічно перерозподіляти відповідно до потреб користувачів - це так званий принцип множинної оренди (Multi-tenancy). Виникає відчуття незалежності від місця розташування, коли замовник не знає, де саме знаходяться ресурси, але може приймати рішення щодо розташування на абстрактному рівні (країна або регіон).

Здатність до швидкої адаптації - це можливість швидко масштабувати ресурси під потреби замовника. З точки зору клієнта, пропоновані йому можливості виглядають необмеженими, якими він може скористатися в будь-який момент.

Хмарні системи автоматично контролюють і оптимізують використання ресурсів. Це здійснюється шляхом вимірювання різних параметрів (розмір сховища даних, обчислювальна потужність, пропускна здатність). Таким чином, як постачальник, так і споживач отримують повну інформацію про обсяг наданих / спожитих послуг.

Що стосується вартості послуг, то процес їх формування може бути досить складним, а ціні змінюватися від постачальника до постачальника. Джейсон Лемкін (Jason M. Lemkin), партнер SaaStr Ventures, вважає, що якщо ваш продукт краще, то не варто соромитися завищувати ціну.

Якщо ви вводите якусь нову функцію, яка здатна кардинально змінити призначений для користувача досвід, то немає нічого поганого в тому, якщо ви спробуєте отримати з цього максимальну вигоду. «Якщо ваш продукт в п'ять разів серйозніше, ніж у конкурента, то ви можете просити за нього в 5 разів більше», - стверджує Джейсон.

Крім характеристик виділяють ще три моделі обслуговування: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS). Відрізняються вони ступенем контролю що надається (рис.1.8).



Рисунок 1.8 – Три моделі обслуговування клієнта

У випадку з IaaS, клієнт отримує можливість використовувати хмарну інфраструктуру на свій розсуд і самостійно управляти ресурсами обробки і зберігання, а також мережами. «Користувач може створити віртуальну інфраструктуру і змінити її в будь-який момент», - говорить консультант Еван Лейт (Ewan Leith). Аутсорсинг став популярним ще в ті часи, коли компанії хотіли використовувати комп'ютери, але не хотіли нести витрати по їх утриманню та обслуговуванню. З цієї причини ми сьогодні маємо технологію віртуалізації.

Віртуалізація - це надання набору обчислювальних ресурсів або їх логічного об'єднання, абстраговані від апаратної реалізації, тобто одна фізична машина може підтримувати кілька віртуальних. Таким чином, фізичні ресурси об'єднуються в пул, а гіпервізор виділяє їх віртуальним машинам, на яких запускаються гостьові операційні системи.

Вам не буде потрібно купувати обладнання, не буде потрібно будувати власний дата-центр, не буде потрібно наймати системних інженерів, які відповідають за обслуговування техніки на фізичному рівні. Дану частину ви віддаєте на обслуговування хмарного провайдера. У вашій

зоні відповідальності залишається управління операційною системою, установка і налаштування додатків.

Другий шар - це платформа як послуга або PaaS. При переході від моделі IaaS до моделі PaaS (Platform as a Service) додатково на сторону хмарного провайдера передається управління операційними системами і базами даних. В цьому випадку клієнтам не доводиться думати про дисковий простір, який необхідно виділити, і розподілі навантаження між серверами. Прикладами PaaS є Google App Engine, Heroku і Force.com.

Програмне забезпечення як послуга (SaaS) - останній рівень хмарних обчислень, зазвичай доповнює PaaS. Це програмне забезпечення для кінцевого користувача, наприклад, що забезпечує роботу з електронною поштою або текстом. Дуже часто воно надається за підпискою. Прикладами SaaS можуть служити Google Apps, Salesforce.com і Business Productivity Online Suite від Microsoft.

Для варіанту SaaS на сторону хмарного провайдера додатково передаються питання установки і налаштування додатків, моніторингу, резервного копіювання, захищеної передачі в Інтернет - тобто всі завдання. Якщо ви вирішили скористатися цією моделлю, то вам навіть не обов'язково тримати в команді технічного фахівця, оскільки всім керує постачальник послуг.

Існує кілька моделей розгортання: приватна хмара, публічна хмара, суспільна хмара, гібридна хмара.

Приватна хмара (private cloud) - це інфраструктура, яка розташовується в межах однієї організації. Дана модель розгортання створена з метою задовольнити потреби внутрішнього робочого персоналу, забезпечуючи високий рівень безпеки даних. Приватна хмара створюється, наприклад, для забезпечення будь-якої дочірньої компанії сервісом корпоративної пошти.

Публічна хмара (public cloud) - це інфраструктура, призначена для вільного використання широкою публікою. Цей тип хмари може перебувати у власності, наприклад, комерційних, наукових і урядових організацій.

Однак слово «публічне» зовсім не означає, що дані користувачів доступні абсолютно всім - тут як і раніше реалізуються механізми безпеки для контролю доступу. Основною перевагою використання публічної хмари є простота настройки і низька вартість. Постачальник послуги робить всю роботу, необхідну для створення хмари, а споживач лише налаштовує необхідну кількість ресурсів.

Громадська хмара (community cloud) має схожі риси з приватною і публічною хмарию. Це вид інфраструктури, призначений для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання. Громадська хмара може управлятися організаціями третьої сторони і існувати як всередині, так і поза юрисдикцією власника. В цьому випадку відповідальність за змістом хмари перекладається з плечей організацій-членів на всю спільноту повністю.

Гібридною ж хмарию (hybrid cloud) називають композицію з двох або більше типів хмар, які пов'язуються між собою стандартизованими технологіями передачі даних. Дуже часто компанії запускають бізнес-критичні програми в приватній хмарі, в той час як інші програми працюють в публічній хмарі.

2 ЗАГРОЗИ ХМАРНИМ ТЕХНОЛОГІЯМ ТА РІШЕННЯ ПО ЗАХИСТУ ВІД НИХ

2.1 Загрози безпеки в публічній хмарі

Хоча використання публічної хмари пов'язане зі значними фінансовими вигодами, воно, як і будь-яка інфраструктура, має свій перелік загроз. Протягом декількох років ми спостерігаємо зростання частоти атак на публічні хмари і різноманітності використовуваного для цього шкідливого ПО. Зі збільшенням інцидентів, пов'язаних з відстеженням вразливостей, веб-додатками і атаками методом грубої сили, стає критично важливо сформулювати розуміння типів загроз, характерних для хмари - завдяки цьому ви зможете створити відповідну всебічну стратегію безпеки, щоб захистити вашу систему від атак.

В публічній хмарі ключ до забезпечення безпеки - чітке розуміння існування моделі поділу обов'язків щодо забезпечення безпеки між клієнтом і провайдером послуг. Без цього розуміння ви можете перебувати в омані щодо того, що ваш провайдер захищає вас, в той час, як відповідальність за певні функції безпеки буде насправді лежати на вас.

Наприклад, ваш сервіс-провайдер несе відповідальність за 100% основоположних послуг, таких як обчислювальні потужності, зберігання даних, бази даних, мережеві послуги. На рівні мереж ваш сервіс-провайдер несе відповідальність за сегментування мереж, послуги захисту периметра, захист від DDOS-атак і спуфінга. Але ви, кінцевий користувач, несете відповідальність за виявлення загроз мережі, оповіщення сервіс-провайдера про них і будь-яких інших інцидентах (пов'язаних з безпекою). На рівні хоста ви відповідальні за управління доступом, оновленнями, зміцнення і моніторинг систем безпеки і аналіз лог-файлів. Компоненти вашого веб-додатку - на 100% ваша відповідальність. Щоб зрозуміти розмежування відповідальності між вами і вашим провайдером, подивіться на графік нижче.

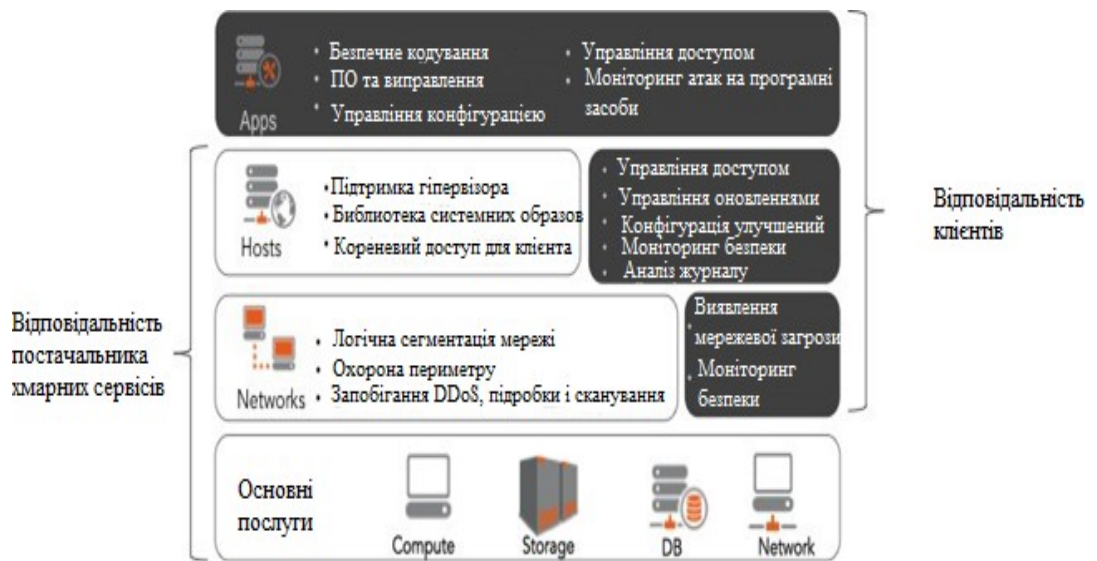


Рисунок 2.1 – Визначення відповідальності користувача та провайдера

Розуміння вашої ролі та ролі вашого хмарного провайдера не тільки допоможе вам прийняти найбільш адекватне рішення щодо хмарної інфраструктури, завдяки йому, ваша стратегія кібербезпеки почне ефективно та економічно захищати ваші дані від небезпеки у хмарі негайно після її впровадження.

Забезпечте безпеку вашого коду. Безпека коду - на 100% ваша відповідальність. По-перше, переконайтеся, що безпека - частина вашого життєвого циклу розробки ПО (SDLC, software development lifecycle). Для цього сформулюйте список завдань на зразок цього:

1. Переконайтеся, що ваш код постійно оновлюється і що ви використовуєте останні версії плагінів.
2. Використовуйте програмний контроль за швидкістю виконання операцій, щоб не стати жертвою ботнету.
3. Використовуйте шифрування всюди, де це можливо.
4. Тестуйте усі бібліотеки і рішення, в яких задіяні сторонні розробки.

5. Будьте в курсі всіх можливих вразливостей продуктів, які ви використовуєте.

6. Постійно перевіряйте код після додавання оновлень.

Створіть політики управління доступом. По-перше, визначте, що входить у ваші активи. Як тільки ви складете свій список, визначте ролі і обов'язки, необхідні для доступу до активів. По можливості централізуйте аутентифікацію - для впровадження аутентифікації почніть з моделі призначення привілеїв.

Використовуйте методику управління оновленнями. Знову ж, сформулюйте список важливих процедур:

1. Складіть перелік своїх ресурсів.
2. По можливості, розробіть план по їх стандартизації.
3. Проведіть дослідження на предмет вразливостей, які можуть вплинути на вас. Класифікуйте ризики на основі типів вразливостей і ймовірності їх виникнення.
4. По можливості тестуйте оновлення до їх релізу.
5. Встановіть розклад регулярних оновлень і не забудьте включити в нього сторонні продукти, які вимагають встановлення оновлень вручну.

Управління логами. Лог файли в даний час виявляються корисні не тільки для контролю витрат, вони стають серйозним інструментом забезпечення безпеки. Ви можете використовувати дані лог-файлів для відстеження шкідливої активності і для проведення розслідувань. Суть процесу перетворення логів в ефективний інструмент забезпечення безпеки полягає в постійному моніторингу, який необхідний для пошуку аномальної поведінки.

Створіть свій набір інструментів для забезпечення безпеки - ви повинні ставитися до хмари як до бізнес-мережі. Вам потрібно впровадити всебічну стратегію забезпечення безпеки, яка охоплювала б усі зони вашої відповідальності. Використовуйте, IP-таблиці, фаєрволи веб-додатків, антивірус, систему виявлення вторгнень, шифрування і управління логами.

Вивчайте нові варіанти забезпечення безпеки і переконайтеся в тому, що рішення, які ви використовуєте, оптимальні для вашого бізнесу.

Будьте в курсі подій - вам потрібно залишатися в курсі всіх вразливостей, які можуть виникнути у вашій системі. Сайти, перераховані нижче містять одні з кращих матеріалів на цю тему. Ці ресурси можуть допомогти вам бути в курсі вразливостей що з'являються і поширюються, експлойтів і атак:

- securityfocus.com;
- www.exploit-db.com;
- seclists.org/fulldisclosure;
- www.securitybloggersnetwork.com;
- www.sans.org;
- www.nist.gov.

Знайте вашого сервіс-провайдера. І нарешті, з'ясуйте, як саме розподіляється відповідальність за безпеку між вами і вашим конкретним провайдером, а також що він може запропонувати відносно забезпечення вашої безпеки. Також необхідно постійно тестувати систему, щоб переконатися в підтримці високого рівня захищеності.

2.2 Загрози хмарних обчислень і методи їх захисту

Центр обробки даних (ЦОД) являє собою сукупність серверів, розміщених на одному майданчику з метою підвищення ефективності і захищеності. Безпека центрів обробки даних являє собою мережевий і фізичний захист, а також відмова стійкість і надійне електроживлення. В даний час на ринку представлений широкий спектр рішень для захисту серверів і ЦОД від різних загроз та підтримки ключових характеристик ЦОД (Рис. 2.2). Їх об'єднує орієнтованість на вузький спектр вирішуваних завдань. Однак спектр цих завдань піддався деякому розширенню внаслідок поступового витіснення класичних апаратних систем віртуальними

платформами. До відомих типів загроз (мережеві атаки, уразливості в додатках операційних систем, шкідливе програмне забезпечення) додалися складнощі, пов'язані з контролем середовища (гіпервізора), трафіку між гостьовими машинами та розмежуванням прав доступу. Розширилися внутрішні питання і політики захисту ЦОД, вимоги зовнішніх регуляторів. Робота сучасних ЦОД в ряді галузей вимагає закриття технічних питань, а також питань пов'язаних з їх безпекою. Фінансові інститути (банки, процесингові центри) підпорядковані ряду стандартів, виконання яких закладено на рівні технічних рішень. Проникнення платформ віртуалізації досягло того рівня, коли практично всі компанії, що використовують ці системи, досить серйозно зайнялися питаннями посилення безпеки в них. Відзначимо, що буквально рік тому інтерес був скоріше теоретичний.

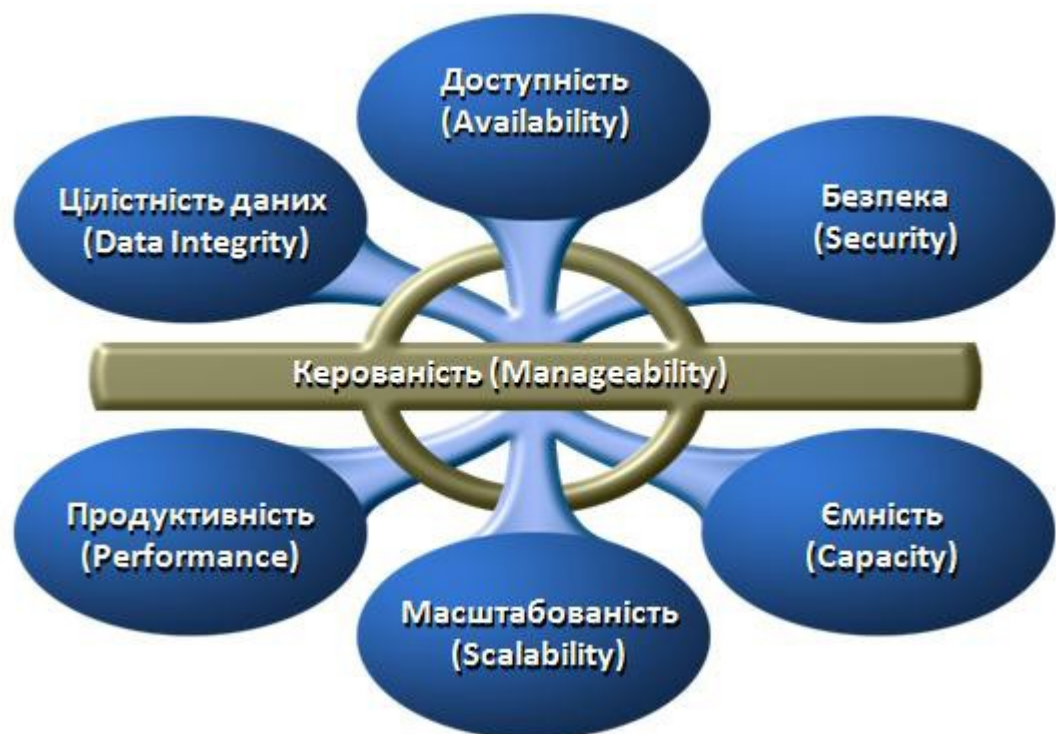


Рисунок 2.2 – Ключові характеристики ЦОД.

В сучасних умовах стає все складніше забезпечити захист критично важливих для бізнесу систем і додатків.

Поява віртуалізації стала актуальною причиною масштабної міграції більшості систем на віртуальні машини, проте рішення задач забезпечення безпеки, пов'язаних з експлуатацією додатків в новому середовищі, вимагає особливого підходу. Багато типів загроз достатньо вивчені і для них розроблені засоби захисту, проте їх ще потрібно адаптувати для використання в хмарі.

Контроль і управління хмарами - є проблемою безпеки. Гарантій, що всі ресурси хмари порашовані і в ньому немає неконтрольованих віртуальних машин, не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари немає. Це високорівневий тип загроз, тому що він пов'язаний з керованістю хмарою, як єдиною інформаційною системою і для нього загальний захист потрібно будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмарних інфраструктур.

В основі забезпечення фізичної безпеки лежить суворий контроль фізичного доступу до серверів і мережевої інфраструктури. На відміну від фізичної безпеки, мережева безпека в першу чергу являє собою побудову надійної моделі загроз, що включає в себе захист від вторгнень і міжмережевий екран. Використання брандмауера передбачає роботу фільтра, з метою розмежування внутрішньої мережі ЦОД на підмережі з різним рівнем довіри. Це можуть бути окремо сервери, доступні з Інтернету або сервери з внутрішніх мереж.

У хмарних обчисленнях найважливішу роль платформи виконує технологія віртуалізації. Для збереження цілісності даних і забезпечення захисту розглянемо основні відомі загрози для хмарних обчислень.

Вимоги до безпеки хмарних обчислень не відрізняються від вимог безпеки до центрів обробки даних. Однак, віртуалізація ЦОД і перехід до хмарних середовищ призводять до появи нових загроз.

Доступ через Інтернет до управління обчислювальною потужністю одна з ключових характеристик хмарних обчислень. У більшості традиційних

ЦОД доступ інженерів до серверів контролюється на фізичному рівні, в хмарних середовищах вони працюють через Інтернет. Розмежування контролю доступу та забезпечення прозорості змін на системному рівні є одним з головних критеріїв захисту.

Віртуальні машини динамічні. Створити нову машину, зупинити її роботу, запустити заново, все це можна зробити за короткий час. Вони клонуються і можуть бути переміщені між фізичними серверами. Данна мінливість важко впливає на розробку цілісності системи безпеки. Однак, уразливості операційної системи або додатків у віртуальному середовищі поширюються безконтрольно і часто проявляються після довільного проміжку часу (наприклад, при відновленні з резервної копії). У середовищах хмарних обчислень важливо надійно зафіксувати стан захисту системи, при цьому це не повинно залежати від її стану та місця розташування.

Сервери хмарних обчислень і локальні сервери використовують одні і ті ж операційні системи і додатки. Для хмарних систем загроза віддаленого злому або зараження шкідливим ПО висока. Ризик для віртуальних систем також високий. Паралельні віртуальні машини збільшують «поверхню атаки». Система виявлення та запобігання вторгнень повинна бути здатна виявляти шкідливу активність на рівні віртуальних машин, незалежно від їх розташування в хмарному середовищі.

Коли віртуальна машина вимкнена, вона наражається на небезпеку зараження. Доступу до сховища образів віртуальних машин через мережу досить. На вимкненій віртуальній машині абсолютно неможливо запустити захисне програмне забезпечення. В даному випадку повинен бути реалізований захист не тільки всередині кожної віртуальної машини, а й на рівні гіпервізора, розмежування доступу представлено на (рис. 2.3)

При використанні хмарних обчислень периметр мережі розмивається або зникає. Це призводить до того, що захист менш захищеної частини мережі визначає загальний рівень захищеності.

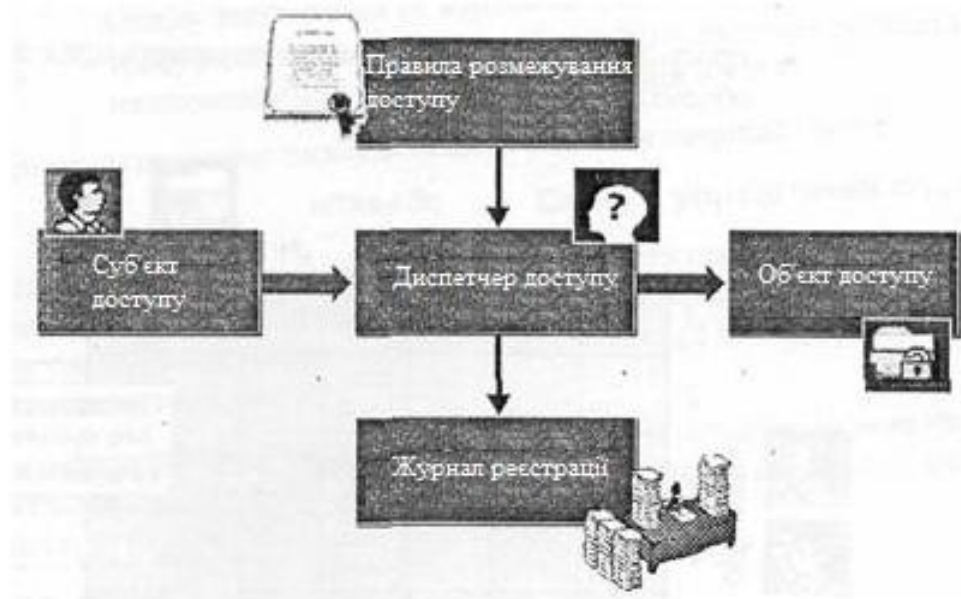


Рисунок 2.3 - Схема роботи механізму розмежування доступу

Для розмежування сегментів з різними рівнями довіри в хмарі віртуальні машини повинні самі забезпечувати себе захистом, переміщуючи мережевий периметр до самої віртуальної машини. Корпоративний firewall - основний компонент для впровадження політики ІТ безпеки і розмежування сегментів мережі, не в змозі вплинути на сервери, розміщені в хмарних середовищах.

2.3 Атаки на хмари і рішення по захисту від них

Вразливості операційних систем, модульних компонентів, мережевих протоколів та іншого - традиційні загрози, для захисту від яких досить встановити межстевой екран, firewall, антивірус і інші компоненти, які вирішують цю проблему. При цьому важливо, щоб кошти виділенні на захист ефективно працювали в умовах віртуалізації.

Цей тип атак пов'язаний з багатошаровістю хмари, загальним принципом безпеки. Для захисту від функціональних атак для кожної частини хмари необхідно використовувати такі засоби захисту: для проксі - ефективний захист від DoS-атак, для веб-сервера - контроль цілісності

сторінок, для сервера додатків - екран рівня додатків, для СУБД - захист від SQL-ін'єкцій, для системи зберігання даних - правильні бекапи (резервне копіювання), розмежування доступу. Окремо кожні з цих захисних механізмів вже створені, але вони не зібрані разом для комплексного захисту хмари, тому завдання по інтеграції їх в єдину систему потрібно вирішувати під час створення хмари.

Більшість користувачів підключаються до хмари, використовуючи браузер. Тут можливі такі атаки, як Cross Site Scripting, «викрадення» паролів, перехоплення веб-сесій, «людина посередині» і багато іншого. Єдиний захист від даного виду атак є правильна аутентифікація і використання шифрованого з'єднання (SSL) з взаємною аутентифікацією. У цій галузі інформаційної безпеки є ще безліч невирішених завдань.

Гіпервізор є одним з ключових елементів віртуальної системи. Основною його функцією є поділ ресурсів між віртуальними машинами. Атака на гіпервізор може привести до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів іншої. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витіснити віртуальну машину з сервера. В якості стандартних методів захисту рекомендується застосовувати спеціалізовані продукти для віртуальних середовищ, інтеграцію хост-серверів зі службою каталогу Active Directory, використання політик складності і обов'язковості паролів, а також стандартизацію процедур доступу до керуючих засобів хост-сервера, застосовувати вбудований брандмауер хоста віртуалізації. Також можливе відключення таких часто невикористовуваних служб як, наприклад, веб-доступ до сервера віртуалізації.

Велика кількість віртуальних машин, які використовуються в хмарах вимагають наявності систем управління, здатних надійно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в систему управління може привести до появи віртуальних машин - невидимок, здатних блокувати одні віртуальні машини і підставляти інші.

2.4 Рішення щодо захисту від загроз безпеки

Шифрування - один з найефективніших способів захисту даних. Провайдер, що надає доступ до даних повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також у випадку необхідності, безповоротно видаляти.

Зашифровані дані при передачі повинні бути доступні тільки після аутентифікації. Дані не вийде прочитати або зробити зміни, навіть у випадку доступу через ненадійні вузли. Такі технології досить відомі, алгоритми і надійні протоколи AES, TLS, IPsec давно використовуються провайдерами.

Аутентифікації - захист паролем. Для забезпечення більш високої надійності, часто вдаються до таких засобів, як токени і сертифікати (рис. 2.4).



Рисунок 2.4 – Процес авторизації користувача.

Токени – це компактний пристрій, призначений для забезпечення інформаційної безпеки користувача, також використовується для ідентифікації його власника, безпечного віддаленого доступу до інформаційних ресурсів і т. д. Як правило, це фізичний пристрій, що використовується для спрощення аутентифікації. Також цей термін може належати і до програмних токенів, які видаються користувачеві після

успішної авторизації і є ключем для доступу до служб. Токени призначені для електронного посвідчення особи (наприклад, клієнта, який отримує доступ до банківського рахунку), при цьому вони можуть використовуватися як замість пароля, так і разом з ним. У певному сенсі токен - це електронний ключ для доступу до чого-небудь.

Широкої практики набуло використання індивідуальної віртуальної машини і віртуальної мережі. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій, як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service). Часто провайдери ізолюють дані користувачів один від одного за рахунок зміни даних коду в єдиному програмному середовищі. Даний підхід має ризики, пов'язані з небезпекою знайти дірку в нестандартному коді, що дозволяє отримати доступ до даних. У випадку можливої помилки в коді користувач може отримати дані іншого і використати на свій розсуд або просто відчувати незручності у зв'язку з отриманням непотрібних даних.

2.5 Майбутнє хмарних обчислень

В майбутньому хмарні обчислення будуть ставати доступнішими для користувачів і компаній. Це буде викликано рядом факторів таких як:

- а) апаратна віртуалізація - підвищення продуктивності хмарних обчислень;
- б) зниження енергоспоживання апаратного забезпечення - зниження енергоспоживання;
- в) підвищення швидкостей - пропускна здатність мережевого обладнання постійно підвищується, що збільшує продуктивність і зменшує кількість обладнання при тому ж каналі.

Сьогодні використання хмарних технологій в будь-яких сферах, від зберігання документів простими користувачами, до систем крупного бізнесу - це певний компроміс між широкими можливостями з одного боку, і

певними ризиками з іншого. Зрозуміло, саме так на хмарні обчислення дивляться і з економічної точки зору: баланс між їх очевидною інвестиційною привабливістю та фінансовими ризиками подібних вкладень поки не знайдений.

Втім, незважаючи на це - технології активно розвиваються, а ринок неухильно зростає. До 2020 року Forrester Research прогнозує збільшення його обсягу до воістину величезної суми - 240 мільярдів доларів. Можна сміливо стверджувати, що у хмарних обчислень, велике майбутнє.

3 ЕФЕКТИВНІСТЬ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ

3.1 Постачальники хмарних сервісів та методи захисту які вони використовують

На сьогоднішній день існує велика кількість постачальників хмарних платформ, сховищ і ПО. У зв'язку з цим робляться спроби якимось чином порівняти їх між собою. В Інтернеті можна знайти масу оглядів на цю тему. Але через різноманіття послуг, що надаються розібратися в тому, хто з них краще, досить важко. Саме тому необхідно вибрати кілька основних показників, які можуть допомогти при порівнянні, наприклад, ємність, захищеність, простота, функціональність, доступність та ін. При цьому, безсумнівно, кожен користувач вибирає те чи інше рішення в залежності від необхідності.

На даний момент основними постачальниками хмарної інфраструктури вважаються Amazon, Google і Microsoft. У кожної з компаній є ціла лінійка послуг, що надаються.

Google Drive - хмарне сховище даних, що належить компанії Google, і дозволяє користувачам зберігати свої дані на серверах в хмарі і ділитися ними з іншими користувачами в Інтернеті. Google Drive відрізняється лаконічним інтерфейсом і пропонує встановити зручні програмні клієнти для смартфонів і планшетів на базі операційної системи Android, ПК і ноутбуків під управлінням операційної системи Windows або MacOS, мобільних пристроїв iPhone і iPad. У майбутньому очікується більш тісна інтеграція сховища з операційною системою Chrome OS і підтримка Linux. Кожен користувач Google Drive отримує до 15 Гбайт вільного простору на всі сервіси Google (в тому числі Gmail і Photos). При цьому він сам може вирішити, скільки саме місця виділити під пошту і який обсяг залишити під важливі файли. Працювати з файлами в Google Drive можна прямо в браузері. Google Drive, за потреби, можна перетворити в окрему папку в

документах смартфона, планшета або ПК, і її вміст буде синхронізуватися автоматично.

Google Docs - безкоштовний онлайн-офіс, що включає в себе текстовий, табличний процесори і сервіс для створення презентацій, а також інтернет-сервіс хмарного зберігання файлів з функціями файлообміну. Дозволяє створювати і редагувати стандартні документи, таблиці та презентації, а також підтримує функції спільної роботи над ними.

Google App Engine - сервіс хостингу сайтів та web-додатків на серверах Google. Безкоштовно надається до 1 Гб дискового простору, 10 Гб вхідного трафіку в день, 10 Гб вихідного трафіку в день і 2 000 операцій відправлення електронної пошти в день. Додатки, що розгортаються на базі App Engine, повинні бути написані на Python, Java або Go. Пропонується набір API для сервісів сховища datastore API (BigTable) акаунтів Google, набір API для завантаження даних по URL, електронної пошти і т.д.

Платформа Google конкурує з аналогічними сервісами від Amazon, які надають можливість розміщувати файли і веб-програми, використовуючи свою інфраструктуру. На відміну від багатьох звичайних розміщень додатків на віртуальних машинах, таких як Amazon EC2, платформа App Engine тісно інтегрована з додатками і накладає на розробників деякі обмеження.

Google Cloud Storage - сервіс хостингу файлів, заснований на IaaS. Всі файли, які записуються або перезаписувати на сервери, автоматично шифруються по алгоритму AES-128. Є конкурентом продукту Amazon S3.

Amazon Simple Storage Service (Amazon S3) - онлайнова веб-служба, пропонована Amazon Web Services, що надає можливість для зберігання і отримання будь-якого обсягу даних, у будь-який час із будь-якої точки мережі, так званий файловий хостинг. 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

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

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.

Платформа Windows Azure має API, побудоване на REST, HTTP і XML, що дозволяє розробникам використовувати хмарні сервіси з будь-якою операційною системою, пристроями та платформами.

Нижче розглянуто кілька типових задач і порівнюються їх можливі рішення на кожній з платформ - Amazon EC2, Google App Engine, Windows Azure.

Завдання 1. Необхідно відправити в хмару на обробку локально створений додаток; причому додаток, як правило, побудований на базі технологій Java або .NET, не повинен змінювати свій зміст в процесі виконання.

Завдання 2. Необхідно запустити web-додаток, що використовує фонове оновлення даних і засоби балансування навантаження.

Завдання 3. Необхідно виконати в автоматичному режимі, без застосування інтерфейсу, з користувачем прикладну обчислювальну задачу з використанням методів паралельної обробки.

Завдання 4. Необхідно запустити в хмарі додаток, який взаємодіє з локальною програмою або обмінюється даними з клієнтським ПК.

Рішення на платформі Amazon, як правило, базуються на тому, що локальний комп'ютер розглядається як сервер, що входить до складу загального ЦОД, і вносяться необхідні зміни в конфігурацію, або необхідно створити кілька віртуальних машин в залежності від необхідного рівня масштабування.

На інших вищезазначених платформах використовують спеціальні засоби динамічного масштабування, скриптові програми, безліч різних API.

Частина з них вельми зручні, в інших випадках необхідно докладати чимало зусиль для істотної або навіть майже повної переробки вихідної програми.

API (програмний інтерфейс додатка, інтерфейс прикладного програмування) (англ. Application programming interface) - опис способів (набір класів, процедур, функцій, структур або констант), якими одна комп'ютерна програма може взаємодіяти з іншою програмою.

Зазвичай входить в опис будь-якого інтернет-протоколу, програмного каркаса (фреймворка) або стандарту викликів функцій операційної системи. Часто реалізується окремою програмною бібліотекою або сервісом операційної системи. Використовується програмістами при написанні різних додатків.

API визначає функціональність, яку надає програма (модуль, бібліотека), при цьому API дозволяє абстрагуватися від того, як саме ця функціональність реалізована. Якщо програму (модуль, бібліотеку) розглядати як чорний ящик, то API - це безліч «ручок», які доступні користувачеві даного ящика і які він може крутити і смикати. Програмні компоненти взаємодіють один з одним за допомогою API. При цьому зазвичай компоненти утворюють ієрархію - високорівневі компоненти використовують API низькорівневих компонентів, а ті, в свою чергу, використовують API ще більш низькорівневих компонентів. За таким принципом побудовані протоколи передачі даних через Інтернет. Стандартний стек протоколів (мережева модель OSI) містить 7 рівнів (від фізичного рівня передачі біт до рівня протоколів програм, подібних протоколів HTTP і IMAP). Кожен рівень користується функціональністю попереднього («нижчого») рівня передачі даних і, в свою чергу, надає потрібну функціональність наступному («вищерозміщеному») рівню. API бібліотеки функцій і класів включає в себе опис сигнатур і семантики функцій.

Практично всі операційні системи (UNIX, Windows, OS X і т.д.) мають API, за допомогою якого програмісти можуть створювати додатки для цієї

операційної системи. Головний API операційних систем - це безліч системних викликів. В індустрії програмного забезпечення загальні стандартні API для стандартної функціональності грають важливу роль, так як вони гарантують, що всі програми, які використовують загальний API, будуть працювати однаково добре або хоча б типовим звичним чином. У випадку API графічних інтерфейсів - це означає, що програми будуть мати схожий користувацький інтерфейс, що полегшує процес освоєння нових програмних продуктів.

SSL (англ. Secure Sockets Layer — рівень захищених сокетів) — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку розроблений компанією Netscape Communications. Згодом на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що отримав ім'я TLS.

Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP/IP, причому для шифрування використовується асиметричний алгоритм з відкритим ключем. При шифруванні з відкритим ключем використовується два ключі, причому будь-який з них може використовуватися для шифрування повідомлення. Тим самим, якщо використовується один ключ для шифрування, то відповідно для розшифрування потрібно використовувати інший ключ. У такій ситуації можна отримувати захищені повідомлення, публікуючи відкритий ключ, і зберігаючи в таємниці секретний ключ.

При використанні SSL-протоколу інформація передається в закодованому вигляді по HTTPS і розшифрувати її можна тільки за допомогою спеціального ключа на відміну від звичного протоколу HTTP. Для роботи SSL-протоколу потрібно, щоб на сервері був встановлений SSL-сертифікат.

SSL-сертифікат - це свого роду унікальний цифровий підпис вашого сайту. Такий сертифікат потрібен, в першу чергу, банкам, платіжним системам і іншим організаціям, що працюють з персональними даними, для

захисту транзакцій і запобігання несанкціонованого доступу до конфіденційної інформації.

SSL-сертифікат містить наступну інформацію:

- доменне ім'я, на яке оформлено SSL-сертифікат;
- юридична особа, яка володіє сертифікатом;
- фізичне місцезнаходження власника сертифіката (місто, країна);
- термін дії сертифіката;
- реквізити компанії-постачальника SSL-сертифіката.

SSL-Сертифікат підтверджує, що домен належить реальній компанії і що його власник має право користуватися секретним ключем на законних підставах.

Advanced Encryption Standard (AES) — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий як американський стандарт шифрування урядом США. Державний інститут стандартів і технологій (англ. National Institute of Standards and Technology, NIST) США опублікував попередню специфікацію AES 26 жовтня 2001 року, після п'ятилітньої підготовки. 26 травня 2002 року AES оголошено стандартом шифрування. Станом на 2009 рік AES є одним із найпоширеніших алгоритмів симетричного шифрування. Через фіксований розмір блоку AES оперує із масивом 4×4 байт, що називається станом (версії алгоритму із більшим розміром блоку мають додаткові колонки).

RSA (аббревіатура від прізвищ Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел.

RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису.

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий

(public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем. Систему RSA використовують для захисту програмного забезпечення та у схемах цифрового підпису. Зокрема, її використовують у відкритій системі шифрування PGP.

Через низьку швидкість шифрування (близько 30 кбіт/сек при 512 бітному ключі на процесорі 2 ГГц), повідомлення звичайно шифрують за допомогою продуктивніших симетричних алгоритмів з випадковим ключем (сеансовий ключ), а за допомогою RSA шифрують лише цей ключ.

Криптосистема RSA використана у різних продуктах, на різних платформах і у багатьох галузях. Криптосистема RSA вбудована в комерційні продукти, число яких постійно зростає. Також її використовують операційні системи Microsoft, Apple, Sun і Novell. В апаратному виконанні RSA алгоритм застосований в захищених телефонах, на мережних платах Ethernet, на смарт-картах, широко використовується в криптографічному обладнанні. Крім того, алгоритм входить до складу всіх основних протоколів для захищених комунікацій Internet, в тому числі SSL також використаний в багатьох установах, наприклад, в урядових службах, у більшості корпорацій, в державних лабораторіях і університетах. На осінь 2000 року технології з застосуванням алгоритму RSA були ліцензовані понад 700 компаніями в усьому світі.

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,

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 "хмарию" 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

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, Android, iOS	Так	Так	Microsoft
Box	10	SSL, AES256	Windows, Android, BlackBerry, iOS, WebOS, Windows Phone	Так	Так	Box
Яндекс Диск	10	Інформація відсутня	Windows, Linux, iOS Android,	Так	Ні	Яндекс

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.2.1 включені дані тільки про безкоштовні сервіси тих чи інших постачальників послуг.

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 Підвищення ефективності захисту хмарних сервісів

Сьогодні явище кіберзлочинності несе в собі загрозу як для компаній, урядових організацій так і для простих користувачів в тому числі в умовах хмарних обчислень. Хакерські атаки реалізуються різними способами: це і шкідливе ПО, ботнети, віруси й інші можливості вторгнень для атак. У той час як інженери в області безпеки інформаційних технологій поки недостатньо вивчили надійність хмарних структур і їх здатність витримувати хакерські атаки, а також здатність відновлюватися після успішно проведених кібератак.

Більше половини порушень безпеки залишаються невідомими через те, що не налагоджений обмін інформацією про потенційні загрози між компаніями.

Крім загроз з боку вірусів і шкідливих програм існують різні види мережових атак, зокрема DDos-атаки ("розподілена відмова в обслуговуванні"). DDos-атаки є спробами вивести з ладу мережеві сервіси організацій шляхом генерації підвищеного трафіку в системі з різних джерел. Кіберзлочинці влаштовують лавинну атаку на конкретні мережі, навантажуючи їх трафіком або направляючи численні запити, які повністю паралізують роботу мережі. Згідно з результатами останнього дослідження компанії Ponemon Institute, IT-фахівці оцінюють DDos-атаки як серйозну небезпеку, а в США вони вважаються проблемою номер один. Наприклад, у випадку з хмарним сервісом, що надається компанією Amazon, атаки такого типу не відразу можна розрізнити. Це відбувається тому, що збільшений трафік, навпаки, приносить прибуток постачальнику хмарних послуг, оскільки система тарифікації влаштована таким чином, що кошти списуються за обсяги завантажених матеріалів. На жаль, страждають компанії і приватні особи, яким доводиться в прямому сенсі розплачуватися за подібного роду кібератаки на хмарні сервіси.

Проте більше половини порушень безпеки залишаються невідомими через те, що не налагоджений обмін інформацією про потенційні загрози між компаніями. Щоб ефективно протистояти сучасним загрозам і забезпечити захист даних, підприємства повинні докласти спільних зусиль для організації такого обміну. Виникає необхідність у використанні технологій, в основі яких лежить збір даних з унікальної глобальної мережі сенсорів виявлення загроз і поширення цієї інформації по шлюзах безпеки в усьому світі. Таким чином, актуалізована інформація про загрози передається безпосередньо на шлюзи клієнтів, дозволяючи своєчасно вживати заходів безпеки проти нових загроз.

Крім цього для безпеки хмарних середовищ необхідно використовувати комплексні рішення, а не розрізнені елементи технологій безпеки, які застосовуються на робочих станціях. Найкраща можливість для реалізації такого захисту - це міжмережеві екрани нового покоління, що

представляють собою не тільки стандартний функціонал брандмауера і VPN, але включають також нові технології, такі як безпечний віддалений доступ, в тому числі з мобільних пристроїв, розширена ідентифікація користувачів, DLP, контроль додатків, фільтрація URL, антибот і антивіруси, де все це управляється з єдиної консолі.

На даний момент активно розробляються рішення для забезпечення безпеки нового покоління, що відповідають сучасним вимогам ринку, в тому числі таким, як хмарні обчислення. Саме завдяки створенню багаторівневої системи захисту можна буде нейтралізувати численні загрози і вберегти підприємства, компанії та урядові організації від новітніх технологій кібератак.

Одним із варіантів підвищення захищеності хмарних технологій може стати спільна робота постачальників хмарних послуг над єдиним відкритим стандартом створення та забезпечення надійної роботи і захисту хмарних систем. Завдяки такому стандарту кожен зміг би створити власну хмару яка забезпечила б широкий функціонал для користувача та мала б надійний всебічний захист від загроз.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Оцінка ефективності капіталовкладень в захист хмарних обчислень в умовах розвитку цифровізації економіки

Поширення хмарних сервісів висуває нові вимоги до центрів обробки даних, Cisco випустила на початку 2018 року сьомий щорічний звіт Cisco Global Cloud Index 2016-2021 («Глобальний індекс розвитку хмарних технологій в період з 2016 по 2021 рр»). Його головні теми - віртуалізація ЦОД і хмарні обчислення, тобто основні елементи, що визначають нові способи доставки споживчих і корпоративних мережевих сервісів.

За даними дослідження, зростання домінування хмарних сервісів в Інтернеті сприяють як споживчі, так і бізнес-додатки. У споживчому сегменті найбільш популярними хмарними додатками стали потокове відео, соціальні мережі та інтернет-пошук. У бізнес-сегменті швидше за інших розвиваються додатки в області планування корпоративних ресурсів (ERP), спільної роботи, аналітики, а також інші додатки для цифрових підприємств.

Швидке зростання трафіку ЦОД визначається збільшенням кількості хмарних додатків. Згідно зі звітом, до 2021 р. глобальний річний трафік хмарних ЦОД виросте в 3,3 рази і досягне 19,5 зетабайт (ЗБ) (в 2016 р. - 6 ЗБ), річний приріст (CAGR) за вказаний період складе 27%. Глобальний хмарний трафік до 2021 р. досягне 95% сукупного трафіку ЦОД, в 2016 році цей показник склав 88%.

Ще недавно основним бар'єром на шляху впровадження хмарних технологій були питання інформаційної безпеки. Удосконалення методів управління ЦОД і контролю даних допомогло мінімізувати ризики підприємств і поліпшити захист користувачів. Інновації в області інформаційної безпеки в поєднанні з такими перевагами хмарних обчислень, як масштабованість і економія масштабу (economies of scale), в значній мірі впливають на зростання хмарного трафіку. Крім того, поширення додатків

Інтернету речей (Internet of Things, IoT), «розумні» міста і автомобілі, підключені охорона здоров'я та енергетика, вимагають масштабованих обчислень і нових рішень для зберігання даних. До 2021 р. Cisco прогнозує зростання IoT-підключень до 13,7 млрд (показник 2016 року - 5,8 млрд).

4.2 Подвоєння числа гіпермасштабних ЦОД

Зростання потреб в ресурсах ЦОД і хмари, призвело до розробки великомасштабних публічних ЦОД, які стали називати гіпермасштабними. Згідно з опублікованими в поточному році прогнозами, до 2021 року в світі з'являться 628 гіпермасштабних ЦОД, тоді як в 2016 р. їх було 338 (зростання за аналізований період в 1,9 рази). До 2021 року на частку гіпермасштабних ЦОД припадатиме:

Таким

- 53% всіх серверів ЦОД (в 2016 р. — 27%);
- 69% усієї обчислювальної потужності ЦОД (в 2016 р. — 41%);
- 65% всіх даних, що зберігаються в ЦОД (в 2016 р. — 51%);
- 55% усього трафіка ЦОД (в 2016 р. — 39%).

Ключові дані і прогнози «Глобального індексу розвитку хмарних технологій»:

1. До 2021 р. 94% завдань і віртуальних обчислень (instance) будуть виконуватися в хмарних ЦОД, в традиційних ЦОД — 6%.
2. Світовий обсяг збережених в ЦОД даних до 2021 р. виросте в 4,6 рази і досягне 1,3 ЗБ (щорічний приріст 36%), в 2016 році цей показник склав 286 ексабайт.
3. На великі дані до 2021 р. припадатиме 30% всіх даних, що зберігаються в ЦОД (2016 г. - 18%).
4. Обсяг даних, збережених на пристроях, до 2021 року в 4,5 рази перевищить обсяг даних в ЦОД і досягне 5,9 ЗБ.

5. Завдяки розвитку Інтернету речей загальний річний обсяг згенерованих різними пристроями (і не обов'язково при цьому збережені) даних до 2021 р. досягне 847 ЗБ (2016 р. - 218 ЗБ). Обсяг згенерованих даних перевищує обсяг збережених на два порядки.

Для цілей дослідження в категорії хмарних обчислень враховувалися платформи, що на вимогу забезпечують повсюдний мережевий доступ до масиву конфігурованих обчислювальних ресурсів загального користування (мережі, сервери, додатки, сервіси і т.п.), які можуть бути швидко виділені або зняті при мінімальних діях з боку систем управління або сервіс-провайдера. Моделі розгортання включають приватні, публічні і гібридні хмари. Хмарні ЦОД можуть експлуатуватися як сервіс-провайдерами, так і приватними підприємствами.

4.3 Дані розвитку ринку хмарних технологій звіту IDC

У 2017 році обсяг глобального ринку публічних хмарних сервісів збільшився на 29% і в грошовому вираженні склав близько \$ 117 млрд. Такі дані наводяться в звіті IDC, опублікованому 22 червня 2018 року.

Експерти відзначають, що високі темпи зростання витрат на публічні хмарні сервіси в світі зберігаються вже протягом п'яти років поспіль, незважаючи на те, що за минулий час виручка на цьому ринку збільшилася втричі (табл.4.1).

Таблиця 4.1 – Сегменти ринку публічних хмарних сервісів, дані IDC.

Сегмент	2017 Прибуток	2016 Прибуток	Зростання протягом року, %	Частка ринку публічних хмарних послуг,%
IaaS	24,886	17,795	39,9	21,3
PaaS	17,026	11,572	47,1	14,6
SaaS	74,781	61,112	22,4	64,1
Загалом	\$116,693	\$90,479	29	100,0

З регіональної точки зору більшу частину продажів продовжують забезпечувати США, хоча частка країни в загальній сумі витрат на публічні хмарні сервіси зменшилася. У 2017-му внесок Сполучених Штатів склав 60%, тоді як роком раніше частковий показник доходив до рівня 62%. Зниження відбулося на тлі зростання участі в продажі публічних хмарних сервісів інших регіонів.

Понад 64% доходу на даному ринку сформував сегмент SaaS (програмне забезпечення як послуга). Серед основних тенденцій в даній категорії аналітики відзначили консолідацію вендорів на тлі стабільного зростання. У 2017 році дохід у цьому сегменті піднявся на 22% і впритул наблизилася до \$ 75 млрд. Прогрес, в основному, забезпечили системи управління ресурсами підприємства (Enterprise Resource Management, ERM), ПО для управління взаємовідносинами з клієнтами (Customer Relationship Management, CRM) і рішення для групової роботи (Collaborative Applications).

За даними досліджень IDC, частка сегмента PaaS (платформа як послуга) займає 14,6% від сумарного обсягу ринку публічних хмарних сервісів. У 2017-му темпи зростання даного сегмента сповільнилися і склали 47% проти 48% в 2016-м, а виручка перевищила \$ 17 млрд. Понад 31% обороту на ринку або близько \$ 25 млрд забезпечив сегмент IaaS (інфраструктура як послуга), який передбачає використання обчислювальних ресурсів постачальника, таких як сервери, мережеве обладнання та сховища даних. Аналітики також відзначили деяке уповільнення темпів зростання даного сегмента, які в 2017-му були в межах 40% замість 45% в 2016 році.

Рейтинг вендорів в дослідженні не наводиться. Зазначається лише, що в 2017 році 16 найбільших постачальників публічних хмарних сервісів контролювали понад 50% ринку.

4.4 Дослідження світового ринку публічних хмар компанією Gartner та IDC

12 квітня 2018 року аналітики Gartner оприлюднили деякі результати дослідження світового ринку публічних хмар. Витрати на ці рішення підвищилися більш ніж на 30% до \$ 153,5 млрд завдяки інфраструктурним сервісам (IaaS) і програмному забезпеченню, що надається в якості послуги (SaaS). У 2017 році сумарні витрати споживачів і компаній на хмарні сервіси, що надаються в рамках публічного доступу, склали \$ 153,5 млрд проти \$ 118 млрд роком раніше.

За даними Gartner, після аналізу сегментів ринку публічних хмар, продажі рішень IaaS підскочили з 25,3 до 30 млрд доларів. Сегменти SaaS і PaaS показали підйом з \$ 38,6 млрд і \$ 7,2 млрд до \$ 60,2 млрд і \$ 11,9 млрд відповідно. Витрати на BPaaS-сервіси (бізнес-процеси як послуга) і послуги хмарного управління і безпеки в 2017 році досягли 42,6 і 8,7 млрд відповідно.

Найбільшим сегментом ринку публічних хмар залишається SaaS, який, за прогнозами Gartner, в 2018 році підвищиться на 22,2%, а до 2021-го на ці рішення буде припадати 45% софтверних витрат в світі. Найбільш швидкозростаючим сегментом аналітики називають IaaS, обсяг якого в 2018 році збільшиться майже на 40%.

22 лютого 2017 року аналітична компанія Gartner оприлюднила результати дослідження світового ринку хмарних послуг, що надаються великій кількості клієнтів, використовуючи загальнодоступні дата-центри. Витрати тут виросли на 20% завдяки інфраструктурним сервісам (IaaS).

За оцінками Gartner, в 2016 році сумарні витрати споживачів і компаній на публічні хмари склали \$ 209,2 млрд проти \$ 175 млрд у 2015-му. Продажі IaaS-рішень піднялися на 56% до \$ 25,3 млрд, чому сприяв зростаючий попит на послуги переведення ІТ-інфраструктури в хмару і високопродуктивні навантаження, на зразок штучного інтелекту, Інтернету речей та аналітики (табл.4.2).

Таблиця 4.2 – Прогноз по ринку публічних хмар на період з 2016 по 2020 роки, дані Gartner.

Послуга	2016	2017	2018	2019	2020
BPaaS (Бізнес процес як послуга)	40,812	43,772	47,556	51,652	56,176
PaaS (Платформа як послуга)	7,169	8,851	10,616	12,580	14,798
SaaS (Програмне забезпечення як послуга)	38,567	46,331	55,143	64,870	75,734
Послуги менеджменту та безпеки	7,150	8,768	10,427	12,159	14,004
IaaS (Інфраструктура як послуга)	25,290	34,603	45,559	57,897	71,552
Хмарна реклама	90,257	104,516	118,520	133,566	151,091
Загальний ринок	209,244	246,841	287,820	332,723	383,355

Високі темпи зростання (23%) в 2016 році також показав сегмент SaaS (програмне забезпечення як послуга), обсяг якого склав \$ 38,6 млрд.

За словами Сіда Нага, компанії вибирають хмарні рішення за їх гнучкість, масштабованість, інноваційність і можливості для зростання бізнесу і скорочення витрат. У дослідженні також йдеться про те, що в 2016 році реалізація PaaS-рішень (платформа як послуга) вимірювалася \$ 7,2 млрд проти \$ 3,8 млрд роком раніше. Доходи в сегментах хмарної реклами, BPaaS-сервісів (бізнес-процеси як послуга) і послуг хмарного управління і безпеки склали 90,3; 40,8 і 7,2 млрд доларів відповідно.

Аналітики прогнозували, що в 2016 році компанії у всьому світі витратять на публічні хмарні послуги \$ 204 млрд. Це на 16,5% більше, ніж у 2015 році (\$ 175 млрд), прогнозував Gartner. Для порівняння, світовий ринок ІТ в цілому в 2016 р. виріс всього на 0,6%. Таким чином, темп зростання

ринку публічних хмарних сервісів в 27,5 разів перевищує темп зростання ІТ-ринку в цілому.

Найбільше зростання, за очікуваннями Gartner, продемонструє сегмент «інфраструктура як послуга» (Infrastructure as a Service - IaaS). За підрахунками аналітиків, в 2016 р. зростання цього напрямку в грошовому вираженні склало 38,4%. Хмарна реклама - найбільший сегмент світового ринку хмарних послуг – продемонстрував 13,6-зростання в 2016 р. і досяг \$ 90,3 млрд. Тоді як обсяг сегмента IaaS - \$ 22,4 млрд.

У IDC, в свою чергу, називають найбільшим сегментом «програмне забезпечення як послугу» (Software as a Service - SaaS). Передбачається, що в найближчі роки на цей вид хмарних сервісів доведеться більше, ніж дві третини всього ринку в грошовому вираженні. При цьому річний темп зростання сегмента IaaS, згідно IDC, складе в середньому 27% в період з 2015 по 2019 рр, а сегмента «платформа як послуга» (Platform as a Service - PaaS) - 30,6%.

IDC вважали, що до 2017 р. 35% всіх додатків будуть розгортатися в хмарі, а виручка від публічних хмарних сервісів зросте на 22,8% в рік протягом найближчих декількох років, що в 6 разів вище темпів зростання традиційних ІТ-продуктів.

У лютому 2016 року аналітики Synergy Research Group опублікувала результати дослідження світового ринку хмарних сервісів. Його обсяг, як з'ясували фахівці, збільшується повільніше в порівнянні з темпами зростання лідерів. Згідно з оцінками Synergy Research, ринок сервісів для розгортання хмарних інфраструктур (включаючи рішення IaaS, PaaS, а також приватні та гібридні хмарні рішення) виріс на 52% в 2015 році, досягнувши 23 млрд доларів.

Найбільшим хмарним провайдером залишилася Amazon, яка записала в актив ринкову частку в розмірі 31%. Ті, що йдуть слідом Microsoft і IBM сильно відстають від лідера, маючи 9- і 7-процентні показники відповідно. У

п'ятірку кращих за підсумками 2015 року також увійшли Google (4%) і Salesforce (4%).

Як відзначають фахівці, Amazon продовжує зміцнювати позиції і нарощувати частку на ринку незважаючи на те, що конкуренти Microsoft і Google ростуть набагато швидше. У жовтні-грудні 2015 року їхня виручка на ринку хмарних інфраструктурних сервісів підвищилися на 124% і 108% відповідно, в той час як бізнес Amazon зріс на 63%. Крім того, IBM показала підйом на 57%, Salesforce - на 40%. Чотири найбільші гравці контролюють більше половини хмарного ринку і ростуть швидше його, говориться в дослідженні.

Аналітики IDC дали оцінку обсягу і структури світового ринку публічних хмарних сервісів в 2014 році. Згідно з оцінкою експертів, в 2014 році загальносвітові витрати на публічні хмари досягли \$ 56,6 млрд, де на частку рішень SaaS припала виручка в розмірі \$ 39,8 млрд. Частину ринку поділили продукти IaaS (\$ 8,7 млрд) і PaaS (\$ 8,1 млрд).

Домінування сегмента SaaS експерти пояснюють тим, що основний попит на ринку публічних хмар зосереджений навколо додатків. При цьому PaaS і рішення в області хмарного зберігання даних є найбільш швидко зростаючими категоріями завдяки збільшенню популярності засобів аналітики великих даних (Big Data) і інтернет-сервісів для розробників, йдеться в звіті IDC.

За прогнозами аналітиків, до 2018 року компанії і споживачі витратять на рішення PaaS близько \$ 20,3 млрд. Найбільшим сегментом ринку публічних хмар залишиться SaaS, де виручка буде вимірюватися \$ 82,7 млрд, що більш ніж в три рази перевищить сектор IaaS (очікуваний обсяг - \$ 24,3 млрд).

Таким чином, в 2018 році на ринку публічних хмарних сервісів матимуть місце інвестиції в розмірі \$ 127,5 млрд, а їх розмір до цього часу буде збільшуватися в середньому на 22,8% в рік, що в шість разів більше прогнозованого зростання глобального ІТ ринку. Очікується, що в 2018 році

на частку публічних хмар доведеться більше половини показника зростання витрат на програмне забезпечення, сервери та системи зберігання даних в світі.

Цьому прогресу сприяють як самі вендори, які ставлять в основу хмарні стратегії, так і їх клієнти, які охоче впроваджують нові рішення. В IDC вважають, що індустрія хмарних сервісів вийшла на «інноваційний етап», який подарує величезну кількість нових продуктів і забезпечить їм додаткову вартість.

У міру розвитку інновацій на хмарному ринку буде посилюватися і конкуренція, а це, в свою чергу, може привести до консолідації компаній. Наприклад, найбільший виробник дискових сховищ EMC часто згадується аналітиками та учасниками ринку в якості потенційної мети для поглинання вертикальними хмарними постачальниками, пише видання EnterpriseTech.

Forrester прогнозує бурхливе зростання ринку хмарних обчислень. Аналітична компанія Forrester Research прогнозує, що з 2011 по 2020 рік обсяг світового ринку «хмарних» обчислень виросте в шість разів - з 40,7 мільярдів доларів до, більш ніж 241 мільярда. При цьому вартість «публічної хмари» (додатків і послуг, що доставляються через Інтернет) за той же період збільшиться ще більше - з 25,5 мільярдів доларів до 159,3 мільярдів доларів.

До 2020 року, за прогнозами аналітиків Forrester Research, обсяг світового ринку хмарних сервісів досягне \$ 191 млрд. Нагадаємо, що три роки тому фахівці говорили про \$ 159 млрд. Світовий ринок платформних сервісів до 2020 року виросте до \$ 44 млрд, а обсяг сектора хмарних бізнес-сервісів збільшиться до \$ 14 млрд, сегмент SaaS досягне \$ 131 млрд.

До драйверів зростання ринку «хмар» можна віднести також збільшення кількості підприємств, в яких керівники прагнуть поліпшити адаптованість без істотного збільшення витрат, надаючи мобільним користувачам більше можливості для роботи, поєднуючи функціональність і модернізовані додатки. Сьогодні все більше компаній використовують

хмарні технології не як додаток до IT-інфраструктури, а як повну заміну класичним локальним рішенням.

Що стосується питання витрат, необхідних для переходу на хмарні технології, то він більш складний, ніж здається на перший погляд. Дійсно, робота в хмарі обходиться компаніям значно дешевше, однак витрати на міграцію, особливо для великих компаній, можуть бути дуже істотними.

Таким чином, за результатами досліджень приходимо до висновку, що перехід до хмарних технологій - не короткочасна акція, а довгострокова стратегія розвитку IT-інфраструктури. Правильно обрана політика в сфері хмарних технологій допоможе компаніям більш гнучко вести бізнес, підвищити продуктивність праці, спростити взаємодію між співробітниками і клієнтами, розкрити потенціал віддаленої роботи і знизити капітальні витрати. Однак успіх переходу в хмару, як і будь-якого іншого стратегічного починання, залежить від вибору постачальників, партнерів та взаємовідносин.

4.5 Економічні ефекти використання хмарних технологій

При переході на хмарні технології, можемо спостерігати наступні ефекти: економічний ефект полягатиме в скороченні необхідності в обслуговуванні та підтримці серверів, що скоротить кількість системного персоналу. Зниження витрат на обслуговування віртуальної інфраструктури, викликане розвитком технологій віртуалізації, за рахунок чого потрібен менший штат для обслуговування всієї IT інфраструктури підприємства. Оплата фактичного використання ресурсів, користувач хмари платить за фактичне використання обчислювальних потужностей хмари, що дозволяє йому ефективно розподіляти свої грошові кошти. Це дозволяє користувачам (підприємствам) заощаджувати на купівлі ліцензій до ПО. Використання хмари на правах оренди дозволяє користувачам знизити витрати на закупівлю дорогого устаткування, і зробити акцент на вкладення грошових

коштів на налаштування бізнес процесів підприємства, що в свою чергу дозволяє легко почати бізнес. Розвиток апаратної частини обчислювальних систем, в зв'язку з чим зниження вартості обладнання. З точки зору інформаційного ефекту, дозволяє компаніям отримати досить гнучку і динамічну інфраструктуру. Але її перевагами вони зможуть скористатися тільки в тому випадку, якщо відмовляться від процесів і методів роботи, які застосовуються для традиційних центрів обробки даних. Інакше всі ресурси та інвестиції виявляться марними. Що стосується безпеки, то хмарні сервіси мають досить високу безпеку при належному її забезпеченні, однак при недбалому ставленні ефект може бути повністю протилежним.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Аналіз потенційних небезпек

Темою диплома є «Дослідження та аналіз сучасних методів та засобів захисту хмарних обчислень». Робота проводиться в офісі, у якому забезпечується підтримка працездатності сервісів, робота з документами та персоналом. Для забезпечення комфортних умов праці проводиться контроль за дотриманням санітарних норм та державних стандартів з охорони праці.

Основними потенційними небезпеками при проведенні робіт в офісі є такі:

1. Небезпека ураження електричним струмом, внаслідок недотримання правил електробезпеки або виходу з ладу електроприладів;
2. Порушення роботи кістково-м'язового апарату внаслідок тривалих статичних навантажень при роботі з ПК.
3. Нервово-психічні перевантаження внаслідок постійного контакту з клієнтами, колегами по роботі, керівництвом при вирішенні робочих питань, які можуть носити конфліктний характер і призвести до емоційного дискомфорту, внутрішнього роздратування, емоційної нестабільності та захворювань нервової системи;
4. Незадовільні ергономічні характеристики робочого місця внаслідок нераціонального планування робочого місця, що може призвести до механічних травм, уражень електричним струмом та порушень кістково-м'язового апарату;
5. Негативний вплив недостатнього освітлення робочої зони на зір та продуктивність роботи працюючого, внаслідок несправності освітлювальних приладів або неправильного проектування освітлювальної системи;

6. Негативний вплив незадовільних параметрів повітряного середовища робочої зони на здоров'я працюючого, внаслідок неправильного проектування системи вентиляції або несправності її несправності;

7. Негативний вплив підвищеного рівня шуму на психоемоційний стан працюючого, який пов'язаний з використанням застарілої периферійної техніки, кондиціонерів, копіювальної техніки, освітлювальних приладів;

8. Небезпека загоряння у зв'язку із несправністю електричного обладнання, недотримання, або порушення правил протипожежної безпеки обслуговуючим персоналом, що може призвести до пожежі.

9. Неправильні дії персоналу у надзвичайних ситуаціях.

5.2 Заходи щодо забезпечення безпеки

Приміщення офісу, в яких перебувають співробітники, відносяться до приміщень без підвищеної небезпеки ураження електричним струмом.

Обладнання, що використовується в цих приміщеннях є споживачем електроенергії, що живиться від змінного струму 220 В від мережі з заземленою нейтраллю, та відноситься до електроустановок до 1000В закритого виконання. За способом захисту людини від ураження електричним струмом відповідає згідно з ГОСТ 12.2.007.0-75* (2001) «ССБТ. Изделия электротехнические. Общие требования безопасности» І (стаціонарні комп'ютери,) та ІІ (освітлювальні прилади, кондиціонери, опалювальні пристрої, ноутбуки, сканери) класу захисту.

Згідно «Правилам улаштування електроустановок» (далі «ПУЕ») виконані такі групи заходів з електробезпеки:

Використано конструктивні заходи для забезпечення захисту від випадкового дотику до струмопровідних частин за допомогою їх ізоляції та захисних оболонок.

Згідно з ГОСТ 12.1.009-76 (1999) «ССБТ. Электробезопасность. Термины и определения» у приладах ІІ класу захисту використовується

подвійна ізоляція - електрична ізоляція, що складається з робочої і додаткової ізоляції.

Так як згідно з НПАОП 40.1-1.32-01 «Правила устрою електроустановок. Электрооборудование специальных установок» офісні приміщення у більшості своїй відносяться до класу пожежебезпечної зони П-Па (приміщення, в яких містяться тверді горючі речовини), тому передбачений ступінь захисту ізоляції обладнання IP44.

Призначені для забезпечення захисту від ураження електричним струмом при дотику до металевих оболонок, які можуть опинитися під напругою в результаті аварій.

Згідно з ГОСТ 12.1.030-81 (2001) «ССБТ. Электробезопасность. Защитное заземление, зануление» у приміщеннях влаштовано занулення.

Експлуатація електроустановок і електроустаткування проводиться відповідно до НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок» (далі «ПБЕЕ») та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів» (далі «ПБЕЕС»). Для запобігання статистичного навантаження при користуванні ПК використовуються перерви в роботі 10 хв. через кожні дві години. Синдром зап'ястного каналу, або тунельний синдром зап'ястя, який може бути наслідком хронічної травми, трапляється у людей внаслідок тривалої роботи з мишею: постійні напруга і здавлювання приводить до мікротравм, здавлювання нерва прилеглими оточуючими тканинами, через що виникає набряк.

Щоб попередити тунельний синдром контролюється дотримання таких правил організації робочого місця:

- оптимальна висота клавіатури від підлоги – 65-75 см;
- наявність ергономічних і зручних миші і клавіатури;
- можливість регулювання висоти і нахилу клавіатури (відстань від поверхні стола до середини клавіатури – не більше 30 мм, кут підйому клавіатури – від 2° до 15°);

- наявність у клавіатури підставки для рук;
- наявність килимка для миші з захистом від тунельного синдрому (спеціальний виступ забезпечує правильне положення кисті);
- наявність стільця або крісла з підлокітниками;

При роботі з мишкою і клавіатурою також проводиться дотримання певних правил. При наборі тексту, рука повинна бути зігнута в лікті під прямим кутом (90°), а при роботі з мишкою кисть була прямою і лежала на столі якнайдалі від краю.

Щоб попередити тунельний синдром проводяться регулярні спеціальні вправи для кистей. Ці вправи допоможуть поліпшити кровообігу в м'язах і розтягнути їх. Комплекс вправ повторюється приблизно кожні 45 хвилин, тривалість однієї вправи – 1-2 хв.

Загальні ергономічні вимоги встановлено ДСТУ ISO 9241-1:2003 «Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 1. Загальні положення». Організація робочого місця передбачає: правильне розміщення робочого місця у виробничому приміщенні; вибір ергономічно обґрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини; раціональне компонування обладнання на робочих місцях; врахування характеру та особливостей трудової діяльності.

Планування розміщення комп'ютеризованих робочих місць у приміщенні проведено із врахуванням наступних вимог:

- робочі місця з ВДТ розміщуються на відстані не менше 1 м від стіни зі світловими прорізами;
- відстань між бічними поверхнями ВДТ має бути не менше за 1,2 м;
- відстань між тильною поверхнею одного ВДТ та екраном іншого не повинна бути меншою за 2,5 м;
- прохід між рядами робочих місць має бути не меншим 1 м.

Враховано розміри меблів на комп'ютеризованих робочих місцях, зокрема робочого столу. Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» дотримано рекомендовані розміри столу для робочого місця з ВДТ становлять: висота – 725 мм, ширина – 600-1400 мм, глибина – 800-1000 мм. Робочий стіл має такі розміри: ширина – 1200 мм, глибина – 800 мм.

Комп'ютеризовані робочі місця розміщено рядами вздовж стіни з вікнами. Це дає змогу унеможливити дзеркальне відбиття на екрані ВДТ джерел природного світла (вікон) та потрапляння останніх у поле зору операторів, що погіршує умови їх зорової роботи.

5.3 Заходи щодо виробничої санітарії та гігієни праці

Згідно ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення» в офісних приміщеннях використано природне та штучне освітлення. Природне освітлення здійснено через світлові прорізи, які забезпечують коефіцієнт природної освітленості (КПО) не нижче 1,5%. Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски на поверхні екранів і клавіатури, використано сонцезахисні пристрої, на вікнах встановлені жалюзі. Штучне освітлення в приміщенні здійснено системою загального рівномірного освітлення. Значення освітленості на поверхні робочого столу в зоні розміщення документів становить 300-500 лк. Як джерела штучного освітлення в приміщенні застосовуються люмінесцентні лампи типу ЛБ

Розрахунок освітлення проводиться для кімнати площею 60м², довжиною - 10м, шириною – 6м і висотою - 3 м. Скористаємося методом світлового потоку.

Для визначення кількості світильників визначимо світловий потік, падаючий на поверхню за формулою:

де Φ – світловий потік, лм;

E - нормована мінімальна освітленість, Лк (визначається за таблицею). Роботу програміста, відповідно до цієї таблиці, можна віднести до розряду точних робіт, отже, мінімальна освітленість буде $E = 300 \text{ лк}$;

S - площа освітлюваного приміщення (у нашому випадку $S = 60 \text{ м}^2$);

Z - відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1,1 ... 1,2, нехай $z = 1,1$);

k_z - коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення залежить від типу приміщення і характеру проведених в ньому робіт і в нашому випадку $k_z = 1,5$);

η - коефіцієнт використання, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в частках одиниці; залежить від характеристик світильника, розмірів приміщення, фарбування стін і стелі, які характеризуються коефіцієнтами відображення від стін (РС) і стелі (РП)), значення коефіцієнтів РС і РП: РС = 40%, РП = 60%.

Значення η визначимо по таблиці коефіцієнтів використання різних світильників. Для цього обчислимо індекс приміщення по формулі:

де S - площа приміщення, $S = 60 \text{ м}^2$;

h - розрахункова висота підвісу, $h = 2.2 \text{ м}$;

A - довжина приміщення, $A = 10 \text{ м}$;

B - ширина приміщення, $B = 6 \text{ м}$.

Підставивши наявні значення у формулу, отримаємо $I = 0.45$

Знаючи індекс приміщення I , $\eta = 0,17$

Підставимо усі значення в формулу (5.1) для визначення світлового потоку і отримаємо $\Phi = 174705$ лм.

Для освітлення вибираємо люмінесцентні лампи типу ЛБ58, світловий потік яких $\Phi = 4320$ лк.

Враховуючи наявні дані, для освітлення офісного приміщення використовуємо 22 світильники, розміщені по 11 у кожному ряді, з загальною кількістю ламп – 44.

Показники мікроклімату в офісних приміщеннях відповідають встановленим санітарно-гігієнічним вимогам ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны» і ГН 2152-80 «Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих та громадських приміщень».

Роботи в приміщеннях офісу, належать до категорії Іб - легка робота, тому встановлені наступні оптимальні значення параметрів мікроклімату:

- у холодний період року: температура 21-23 °С; відносна вологість: 40-60%; швидкість переміщення повітря: 0,1 м/с;
- у теплий період року: температура 22-24 °С; відносна вологість: 40-60%; швидкість переміщення повітря: 0,2 м/с.

Оптимальні рівні позитивних (n^+) і негативних (n^-) іонів у повітрі приміщення з ПК нормовані згідно ГН 2152-80 «Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих та громадських приміщень» і становлять: $n^+ = 1500-30000$ (шт. на 1см^3); $n^- = 3000-5000$ (шт. на 1см^3).

Підтримка оптимального рівня легких позитивних і негативних аероіонів у повітрі на робочих місцях забезпечено за допомогою біполярних коронних аероіонізаторів.

Дотримання вимог цих документів досягається оснащенням приміщень і транспортних засобів пристроями кондиціонування і вентиляції,

дезодорації повітря, опалювання згідно вимог ДБН В.2.5-67:2013 «Опалення, вентиляція та кондиціонування».

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях у приміщення нормуються згідно ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» та ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

Зниження рівня шуму в приміщенні здійснено за допомогою:

- використання більш сучасного обладнання;
- розташування принтерів та різноманітного устаткування колективного користування на значній відстані від більшості робочих місць працівників;
- переведення жорсткого диска в режим сну (Standby), якщо комп'ютер не працює протягом визначеного часу;
- використання блоків живлення ПК з вентиляторами на гумових підвісках.

5.4 Заходи з пожежної безпеки

Закон України «Про пожежну безпеку» визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності.

Пожежна безпека - стан об'єкта, при якому з регламентованою ймовірністю виключається можливість виникнення та розвиток пожежі і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей.

Для ліквідації пожежі у початковій стадії її розвитку силами персоналу об'єктів застосовуються первинні засоби пожежогасіння. До них

відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, ящики з піском, пожежні відра, совкові лопати, ломи, сокири тощо), системи автоматичного пожежогасіння.

Первинні засоби пожежогасіння, в залежності від категорії приміщень, можуть розташовуватись як окремо, так і в складі пожежних щитів.

Залежно від агрегатного стану й особливостей горіння різних горючих речовин і матеріалів пожежі за ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва» поділяються на відповідні класи.

Для забезпечення пожежної безпеки в установі проводимо пожежну профілактику, яка включає в себе комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження її поширення, а також на створення умов для успішного гасіння пожежі.

В офісному приміщенні знаходиться дерев'яна мебель, електронна апаратура, паперові носії інформації.

Клас пожежі у офісному приміщенні (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») – пожежі твердих речовин, переважно органічного походження, горіння яких супроводжується тлінням (деревина, пластмаси, папір) - визначається як клас А. Категорія приміщення (згідно із НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою») – визначається як категорії Д.

Визначення типу та розрахунок кількості первинних засобів пожежогасіння (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») – для офісного приміщення площею 50м² до 150м² включно застосовуються чотири порошкових вогнегасники типу ВП–5 (НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою»). ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва»). Крім цього

адміністративні приміщення обладнані автоматичними пожежними сповіщувачами, що реагують на підвищення температури, дим, полум'я моделей ДТЛ, ІТМ.

Згідно з ДБН В.1.1-7-2002. "Пожежна безпека об'єктів будівництва" на випадок пожежі передбачені шляхи евакуації працюючих - проходи, проїзди, евакуаційні виходи. Згідно з п. 13 "Рекомендацій по складанню планів евакуації людей на випадок пожежі" план евакуації розміром формату А4 розміщено на видному місці під склом (плівкою).

Згідно з НАПБ Б.02.005-2003 "Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України" працівники пройшли інструктаж з пожежної безпеки та ознайомлені з евакуаційними заходами при пожежі.

5.5 Заходи безпеки у надзвичайних ситуаціях

Укриття населення у захисних спорудах цивільного захисту та евакуаційні заходи.

1. До захисних споруд цивільного захисту належать:

а) сховище - герметична споруда для захисту людей, в якій протягом певного часу створюються умови, що виключають вплив на них небезпечних факторів, які виникають внаслідок надзвичайної ситуації, воєнних (бойових) дій та терористичних актів;

б) протирадіаційне укриття - негерметична споруда для захисту людей, в якій створюються умови, що виключають вплив на них іонізуючого опромінення у разі радіоактивного забруднення місцевості;

в) швидкостпурджувана захисна споруда цивільного захисту - захисна споруда, що зводиться із спеціальних конструкцій за короткий час для захисту людей від дії засобів ураження в особливий період.

2. Для захисту людей від деяких факторів небезпеки, що виникають внаслідок надзвичайних ситуацій у мирний час, та дії засобів ураження в особливий період також використовуються споруди подвійного призначення та найпростіші укриття. Споруда подвійного призначення - це наземна або підземна споруда, що може бути використана за основним функціональним призначенням і для захисту населення. Найпростіше укриття - це фортифікаційна споруда, цокольне або підвальне приміщення, що знижує комбіноване ураження людей від небезпечних наслідків надзвичайних ситуацій, а також від дії засобів ураження в особливий період.

3. Укриттю підлягають:

1) у сховищах:

а) працівники найбільшої працюючої зміни суб'єктів господарювання, віднесених до відповідних категорій цивільного захисту та розташованих у зонах можливих значних руйнувань населених пунктів, які продовжують свою діяльність в особливий період;

б) персонал атомних електростанцій, інших ядерних установок і працівники суб'єктів господарювання, які забезпечують функціонування таких станцій (установок);

в) працівники найбільшої працюючої зміни суб'єктів господарювання, віднесених до категорії особливої важливості цивільного захисту та розташованих за межами зон можливих значних руйнувань населених пунктів, а також працівники чергового персоналу суб'єктів господарювання, які забезпечують життєдіяльність міст, віднесених до відповідних груп цивільного захисту;

г) хворі, медичний та обслуговуючий персонал закладів охорони здоров'я, які не підлягають евакуації або не можуть бути евакуйовані у безпечне місце;

2) у протирадіаційних укриттях:

а) працівники суб'єктів господарювання, віднесених до першої та другої категорій цивільного захисту та розташованих за межами

зон можливих значних руйнувань населених пунктів, які продовжують свою діяльність у воєнний час;

б) працівники суб'єктів господарювання, розташованих у зонах можливих руйнувань, небезпечного і значного радіоактивного забруднення навколо атомних електростанцій;

в) населення міст, не віднесених до груп цивільного захисту, та інших населених пунктів, а також населення, евакуйоване з міст, віднесених до груп цивільного захисту і зон можливих значних руйнувань;

г) хворі, медичний та обслуговуючий персонал закладів охорони здоров'я, розташованих за межами зон можливих значних руйнувань міст, віднесених до груп цивільного захисту, і суб'єктів господарювання, віднесених до категорій цивільного захисту, а також закладів охорони здоров'я, які продовжують свою діяльність у воєнний час;

3) у швидкоспоруджуваних захисних спорудах цивільного захисту, найпростіших укриттях та спорудах подвійного призначення - населення міст, віднесених до груп цивільного захисту, яке не підлягає евакуації у безпечне місце, а також інших населених пунктів.

4. Для вирішення питань щодо укриття населення в захисних спорудах цивільного захисту центральні органи виконавчої влади, Рада міністрів Автономної Республіки Крим, місцеві державні адміністрації, органи місцевого самоврядування та суб'єкти господарювання завчасно створюють фонд таких споруд.

5. Порядок створення, утримання фонду захисних споруд цивільного захисту та ведення його обліку визначається Кабінетом Міністрів України.

6. Проектування, будівництво, пристосування і розміщення захисних споруд та об'єктів подвійного призначення здійснюються згідно з нормами, які розробляються відповідно до Закону України "Про будівельні норми".

7. Вимоги щодо утримання та експлуатації захисних споруд визначаються центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту.

8. Утримання захисних споруд цивільного захисту у готовності до використання за призначенням здійснюється суб'єктами господарювання, на балансі яких вони перебувають (у тому числі споруд, що не увійшли до їх статутних капіталів у процесі приватизації (корпоратизації), за рахунок власних коштів.

9. У разі використання однієї захисної споруди кількома суб'єктами господарювання вони беруть участь в утриманні споруди відповідно до укладених між ними договорів.

10. Захисні споруди цивільного захисту можуть використовуватися у мирний час для господарських, культурних і побутових потреб у порядку, що визначається Кабінетом Міністрів України.

11. З моменту виключення захисної споруди із фонду споруд цивільного захисту вона втрачає статус захисної споруди цивільного захисту. Володіння, користування та розпорядження спорудами, які втратили статус захисних споруд цивільного захисту, здійснюється відповідно до закону.

12. Захисні споруди цивільного захисту державної та комунальної власності не підлягають приватизації (відчуженню).

13. Захисні споруди у мирний час можуть передаватися в оренду для задоволення господарських, культурних та побутових потреб із збереженням цільового призначення таких споруд, крім тих, що перебувають у постійній готовності до використання за призначенням, а саме:

- а) в яких розташовані пункти управління;
- б) призначених для укриття працівників суб'єктів господарювання, що мають об'єкти підвищеної небезпеки;
- в) розташованих у зонах спостереження атомних електростанцій та призначених для укриття населення під час радіаційних аварій.

14. Особливості оренди захисних споруд визначаються типовим договором оренди, який затверджується Кабінетом Міністрів України.

15. Контроль за готовністю захисних споруд цивільного захисту до використання за призначенням забезпечує центральний орган виконавчої влади, який здійснює державний нагляд у сферах техногенної та пожежної безпеки, спільно з відповідними органами та підрозділами цивільного захисту, місцевими державними адміністраціями.

ВИСНОВКИ

У ході проведення досліджень в області хмарних технологій стояла задача аналізу наявних сучасних хмарних сервісів.

Було досліджено наявні методи захисту в хмарних сервісах, проведено аналіз компонентів технології, можливих загроз та способів протидії атакам. Запропоновано оптимальні сервіси в залежності від потреб користувача.

В першій частині було розглянуто переваги та недоліки використання хмарних технологій, види послуг що надаються хмарними сервісами. Завдяки наведеним даним історії та ключовим факторам розвитку, які доповнюються кількісними значеннями, очевидно стабільний розвиток та зростання ринку хмарних послуг, що підтверджує актуальність проведеної роботи.

Для розуміння функціоналу технологій було наведено послуги, що надаються користувачам, визначена класифікація хмарних сервісів.

У другій частині для повного розуміння небезпек, що загрожують користувачам хмарних сервісів було досліджено загрози та можливі атаки на різні компоненти хмарних сервісів. Виходячи з наведених загроз, було представлено сучасні способи захисту вразливостей кожного з компонентів хмарного сервісу для запобігання небажаних наслідків як, наприклад, втрата даних користувача, перехоплення повідомлень чи недоступність послуг що надаються через різні причини.

В ході роботи був складений список постачальників хмарних послуг та методів захисту в різних сервісах. Розглянуто кілька типових задач і порівнюються їх можливі рішення на кожній з платформ Amazon, Google, Windows.

Була проведена оцінка ефективності капіталовкладень в захист хмарних обчислень в умовах розвитку цифровізації економіки. Ринок ІТ-технологій у даному напрямі демонструє стабільний розвиток та ріст, так, за даними IDC, опублікованим 22 червня 2018 року, у 2017 році обсяг глобального ринку публічних хмарних сервісів у грошовому вираженні склав

близько \$ 117 млрд. Зважаючи на наведені дані, хмарні технології будуть і надалі розвиватися приваблюючи ще більшу кількість компаній готових вкладати гроші та користувачів, що будуть підтримувати попит на сервіси та послуги.

Було сформовано порівняльну таблицю хмарних сервісів з різними способами захисту що використовуються в кожному з сервісів.

В якості результату роботи було надано порівняльну таблицю хмарних сервісів, визначено оптимальні продукти для клієнтів з різними потребами в забезпеченні безпеки та можливості спільної роботи користувачів. Були запропоновані рішення для підвищення ефективності захисту хмарних технологій такі як використання технологій, в основі яких лежить збір даних з унікальної глобальної мережі сенсорів виявлення загроз і поширення цієї інформації по шлюзах безпеки в усьому світі, міжмережеві екрани нового покоління, що представляють собою не тільки стандартний функціонал брандмауера і VPN, але включають також нові технології, такі як безпечний віддалений доступ, в тому числі з мобільних пристроїв, розширена ідентифікація користувачів, DLP, контроль додатків, фільтрація URL, антибот і антивіруси, де все це управляється з єдиної консолі. Також як один з варіантів підвищення захищеності хмарних технологій було запропоновано створення кампанії з проведення спільної роботи постачальників хмарних послуг над єдиним відкритим стандартом створення та забезпечення надійної роботи і захисту хмарних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Облачные вычисления, краткий обзор или статья для начинающих. [Электронный ресурс] Habrahabr – Режим доступа: <https://habr.com/post/111274/>
2. Кононюк, А. Е. Облачные технологии / А. Е. Кононюк – Київ: «Освіта України», 2018. – Книга 1 – 621 с.
3. Обеспечение безопасности данных при использовании облачных технологий [Электронный ресурс] Первая миля – Режим доступа: <http://www.lastmile.su/journal/article/3823>
4. Угрозы облачных вычислений и методы их защиты. [Электронный ресурс] Habrahabr – Режим доступа: <https://www.lektorium.tv/lecture/13538>
5. Откуда взялись «облака» и какими они бывают? [Электронный ресурс] Rusbase – Режим доступа: <https://rb.ru/opinion/raznye-oblaka/>
6. Памятка: Как стартапам обеспечить защиту данных в облаке. [Электронный ресурс] Habr – Режим доступа: <https://habr.com/company/1cloud/blog/243001/>
7. Кононюк, А. Е. Облачные технологии / А. Е. Кононюк – Київ: «Освіта України», 2018. – Книга 2 – 526 с.
8. Специальные цифровые решения. [Электронный ресурс] SDS – Режим доступа: <http://sds.co.ua/data-tsentry.html/>
9. Суть облачных технологий и их классификация. [Электронный ресурс] – Режим доступа: https://studbooks.net/2016302/informatika/sut_oblachnyh_tehnologiy_klassifikatsiya
10. Как супер компьютеры объединяются в сеть. [Электронный ресурс] – Режим доступа: <https://www.kv.by/content/kak-superkompyutery-obedinyayutsya-v-seti>

11. Простыми словами: Разбираемся с облачными услугами. [Электронный ресурс] – Режим доступа: <https://habr.com/company/1cloud/blog/280376/>

12. Памятка: Как стартапам обеспечить защиту данных в облаке. [Электронный ресурс] – Режим доступа: <https://habr.com/company/1cloud/blog/243001/>

13. Газета InfoSecurity.ru [Электронный ресурс] – Режим доступа: http://www.infosecurity.ru/_gazeta//130614.shtml

14. Розділ "Охорона праці та безпека у надзвичайних ситуаціях" у дипломних проектах (роботах) спеціалістів [Електронний ресурс] – Режим доступу: <http://www.zntu.edu.ua/pryklady-oformlennya-dokumentiv-6>

15. Парадигма безопасности облачных вычислений [Электронный ресурс] – Режим доступа: <http://itzashita.ru/oblachnyievyichisleniya/paradigma-bezopasnosti-oblachnyih-vyichisleniy.html>