Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Розробка рекомендацій захисту хмарних сервісів»

Виконавець: студент IV курсу, групи КБ-41
_____ Архипов Ярослав Анатолійович
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Ігніска В.І	

Нормоконтроль	Даков С. Ю.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-41** **Архипова Ярослава Анатолійовича**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Розробка рекомендацій захисту хмарних сервісів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція хмарних обчислень та сервісів

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією хмарних обчислень та сервісів, моделями розгортання, сервісними моделями та вразливостями. Розробити рекомендації захисту хмарних сервісів.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Поєднання різних методів захисту хмарних сервісів та формування рекомендацій.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав		В. І. Ігніска
	(підпис)	(ініціали, прізвище)
Завдання прийняла до виконання		Я. А Архипов
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 27.01.2021	*виконано*
2	Аналіз літератури	28.01.2021– 11.02.2021	*виконано*
3	Аналіз нормативно-правового забезпечення	12.02.2021 – 24.02.2021	*виконано*
4	Розгляд моделей розгортання та сервісних моделей	25.02.2021 – 24.03.2021	*виконано*
5	Дослідження вразливостей та загроз	25.03.2021 – 21.04.2021	*виконано*
6	Порівняння безпеки хмарних провайдерів	22.04.2021 – 08.05.2021	*виконано*
7	Вироблення рекомендацій щодо захисту хмарних сервісів	09.05.2021 – 17.05.2021	*виконано*
8	Оформлення пояснювальної записки	18.05.2021 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Завдання видав		В. І. Ігніска
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання		Я. А Архипов
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Розробка рекомендацій захисту хмарних сервісів» складається зі списку скорочень, вступу, основної частини, що містить 3 розділи, висновків, списку літератури та джерел. Загальний обсяг роботи – 67 сторінок. Робота містить 6 рисунків та 2 таблиці. Список використаних джерел включає 32 джерела.

Метою даної роботи є огляд структури побудови хмарних сервісів, оцінка їх поточного стану захищеності та розробка рекомендацій щодо захисту хмарних сервісів.

У роботі проаналізовано існуюча література з хмарних обчислень, виконаний аналіз стандартів, порівняння, вивчення практики з теми хмарних технологій, розроблено рекомендації щодо захисту хмарних сервісів.

Розроблені рекомендації призначені для користувачів, що хочуть забезпечити безпеку своїх персональних даних в хмарних сервісах.

Ключові слова: Хмарні сервіси, хмарні обчислення, стандарти інформаційної безпеки, безпека хмарних технологій, захист даних, хмарні технології.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІТС	–	Інформаційно-телекомунікаційна система
АС	–	Автоматизована система
КСЗІ	–	Комплексна система захисту інформації
ЦОД	–	Центр обробки даних
ПЗ	–	Програмне забезпечення
ТЗІ	–	Технічний захист інформації
БД	–	База даних
ІТ	–	Інформаційні технології
СУІБ	–	Система управління інформаційною безпекою
CISA	–	Cybersecurity & Infrastructure Security Agency
CISM	–	Certified Information Security Manager
CRISC	–	Certified in Risk and Information Systems Control
CGEIT	–	Certified in the Governance of Enterprise IT
IaaS	–	Infrastructure-as-a-Service
PaaS	–	Platform-as-a-Service
SaaS	–	Software-as-a-Service
CRM	–	Customer relationship management
ERP	–	Enterprise resource planning
VPC	–	Virtual Private Cloud
API	–	Application programming interface
WAF	–	Web Application Firewall
DLP	–	Data Loss Prevention
IAM	–	Identity and Access Management
GCP	–	Google Cloud Platform
ASC	–	Accounting Standards Codification
AWS	–	Amazon Web Services
AI	–	Artificial intelligence
DDoS	–	Distributed denial-of-service
SLA	–	Service Level Agreement
ISO	–	International Organization for Standardization
CSA	–	Cloud Security Alliance

NIST	–	National Institute of Standards and Technology
CENELEC	–	European committee for electrotechnical standardization
ISMS	–	Information Security Management System
IEC	–	International Electrotechnical Commisson
CCAK	–	Certificate of Cloud Auditing Knowledge
CCSK	–	Certificate of Cloud Security Knowledge
ISACA	–	Information Systems Audit and Control Association
ISSA	–	Information Systems Security Association International
ANSI	–	American National Standards Institute
CISCO	–	Commercial & Industrial Security Corporation
ETSI	–	European Telecommunications Standards Institute
CEN	–	Cloud Enterprise Network
PCI / DSS	–	Payment Card Industry Data Security Standard

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тим, що на даний момент практично кожен користувач стикається у своїй роботі з хмарними обчисленнями.

В даний час інформація є одним з найбільш важливих ресурсів. При цьому обробка і зберігання інформації потребує значної кількості потужності обчислювальних машин. Тому вимоги до них збільшуються з вражаючою швидкістю. А разом з тим і вартість. У зв'язку зі стрімким розвитком технологій бездротового доступу відпала необхідність розташування комплексу засобів обробки і зберігання інформації безпосередньо на території організації і стала можливою дистанційна робота з даними. Це дало перший поштовх до виникнення хмарних сервісів.

І тому дуже важливо щоб уся інформація була ретельно захищена.

Метою даної роботи є огляд структури побудови хмарних сервісів, оцінка їх поточного стану захищеності та розробка рекомендацій щодо захисту хмарних сервісів.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- Розглянути особливості побудови хмарних обчислень та сервісів;
- Дослідити проблематику захисту інформації хмарних обчислень та сервісів;
- Розглянути існуючі методи захисту інформації хмарних обчислень та сервісів;

Об'єктом дослідження в даній роботі є процес захисту даних в хмарних сервісах.

Предметом дослідження в даній роботі є методи, засоби і методики захисту хмарного середовища.

Практична цінність - поєднання різних методів захисту хмарних сервісів та формування власних рекомендацій.

Методи дослідження дипломної роботи:

- аналіз літератури;

- аналіз стандартів;
- аналіз побудови хмарних сервісів;
- аналіз структури хмарних сервісів;
- порівняння захисту хмарних сервісів від різних постачальників.

РОЗДІЛ 1
НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ

1.1 Актуальність хмарних обчислень

Хмарні обчислення – одна з найтехнологічніших інновацій 21 століття. Це спричинено постійним зростанням кількості пристроїв, які можуть отримати доступ до Інтернету. Хмарні обчислення призначені не лише для організацій та бізнесу. Це корисно для будь-якої людини. Хмарні обчислення вплинули на глобальний розвиток не лише IT-індустрії, але й бізнесу, фінансів, державного управління, медицини, освіти і багатьох інших сфер людського життя. Вони дозволяють нам запускати програми, не встановлюючи їх на наших пристроях. Можемо зберігати та отримувати доступ до нашого мультимедійного вмісту через Інтернет, це дозволяє нам розробляти та тестувати програми без необхідності мати сервери тощо. Хмарні обчислення - це диво 21 століття, яке використовується майже в усіх сферах, про які ми можете подумати.

В основному, нам потрібні хмарні обчислення через численні індивідуальні та ділові проблеми, з якими ми стикаємось сьогодні. Ці проблеми варіюються від придбання та обслуговування дорогих апаратних та програмних ресурсів, які ми використовуємо у своїй щоденній діяльності, до найефективнішого впорядкування цих ресурсів на нашу користь та на благо суспільства в цілому. Вирішуючи ці виклики, хмарні обчислення дають численні переваги, які перевершили наші очікування і забезпечили більше, ніж ми думали раніше.

Переваги можна класифікувати за трьома категоріями, а саме:

1.1.1 Ефективність

Ефективність досягається наступними способами:

- Доступність. Хмарні обчислення полегшують доступ до програм та даних з будь-якого місця в усьому світі та з будь-якого пристрою, що має Інтернет-з'єднання.

- Економія витрат. Хмарні обчислення пропонують підприємствам масштабовані обчислювальні ресурси. Економія на витратах на їх придбання та обслуговування. Платити потрібно лише за те, цим користуєшься. Це набагато дешевше, ніж самостійно купувати.

- Безпека. Хмарні провайдери, особливо ті, що пропонують приватні хмарні послуги, запровадили найкращі стандарти та процедури безпеки, щоб захистити дані клієнта, збережені в хмарі.

- Аварійне відновлення. Хмарні обчислення пропонують найефективніші засоби для малих, середніх і навіть великих підприємств для швидкого та надійного резервного копіювання та відновлення своїх даних та програм.

1.1.2 Гнучкість

Гнучкість досягається наступними способами:

- Масштабованість. Хмарні обчислення - найкращий варіант для підприємств з коливаннями робочих навантажень, оскільки хмарна інфраструктура масштабується залежно від потреб бізнесу.

- Вибір інструментів. Хмарні обчислення дозволяють компаніям вибрати конкретні попередньо побудовані інструменти та функції для пошуку рішень, адаптованих до їх конкретних потреб.

- Хмарні параметри. Хмарні обчислення пропонують приватні, загальнодоступні та гібридні хмарні рішення, кожна з яких має різні функції. Організації можуть вибрати ці варіанти залежно від того, що найкраще відповідає їх потребам.

1.1.3 Стратегічна цінність

Хмарні обчислення дозволяють компаніям отримати стратегічну перевагу у своїй ніші наступними способами:

- Підвищена продуктивність праці. Постачальники хмарних послуг купують та управляють базовою хмарною інфраструктурою, що дозволяє бізнесу зосереджувати свої сили на своїх основних бізнес-операціях.
- Автоматичне оновлення програмного забезпечення. Усі послуги, доступ до яких відбувається через хмару, як правило, оновлюються. Це дозволяє користувачам отримувати доступ до найновіших функцій без необхідності самостійно підтримувати систему.
- Конкурентоспроможність. Підприємства, що використовують хмарні обчислення, можуть маневрувати більш спритно у порівнянні з конкурентами, які віддають свої сили придбанню та підтримці IT-ресурсів.

Беручи до уваги численні переваги, які хмарні обчислення пропонують організаціям, можна сказати, що хмарні обчислення все частіше стають новою нормою. Хмарні обчислення допомагають суспільству впоратися з майбутніми проблемами, такими як управління великими даними, кібербезпека та контроль якості. На додаток до цього, нові технології, такі як штучний інтелект, технологія розподіленого реєстру та багато інших можливостей, стають доступними як послуги за допомогою хмарних обчислень. Остаточним вердиктом хмарних обчислень є те, що це трансформаційна технологія, яка допомогла організаціям з різних юрисдикцій доставляти свої товари та послуги кращим чином, ніж раніше.

1.2 Важливість безпеки хмарних технологій

Хмарна безпека є критично важливою, оскільки більшість організацій вже використовують хмарні обчислення в тій чи іншій формі. Компанії переносять більше даних та додатків у хмару, IT-фахівці залишаються стурбованими

проблемами безпеки, управлінням та дотриманням вимог. Адже надзвичайно конфіденційна, ділова інформація та інтелектуальна власність можуть бути піддані випадковому витоку інформації або кібератаці.

Запобігання витоку інформації та крадіжці даних має вирішальне значення для збереження довіри клієнтів та захисту активів, що сприяють конкурентним перевагам.

Підтримання сильної позиції безпеки в хмарі допомагає організаціям досягти загальновизнаних переваг хмарних обчислень: зниження початкових витрат, зменшення поточних операційних та адміністративних витрат, простота масштабування, підвищена надійність та доступність, а також абсолютно новий спосіб роботи.

1.3 Нормативно-правові документи

Визначивши переваги та чому потрібно захищати хмарні обчислення перейдемо до класифікації та аналізу організацій та органів, які розробляють нормативно-правові документи для хмарних обчислень. Вони створюють міжнародні стандарти і мають наступну ієрархію рівнів:

1. Міжнародний (ISO/IEC);
2. Міждержавний (форуми і консорціуми (Cisco, CSA));
3. Регіональний (європейські органи ETSI, CEN / CENELEC);
4. Національний (закони та державні стандарти, відомчі нормативні документи, керівництва, інструкції, наприклад: (NIST).

1.3.1 Стандарт. Стандарт інформаційної безпеки

Стандарт безпеки схожий на будь-який інший стандарт будь-якої іншої галузі. Стандарт - це загальний набір правил, визначень та узгоджених «регламентів», на які всі сторони можуть посилатися для загальної довідки. Стандарт є набором мінімальних вимог, яким повинна відповідати організація, щоб заявити про

відповідність стандарту. Стандарти сприяють спрощенню життя, підвищенню надійності та ефективності товарів та послуг, якими ми користуємось.

Стандарти надають нам загальний набір контрольних точок, щоб ми могли оцінити, чи існує в організації процеси, процедури та інші засоби контролю, які відповідають узгодженим мінімальним вимогам. Якщо організація відповідає вимогам та відповідає певним стандартам, то вона надає третім сторонам, таким як замовники, постачальники та партнери, впевненість у здатності цієї організації дотримуватися цього стандарту. Це також може забезпечити організації конкурентні переваги перед іншими організаціями. Наприклад, організація, яка відповідає стандартам безпеки, може мати перевагу перед конкурентом, який цього не робить, коли клієнти оцінюють їх продукцію чи послуги. Використовуючи стандарт для створення міцної основи для управління та захисту ваших систем, вам буде легше відповідати новим вимогам регулювання, ніж організація, яка цього не робить.

Певні нормативно-правові вимоги можуть визначати певні стандарти, яким необхідно дотримуватися. Наприклад, якщо ваша компанія обробляє кредитні картки, ви повинні відповідати стандарту PCI DSS Data Security. Цей стандарт є стандартом, визначеним найбільшими компаніями, що займаються кредитними картками, такими як VISA та Mastercard. Якщо ви не відповідаєте цьому стандарту, вас можуть штрафувати, стягувати більш високі збори за обробку, або ці компанії, що видають кредитні картки, можуть відмовити вам у бізнесі.

Щоб врегулювати усі підходи до проблеми створення захищених систем були розроблені стандарти інформаційної безпеки – це документи, які визначають основні поняття та суть інформаційної безпеки на державному та міждержавному рівнях, визначають поняття “захищена система” шляхом стандартизації вимог та критеріїв безпеки, які формують шкалу оцінки ступеня захищеності інформаційної системи. Присутність стандартів дозволяє регулювати потреби користувачів та замовників інформаційних систем з якісними характеристиками програмного забезпечення, що створюють розробники інформаційних систем.

1.3.1 Стандарти ISO/IEC

ISO (Міжнародна організація зі стандартизації) - це всесвітня федерація національних органів зі стандартів (органи-члени ISO). Робота з підготовки міжнародних стандартів зазвичай проводиться через технічні комітети ISO. Кожен орган-член, для якого створено технічний комітет, має право бути представленим у цьому комітеті. У роботі беруть участь також міжнародні організації, урядові та неурядові, що підтримують зв'язок з ISO. ISO тісно співпрацює з Міжнародною електротехнічною комісією (IEC) з усіх питань електротехнічної стандартизації.

ISO підтримує експертний комітет, присвячений розробці міжнародних стандартів систем управління інформаційною безпекою, інакше відомих як сімейство стандартів Системи управління інформаційною безпекою (ISMS).

Застосовуючи сімейство стандартів ISMS, організації можуть розробити та впровадити систему управління безпекою своїх інформаційних активів, включаючи фінансову інформацію, інтелектуальну власність та дані про співробітників, або інформацію, довірену їм клієнтами або третіми сторонами. Ці стандарти також можуть бути використані для підготовки до незалежної оцінки їх СУІБ, що застосовуються до захисту інформації.

Сімейство стандартів ISMS включає стандарти, які:

а) визначають вимоги до СУІБ та до тих, хто сертифікує такі системи;

b) надає пряму підтримку, детальне керівництво та інтерпретацію загального процесу створення, впровадження, підтримки та вдосконалення СУІБ;

в) враховує галузеві настанови щодо СУІБ;

г) звертається до оцінки відповідності СУІБ.

ISO/IEC 27001 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»

ISO / IEC 27001 - це міжнародний стандарт щодо управління інформаційною безпекою. Спочатку стандарт був опублікований спільно з Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) у 2005 р., а потім переглянутий у 2013 р. У ньому детально викладено вимоги

щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) - метою якої є допомогти організаціям зробити інформаційні активи, якими вони володіють, більш захищеними.

Більшість організацій мають ряд засобів контролю інформаційної безпеки. Однак без системи управління інформаційною безпекою (СУІБ) засоби управління, як правило, дезорганізовані та роз'єднані, часто застосовуються як рішення конкретних ситуацій або просто як умова. Засоби контролю безпеки, що функціонують, зазвичай стосуються певних аспектів інформаційних технологій (ІТ) або безпеки даних. Залишаючи інформаційні активи, що не належать до ІТ (такі як документи та власні знання), в цілому менш захищеними. Більше того, плануванням безперервності бізнесу та фізичною безпекою можна керувати цілком незалежно від ІТ чи інформаційної безпеки, тоді як практика управління персоналом може мало посилатися на необхідність визначення та розподілу ролей та відповідальності за інформаційну безпеку в організації.

ISO / IEC 27001 вимагає, щоб управління:

- Систематично вивчало ризики інформаційної безпеки організації, беручи до уваги загрози, вразливості та наслідки;

- Розробило та впровадило послідовний та всебічний набір засобів контролю інформаційної безпеки або інші форми лікування ризиків (таких як уникнення ризику або передача ризику) для вирішення тих ризиків, які визнані неприйнятними;

- Прийняти всебічний процес управління, щоб забезпечити, щоб засоби управління інформаційною безпекою продовжували задовольняти потреби організації в галузі інформаційної безпеки на постійній основі.

Те, які засоби контролю будуть перевірені в рамках сертифікації за ISO / IEC 27001, залежить від аудитора сертифікації. Це може включати будь-які засоби контролю, які організація вважала такими, що входять до сфери застосування СУІБ, і це тестування може здійснюватися на будь-яку глибину або ступінь, за оцінкою аудитора, якщо це необхідно для перевірки того, що контроль був впроваджений та діє ефективно.

Керівництво визначає сферу застосування СУІБ для цілей сертифікації та може обмежити її, скажімо, окремим бізнес-підрозділом або місцем розташування.

ISO/IEC 27002 «Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки»

ISO / IEC 27002 - це стандарт інформаційної безпеки, опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). ISO / IEC 27002 надає рекомендації щодо найкращих практик щодо засобів контролю інформаційної безпеки для використання тими, хто відповідає за ініціювання, впровадження або підтримку систем управління інформаційною безпекою (СУІБ). Інформаційна безпека визначена в рамках стандарту в контексті тріади:

- збереження конфіденційності (забезпечення того, щоб інформація була доступна лише тим, хто має дозвіл на доступ);
- цілісності (забезпечення точності та повноти інформації та методів обробки);
- доступності (забезпечення доступу уповноважених користувачів до інформації та пов'язаних з нею активів, коли це потрібно).

Сфера дії:

Цей міжнародний стандарт надає вказівки щодо організаційних стандартів інформаційної безпеки та практики управління інформаційною безпекою, включаючи вибір, впровадження та управління засобами контролю, беручи до уваги середовище (ризики) захисту інформації.

Цей міжнародний стандарт призначений для використання організаціями, які мають намір:

а) вибрати елементи контролю в процесі впровадження Системи управління інформаційною безпекою на основі ISO / IEC 27001;

б) впроваджувати загальновизнані засоби контролю інформаційної безпеки;

в) розробити власні керівні принципи управління інформаційною безпекою.

Вимоги до інформаційної безпеки.

Важливо, щоб організація визначила свої вимоги до безпеки. Є три основні джерела вимог безпеки:

а) оцінка ризиків для організації з урахуванням загальної ділової стратегії та цілей організації. За допомогою оцінки ризику визначаються загрози активам, оцінюється вразливість та ймовірність виникнення та оцінюється потенційний вплив;

б) юридичні, статутні, нормативні та договірні вимоги, яким повинна відповідати організація, її торгові партнери, підрядники та постачальники послуг, а також їх соціально-культурне середовище;

в) сукупність принципів, цілей та бізнес-вимог щодо обробки, зберігання, передачі та архівування інформації, яку організація розробила для підтримки своєї діяльності.

Ресурси, що використовуються для впровадження засобів контролю, повинні бути збалансовані проти шкоди для бізнесу, яка, можливо, буде спричинена проблемами безпеки, якщо таких засобів контролю не буде. Результати оцінки ризиків допоможуть направити та визначити відповідні управлінські дії та пріоритети для управління ризиками інформаційної безпеки та для здійснення контролю, обраного для захисту від цих ризиків.

Інформація має природний життєвий цикл - від створення та походження через зберігання, обробку, використання та передачу до її можливого знищення або розпаду. Вартість активів та ризики для них можуть змінюватися протягом усього життя (наприклад, несанкціоноване розголошення або розкрадання фінансових рахунків компанії набагато менш значні після їх офіційного опублікування), але інформаційна безпека залишається важливою до певної міри на всіх етапах.

Інформаційні системи мають життєві цикли, в рамках яких вони розробляються, уточнюються, випробовуються, впроваджуються, використовуються, підтримуються і врешті-решт виходять з експлуатації та утилізуються. Інформаційну безпеку слід враховувати на кожному етапі. Нові системні розробки та зміни існуючих систем представляють можливість

організаціям оновлювати та вдосконалювати засоби контролю безпеки, беручи до уваги фактичні інциденти та поточні прогнозовані ризики інформаційної безпеки.

ISO/IEC 27004 «Інформаційні технології. Методи безпеки. Управління інформаційною безпекою. Моніторинг, вимірювання, аналіз та оцінка»

ISO / IEC 27004 - це стандарт інформаційної безпеки, опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Цей документ призначений допомогти організаціям оцінити ефективність інформаційної безпеки та ефективність системи управління інформаційною безпекою з метою виконання вимог ISO / IEC 27001: 2013, 9.1: моніторинг, вимірювання, аналіз та оцінка.

Результати моніторингу та вимірювання системи управління інформаційною безпекою (СУІБ) можуть бути підтримкою рішень, що стосуються управління СУІБ, управління, операційної ефективності та постійного вдосконалення.

Як і у випадку з іншими документами ISO / IEC 27000, цей документ слід розглядати, інтерпретувати та адаптувати відповідно до конкретної ситуації кожної організації. Поняття та підходи мають бути широко застосовними, але конкретні заходи, які вимагає будь-яка конкретна організація, залежать від контекстуальних факторів (таких як її розмір, сектор, зрілість, ризики інформаційної безпеки, зобов'язання щодо дотримання та стиль управління), які на практиці широко варіюються.

Цей документ рекомендується організаціям, які впроваджують СУІБ, що відповідає вимогам ISO / IEC 27001. Однак він не встановлює жодних нових вимог до СУІБ, які відповідають ISO / IEC 27001 або накладають будь-які зобов'язання на організації дотримуватися представлених настанов.

Сфера дії

Цей документ містить керівні принципи, спрямовані на допомогу організаціям в оцінці ефективності інформаційної безпеки та ефективності системи управління інформаційною безпекою з метою виконання вимог ISO / IEC 27001: 2013, 9.1. Він встановлює:

а) моніторинг та вимірювання ефективності інформаційної безпеки;

b) моніторинг та вимірювання ефективності системи управління інформаційною безпекою (СУІБ), включаючи її процеси та засоби управління;

в) аналіз та оцінка результатів моніторингу та вимірювання.

Цей документ застосовується до всіх типів та розмірів організацій.

ISO/IEC 27005 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки»

ISO / IEC 27005 - це міжнародний стандарт, опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), що надає рекомендації щодо передової практики щодо управління ризиками для інформації. Це основна частина стандартів серії ISO / IEC 27000, широко відомих як ISO27k.

Стандарт пропонує поради щодо систематичного виявлення, оцінки та лікування ризиків інформаційної безпеки - процесів, що лежать в основі системи управління інформаційною безпекою ISO27k (СУІБ). Вона спрямована на забезпечення того, щоб організації раціонально розробляли, впроваджували, управляли, контролювали та підтримували свої засоби управління інформаційною безпекою та інші механізми відповідно до своїх ризиків інформаційної безпеки.

ISO / IEC 27005 не вказує та не рекомендує детально конкретні методи управління ризиками. Натомість він обговорює процес у більш загальному плані, спираючись на загальний метод управління ризиками, описаний у ISO 31000, тобто:

- Виявити та оцінити ризики;
- Вирішіть, що робити з ризиками (як їх «лікувати»);
- Моніторинг ризиків, лікування ризиків, виявлення та відповідне реагування на значні зміни, проблеми чи можливості для вдосконалення;
- Інформує зацікавлені сторони (головним чином керівництво організації) протягом всього процесу.

Організаціям пропонується відбирати, розробляти та використовувати ті методи, стратегії та підходи щодо управління інформаційним ризиком, які найкраще відповідають їхнім конкретним потребам - наприклад:

- Визначення можливостей різних інцидентів, ситуацій або сценаріїв, які можуть поставити під загрозу або зашкодити конфіденційності, цілісності та доступності інформації;

- Оцінка загроз, вразливості всередині та наслідків для бізнесу, що потенційно можуть виникнути внаслідок інцидентів, що стосуються IT-систем та мереж, а також ручна обробка інформації, інформація на папері або виражена словами та малюнками, плюс нематеріальна інформація, така як знання, інтелектуальна власність тощо;

- Визначення абсолютних або відносних значень різних форм, типів або категорій інформації для організації, зокрема інформації та обробки інформації, що є критично важливою для досягнення важливих бізнес-цілей;

- Застосування, адаптація методів та підходів до управління ризиками, які вже використовуються організацією, прийняття передової практики або розробка нових гібридних підходів;

- Розстановка пріоритетів відповідно до значущості або характеру ризиків, а також економічної ефективності чи інших наслідків розглядуваних методів лікування ризиків, планування їх відповідного лікування, розподілу ресурсів тощо;

- Зменшення інформаційних ризиків шляхом зменшення їх вірогідності та впливу різними способами, наприклад вибір автоматизованого, ручного, фізичного чи адміністративного контролю, який є превентивним, детективним або коригувальним;

- Вирішення невизначеностей, у тому числі тих, що знаходяться в самому процесі управління ризиками (наприклад, виникнення непередбачуваних інцидентів, нещасних збігів, помилок судження та часткової або повної відмови контролю);

- Дотримання відповідних вимог або зобов'язань, які накладаються на організацію або добровільно приймаються організацією за допомогою різних законів, положень, контрактів, угод, стандартів, кодексів тощо (наприклад, закони про конфіденційність, PCI-DSS, етичні та екологічні міркування).

ISO / IEC 27017 «Інформаційні технології. Керівництво по заходам інформаційної безпеки для використання сервісів хмарних обчислень»

SO / IEC 27017 - це стандарт безпеки, розроблений для постачальників хмарних послуг та користувачів, щоб зробити безпечніше хмарне середовище та зменшити ризик проблем із безпекою. Він був опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) в рамках спільного підкомітету ISO та IEC, ISO / IEC JTC 1 / SC 27. Він є частиною сімейства стандартів ISO / IEC 27000, що містить рекомендації щодо найкращих практик щодо управління інформаційною безпекою. Цей стандарт був побудований на основі ISO/IEC 27002, пропонуючи додаткові засоби контролю для хмари, які не були повністю визначені в ISO/IEC 27002.

Цей міжнародний стандарт надає вказівки, що підтримують впровадження засобів контролю інформаційної безпеки для клієнтів хмарних служб, які впроваджують елементи керування, та постачальників хмарних послуг для підтримки впровадження цих засобів управління. Вибір відповідних засобів контролю інформаційної безпеки та застосування наданих вказівок щодо впровадження залежатиме від оцінки ризику та будь-яких юридичних, договірних, регуляторних чи інших специфічних вимог до інформаційної безпеки у хмарному секторі.

ISO/IEC 27017 надає вказівки щодо засобів управління інформаційною безпекою, що застосовуються до використання хмарних служб, надаючи додаткові вказівки щодо впровадження для 37 елементів керування, зазначених у ISO / IEC 27002 та 7 додаткових засобів контролю, пов’язаних із хмарними послугами, які стосуються наступного:

- Хто за що відповідає між постачальником хмарних послуг та хмарним клієнтом.
- Вилучення або повернення активів в кінці договору.
- Захист та відокремлення віртуального середовища замовника.
- Конфігурація віртуальної машини.
- Адміністративні операції та процедури, пов'язані з хмарним середовищем.
- Хмарний моніторинг діяльності клієнтів.
- Вирівнювання середовища віртуальної та хмарної мережі.

ISO / IEC 27018 «Звід практик щодо заходів захисту персональних даних при наданні публічних хмарних послуг»

ISO / IEC 27018 є стандартом безпеки, що входить до сімейства стандартів ISO / IEC 27000. Це був перший міжнародний стандарт щодо конфіденційності послуг хмарних обчислень. Він був створений у 2014 році як додаток до ISO / IEC 27001, першого міжнародного кодексу практики щодо конфіденційності у хмарі. Це допомагає постачальникам хмарних послуг, які обробляють особисту інформацію, оцінити ризик та запровадити засоби контролю для захисту. Він був опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) в рамках спільного підкомітету ISO та IEC, ISO / IEC JTC 1 / SC 27.

Завдання цього документа, який використовується разом із цілями та засобами управління інформаційною безпекою в ISO / IEC 27002, полягає у створенні загального набору категорій безпеки та засобів контролю, які можуть бути реалізовані постачальником послуг загальнодоступних хмарних обчислень, що діє як процесор ідентифікації персональних даних. Він має наступні цілі:

- Допомогти постачальнику хмарних послуг виконувати діючі зобов'язання, виконуючи обов'язки процесора, що ідентифікує персональні дані, незалежно від того, покладаються ці зобов'язання на процесор персональних даних безпосередньо або за контрактом.

- Увімкнути публічний хмарний процесор ідентифікації персональних даних, щоб він був прозорим у відповідних питаннях, щоб клієнти хмарних послуг могли вибирати добре керовані хмарні послуги обробки ідентифікаційних даних.

- Надати клієнтам хмарних послуг механізм здійснення прав та обов'язків щодо аудиту та дотримання вимог у випадках, коли окремі аудитори даних хмарних служб, розміщені у багатопартійному, віртуалізованому серверному (хмарному) середовищі, можуть бути непрактичними з технічної точки зору та можуть збільшити ризики для цих фізичних та логічних мереж.

ISO / IEC 17788 «Інформаційні технології. Розподілені прикладні платформи і сервіси. Хмарні обчислення. Загальні положення та словник»

Стандарт описує концепцію хмарних обчислень і містить ряд термінів і визначень. Він є термінологічної основою для подальшої роботи по стандартизації в сфері хмарних обчислень.

ISO / IEC 17789 «Інформаційні технології. Хмарні обчислення. Еталонна архітектура»

Стандарт містить огляд загальних понять і характеристик хмарних обчислень, типів хмар, компонентів хмарних обчислень сторін-учасниць, а також взаємовідносини між цими елементами. У ньому зроблено наголос на вимоги до того, що повинні забезпечувати хмарні сервіси, а не на питання проектування і впровадження відповідних рішень.

ISO / IEC 27040 «Інформаційні технології. Безпека зберігання даних»

Стандарт містить детальні технічні рекомендації щодо того, як організаціям визначити відповідний рівень заходів зниження ризиків шляхом планування, розробки та реалізації системи безпеки при зберіганні даних. У ньому дано огляд загальних уявлень про безпеку при зберіганні даних і відповідні визначення, а також рекомендації, що стосуються типових технологій і сценаріїв зберігання. Стандарт застосовується при забезпеченні безпеки пристроїв і носіїв та відповідних положень управлінської діяльності, а також при забезпеченні безпеки додатків і сервісів. В ньому охоплюються питання безпеки, пов'язані з кінцевими користувачами.

1.3.2 Стандарти CSA

Cloud Security Alliance (CSA) - це провідна організація у світі, яка займається визначенням та підвищенням обізнаності щодо найкращих практик, які допоможуть забезпечити безпечне середовище хмарних обчислень. CSA використовує експертні знання галузевих практиків, асоціацій, урядів та корпоративних та окремих членів, щоб запропонувати спеціальні хмарні дослідження, освіту, сертифікацію, події та продукти. Діяльність CSA, знання та розгалужена мережа приносять вигоду всій спільноті, на яку впливає хмара - від постачальників та споживачів, до уряду, підприємців та індустрії страхування - та забезпечують форум, за допомогою якого різні сторони можуть спільно працювати над створенням та підтримкою довіреної хмарної екосистеми.

CSA оперує найпопулярнішою програмою сертифікації постачальників хмарних служб - CSA Security, Trust & Assurance Registry (STAR), трирівневою програмою забезпечення оцінки, незалежного аудиту та постійного моніторингу. CSA також керує CSA Global Consulting Program, професійною програмою, яку вона розробила, що дозволяє хмарним користувачам працювати з мережею надійних фахівців із безпеки та організацій, які пропонують кваліфіковані професійні послуги на основі найкращих практик CSA.

CCSK

По мірі того, як організації переходять на хмарні сервіси, їм потрібні фахівці з інформаційної безпеки, які мають досвід роботи в хмарі. Сертифікат CCSK є загальновизнаним стандартом знань щодо хмарної безпеки. Повноваження CCSK є основою для підготовки вас до отримання додаткових хмарних облікових даних.

Працівники, які зазвичай використовують знання, отримані завдяки CCSK, включають аналітика хмарних обчислень, хмарного адміністратора, хмарного архітектора, хмарного інженера, архітектора підприємств, адміністратора безпеки, архітектора безпеки та системного інженера.

Сертифікація визнає знання, вміння та навички кандидата. Обсяг сертифікату є вужчим і надає лише підтвердження закінчення навчального курсу.

Сертифікація надає кандидату доступ до членської організації і майже завжди вимагає щорічного зобов'язання щодо постійної професійної освіти (CPE) для підтримки сертифікації.

CCAK

Сертифікат знань хмарного аудиту (CCAK) є першим посвідченням, доступним для професіоналів галузі, щоб продемонструвати свій досвід у основних принципах аудиту систем хмарних обчислень. Програма сертифікатів та навчання CCAK заповнює прогалину на ринку технічної освіти для хмарного IT-аудиту.

Цей документ використовує хмарний досвід CSA та традиційний аудиторський досвід ISACA, поєднуючи досвід для розробки та надання найкращого можливого рішення для навчання хмарного аудиту. CCAK приносить користь як членам CSA та ISACA, так і власникам сертифікації, оскільки він базується на сукупності знань, викладених у Сертифікаті знань про хмарну безпеку (CCSK) CSA, та доповнює акредитовані ISSAA сертифікати ANSI, такі як CISA, CISM, CRISC та CGEIT.

Організація, яка використовує хмарні обчислення, матиме зовсім інший підхід до задоволення цілей контролю. Орендар хмарних послуг, безумовно, не матиме такого ж адміністративного доступу, як у застарілій IT-системі, і використовуватиме широкий спектр засобів контролю, який буде чужим для фахівців з аудиту та гарантій, що базується на традиційній практиці аудиту IT.

CCAK доповнює та вдосконалює навички та знання в таких повноваженнях:

- Сертифікат знань про хмарну безпеку (CCSK);
- Сертифікований аудитор інформаційних систем (CISA);
- Кваліфікований оцінювач безпеки PCI / DSS;
- Повноваження провідного аудитора ISO 27001.

1.3.3 Стандарти NIST

Національний інститут стандартів і технологій (NIST) був заснований в 1901 році і зараз є частиною Міністерства торгівлі США. NIST - одна з найстаріших

лабораторій фізичної науки в країні. Конгрес створив агентство для усунення головного виклику промисловій конкурентоспроможності США на той час - інфраструктури вимірювання другого рівня, яка відставала від можливостей Сполученого Королівства, Німеччини та інших економічних конкурентів. Починаючи від розумної електромережі та електронних медичних записів, закінчуючи атомними годинниками, вдосконаленими наноматеріалами та комп'ютерними чіпами, незліченна кількість продуктів та послуг певним чином покладається на технології, вимірювання та стандарти, надані Національним інститутом стандартів та технологій. Сьогодні вимірювання NIST підтримують від найменших технології до найбільших і найскладніших створених людиною творінь - від наномасштабних пристроїв, настільки крихітних, що десятки тисяч можуть поміститися на кінці одного людського волосся до стійких до землетрусів хмарочосів та глобальних комунікаційних мереж.

До основних стандартів, що стосуються хмарних технологій, відносяться:

- NIST SP 800-145 та NIST SP 800-146, які визначають поняття хмарних обчислень та надають загальні рекомендації з їх використання.

- NIST SP 500-292 та NIST SP 500-293, які визначають хмарну архітектуру, основні її компоненти та механізми взаємодії між ними.

-NIST SP 500-292 «Базова архітектура хмарних обчислень» – це керівництво, що містить модель архітектури та словник, які не залежать від постачальника хмарних послуг. У ньому визначено п'ять ролей (діючих осіб): споживач послуг, постачальник послуг, брокер, аудитор і оператор. Для них і описані словник і базова архітектура. Перехідним на використання хмарних обчислень державним органам рекомендується слідувати викладеним в керівництві визначенням і положенням, щоб забезпечити узгоджене впровадження хмарних послуг.

- NIST SP 800-144 «Керівництво по забезпеченню безпеки і захисту персональних даних при використання публічних хмарних обчислень». Керівництво містить огляд проблем в області безпеки і захисту недоторканності приватного життя, що виникають при використанні публічних хмар, і рекомендації, які слід взяти до уваги організаціям при аутсорсингу даних, додатків та інфраструктури в

середовищі публічної хмари. В анотації зазначається: «Даний документ дає уявлення про загрози, технологічні ризики і запобіжні заходи, що пов'язані із середовищем публічних хмарних обчислень. Це повинно допомогти організаціям приймати обґрунтовані рішення щодо використання цієї технології »

- NIST SP 500-299 «Базова архітектура забезпечення безпеки хмарних обчислень». Документ доповнює керівництво NIST SP 500-292 «Базова (референтна) архітектура хмарних обчислень» повномасштабною моделю безпеки. Ця модель визначає базовий набір компонентів забезпечення безпеки, рекомендованих для створення успішних і надійних екосистем хмарних обчислень. Документ допомагає зрозуміти взаємозалежність діючих осіб для забезпечення безпеки хмарних сервісів, а також розібратися з вимогами, які повинні сформулювати групи технічного планування і впровадження органів виконавчої влади, щоб забезпечити придбання хмарних сервісів з рівнями безпеки, що відповідають потребам.

- Стандарт NIST SP 800-125, який описує безпеку технологій повної віртуалізації. Крім того, загальні стандарти з безпеки, що розроблені NIST, застосовуються до хмарних обчислень, а саме стандарт з керування ризиками, визначення механізмів управління безпекою та конфіденційністю, а також рекомендації з управління безпекою для федеральних інформаційних систем та організацій NIST SP 800-53, безперервний моніторинг безпеки в федеральних інформаційних системах та організаціях NIST SP 800-137, запис до журналу подій безпеки (NIST SP 800-92) та інші.

Висновки за розділом 1

В першому розділі під назвою нормативно-правове забезпечення захисту хмарних сервісів я детально розглянув наступні питання:

- актуальність хмарних обчислень (детально розписав їх переваги);
- чому потрібно захищати хмарні обчислення;

- надав класифікацію організацій та органів, які розробляють нормативно-правові документи для хмарних обчислень. Та привів їх приклади, які стосуються хмарних обчислень.

РОЗДІЛ 2
ПОБУДОВА ТА СТРУКТУРА ХМАРНИХ ОБЧИСЛЕНЬ ТА СЕРВІСІВ

2.1 Хмарні обчислення та сервіси

Хмарні обчислення - модель забезпечення повсюдного та зручного доступу на вимогу через мережу до обчислювальних ресурсів, що підлягають налаштуванню (комунікаційні мережі, сервери, засоби збереження даних, прикладні програми та сервіси), які можуть бути оперативно надані з мінімальними управлінськими затратами та зверненнями до провайдера.

Хмарні сервіси - новітній вид мережевих послуг, які дозволяють інформаційними засобами віртуального середовища розширити програмно-технічні ресурси комп'ютерного пристрою користувача. Поява хмарних сервісів стала можливою у процесі розвитку технологій хмарних обчислень, які реалізуються за умов динамічного масштабного доступу до розподілених зовнішніх мережевих ресурсів.

2.2 Моделі розгортання

Існує чотири основних типи: громадська, приватна, гібридна та публічна хмари. Крім того, існують також розподілені хмари, які не настільки широко поширені, як мультихмара, поліхмара та інші моделі.

Перш ніж поглибитись в основи найпопулярніших моделей розгортання хмарних обчислень, з'ясуємо, що саме являє собою модель розгортання хмарних технологій. Модель хмарного розгортання - це конкретна конфігурація параметрів середовища, таких як доступність та власність інфраструктури розгортання та

розмір сховища. Це означає, що типи розгортання різняться залежно від того, хто контролює інфраструктуру та де вона знаходиться.

2.2.1 Публічна хмара

Загальнодоступні хмари доступні широкому загалу, а дані створюються та зберігаються на сторонніх серверах.

Серверна інфраструктура належить постачальникам послуг, які керують нею та адмініструють ресурси, саме тому користувачам не потрібно купувати та обслуговувати власне обладнання.

Публічна хмара - це, мабуть, найпростіший із усіх хмарних розгортань. Інфраструктура, сховище чи хмарні додатки віртуалізації з обладнання, що належать постачальнику, об'єднуються в пул даних, організовуються програмним забезпеченням для управління та автоматизації та передаються через Інтернет - або через спеціальне мережеве підключення - клієнту.

Переваги публічної хмари:

- Безпроблемне управління інфраструктурою. Наявність третьої сторони, яка керує вашою хмарною інфраструктурою, зручна: вам не потрібно розробляти та обслуговувати програмне забезпечення, оскільки постачальник послуг робить це за вас. Крім того, налаштування та використання інфраструктури є нескладними.
- Висока масштабованість. Ви можете легко розширити потужність хмари у міру зростання ваших вимог.
- Зниження витрат. Ви платите лише за послугу, якою ви користуєтесь, тому немає необхідності вкладати гроші в обладнання чи програмне забезпечення.
- Безвідмовна робота. Розгалужена мережа серверів вашого провайдера забезпечує постійну доступність вашої інфраструктури та покращує час роботи.

Недоліки публічної хмари:

- Проблеми безпеки та конфіденційності даних. Доступ до даних є простим, загальнодоступна модель розгортання позбавляє користувачів знання, де зберігається їх інформація та хто має до неї доступ.

- Відсутність певних послуг. Постачальники послуг мають лише стандартизовані варіанти послуг, саме тому їм часто не вдається задовольнити більш складні вимоги.

2.2.2 Приватна хмара

З технічної точки зору між публічною та приватною моделю практично немає різниці, оскільки їхні архітектури дуже схожі. Однак, на відміну від публічної хмари, яка доступна широкому загалу, лише одна конкретна компанія володіє приватною хмарою. Ось чому її ще називають внутрішньою або корпоративною моделю.

Сервер може розміщуватися зовні або в приміщенні компанії-власника. Незалежно від їх фізичного розташування, ці інфраструктури підтримуються у призначеній приватній мережі та використовують програмне та апаратне забезпечення, призначене для використання лише власником компанії.

Чітко визначений обсяг людей має доступ до інформації, що зберігається у приватному сховищі, що заважає широкому загалу користуватися нею. У світлі численних порушень за останні роки все більша кількість великих корпорацій прийняла рішення про закриту приватну хмарну модель, оскільки це мінімізує проблеми безпеки даних.

Порівняно з публічною моделю, приватна хмара надає ширші можливості для налаштування інфраструктури під вимоги компанії. Приватна модель особливо підходить для компаній, які прагнуть захистити свої критично важливі операції, або для підприємств, що постійно змінюють вимоги.

Переваги приватної хмари:

- Гнучка розробка та висока масштабованість, що дозволяє компаніям налаштовувати свою інфраструктуру відповідно до своїх вимог.

- Високий рівень безпеки, конфіденційності та надійності, оскільки лише уповноважені особи можуть отримати доступ до ресурсів.

Недоліки приватної хмари:

- Основним недоліком моделі розгортання приватної хмари є її вартість, оскільки вона вимагає значних витрат на обладнання, програмне забезпечення та навчання персоналу. Ось чому ця безпечна та гнучка модель розгортання обчислень не є правильним вибором для невеликих компаній.

2.2.3 Громадська хмара

Модель розгортання громадської хмари багато в чому нагадує приватну. Різниця лише в наборі користувачів. Тоді як приватною хмарою володіє одна компанія. В громадській хмарі кілька організацій зі схожим фоном діляться інфраструктурою та відповідними ресурсами.

Якщо всі організації, що беруть участь, мають однакові вимоги щодо безпеки, конфіденційності та продуктивності, ця архітектура центрів обробки даних для багатьох орендарів допомагає цим компаніям підвищити свою ефективність, як у випадку спільних проектів. Громадська хмара полегшує розробку, управління та реалізацію проектів. Витрати розподіляють усі користувачі.

Переваги громадської хмари:

- Зниження витрат. Оскільки громадську хмару використовують одразу декілька компаній, то і витрати розподіляються між ними.

- Покращена безпека, конфіденційність та надійність. Лише уповноважені особи можуть отримати доступ до ресурсів.

- Простота обміну даними та співпраці.

Недоліки громадської хмари:

- Висока вартість. Хоч громадська хмара використовується кількома компаніями, але її вартість все ще велика, особливо, в порівнянні з публічною хмарою.

- Спільне використання фіксованої пам'яті та пропускної здатності. Оскільки громадську хмару використовують одразу декілька компаній, тому пам'ять та пропускна здатність зменшується.

2.2.4 Гібридна хмара

Як це зазвичай буває з будь-яким гібридним явищем, гібридна хмара охоплює найкращі особливості вищезазначених моделей розгортання. Це дозволяє компаніям поєднувати три типи, які найкраще відповідають їхнім вимогам.

Як приклад, компанія може збалансувати своє навантаження, розміщуючи критично важливі робочі навантаження на захищеній приватній хмарі та розгортаючи менш чутливі на загальнодоступній. Гібридна модель розгортання хмар не тільки захищає та контролює стратегічно важливі активи, але робить це економічно та ефективно. Крім того, такий підхід полегшує перенесення даних та додатків.

Однак гібридна модель розгортання має сенс лише в тому випадку, якщо компанії можуть розділити свої дані на критично важливі та нечутливі.

Переваги гібридної хмари:

- Покращена безпека та конфіденційність. Оскільки усі критично важливі дані розміщуються у приватній хмарі.
- Доступна ціна. Самостійно можна вирішувати які і де будуть зберігатися дані.
- Покращена масштабованість та гнучкість.

2.3 Сервісні моделі

Хмарні обчислення пропонуються у трьох різних моделях обслуговування, кожна з яких відповідає унікальному набору бізнес-вимог.

2.3.1 Інфраструктура як послуга (IaaS)

Інфраструктура як послуга (IaaS) - це обчислювальна інфраструктура, яка миттєво підготовлюється і керується через Інтернет. Надає користувачам доступ до віртуальних серверів з певною обчислювальною потужністю.

IaaS швидко збільшує і зменшує масштаб за запитом, тому ви платите тільки за те, що використовуєте. Ця служба допомагає уникнути витрат і труднощів, пов'язаних з придбанням власних фізичних серверів, а також іншої інфраструктури центру обробки даних і управлінням цією інфраструктурою. Кожен ресурс надається як окремий компонент служби, і вам необхідно орендувати тільки конкретний компонент на певний час. Постачальник служб хмарних обчислень управляє інфраструктурою, а ви купуєте, встановлюєте і налаштовуєте власне програмне забезпечення (включаючи операційні системи, ПО проміжного шару і додатки), а також керуєте їми.

Ось найпоширеніші бізнес-завдання, які вирішуються завдяки IaaS:

- Тестування і розробка. Команда може швидко розгортати і демонтувати середовища тестування і розробки, швидше виводячи нові додатки на ринок. IaaS дозволяє збільшувати масштаб середовищ тестування і розробки швидко і економічно.

- Розміщення веб-сайтів. Робота веб-сайтів при використанні IaaS може бути менш витратною, ніж традиційне розгортання в Інтернеті.

- Зберігання, архівація і відновлення даних. Організації позбавляються від необхідності робити капітальні вкладення і долати труднощі, пов'язані зі зберіганням даних і управлінням сховищем, для чого звичайно потрібні висококваліфіковані фахівці з управління даними і забезпечення відповідності нормативним вимогам. IaaS дозволяє справлятися з непередбачуваним попитом і стабільно зростаючими потребами в зберіганні даних. IaaS також може легко спланувати свою систему резервного копіювання та відновлення і управління ними.

- Веб-додатки. IaaS забезпечує всю інфраструктуру для підтримки веб-додатків, включаючи сховище, веб-сервери і сервери додатків, а також мережеві ресурси. Організації можуть швидко розгортати веб-додатки на базі IaaS і легко масштабувати інфраструктуру, коли число звернень до додатків стає непередбачуваним.

- Високопродуктивні обчислення. Високопродуктивні обчислення на суперкомп'ютерах, в комп'ютерних мережах або кластерах допомагають вирішувати

складні завдання, які включають мільйони змінних і великі обсяги обчислень. Як приклади можна привести моделювання землетрусів і згортання білка, прогнози змін клімату і погоди, фінансове моделювання та оцінку проекту продукту.

- Аналіз великих даних. Інтелектуальний аналіз наборів даних для виявлення прихованих шаблонів вимагає великих обчислювальних потужностей, які може забезпечити IaaS без значного вкладення коштів.

Переваги IaaS:

- Усуває капітальні витрати і знижує поточні витрати. IaaS дозволяє уникнути попередніх витрат на розгортання локального центру обробки даних і управління ним, відкриваючи можливості для організації стартапів і компаній, що тестують нові ідеї.

- Покращує безперервність бізнес-процесів і ефективність аварійного відновлення. Реалізація високого рівня доступності, безперервності бізнес-процесів і аварійного відновлення вимагає значних витрат, так як для цього потрібно багато одиниць обладнання та співробітників. Однак завдяки правильній угоді про рівень обслуговування IaaS дозволяє знизити витрати і використовувати додатки і дані в звичайному порядку при виникненні надзвичайної ситуації або відключенні живлення.

- Швидко впроваджуйте інновації. Як тільки ви вирішите запустити новий продукт або ініціативу, необхідна обчислювальна інфраструктура буде підготовлена за хвилини або години, а не за дні або тижні, а то й місяці, як в разі внутрішньої інфраструктури.

- Реагуйте швидше на мінливі умови бізнесу. IaaS дозволяє швидко масштабувати ресурси, щоб обробляти піковий обсяг звернень такі програми, як у вихідні дні, а потім знову зменшувати обсяг виділених ресурсів при зменшенні активності, щоб заощадити кошти.

- Сконцентруйтеся на своєму бізнесі. IaaS звільняє вашу команду і дозволяє їй концентруватися не на IT-інфраструктуру, а на бізнес-завдання компанії.

- Підвищуйте стабільність і надійність системи, а також якість підтримки. Завдяки IaaS немає необхідності обслуговувати і оновлювати програмне

забезпечення та обладнання або усувати проблеми в роботі обладнання. Завдяки необхідній угоді про рівень обслуговування постачальник служб працює над тим, щоб ваша інфраструктура була надійною і відповідала вимогам угоди.

- Покращена безпека. Завдяки необхідній угоді про обслуговування постачальник хмарних служб забезпечує безпеку додатків і даних, яка може бути вищою за ту, яку ви могли б забезпечити самостійно.

- Швидше надавайте користувачам нові додатки. Оскільки вам не потрібно спочатку налаштовувати інфраструктуру, щоб розробляти і надавати додатки, при використанні IaaS ви можете швидше надавати користувачам нові додатки.

2.3.2 Платформа як послуга (PaaS)

Платформа як послуга (PaaS) - це повне середовище розробки та розгортання в хмарі з ресурсами, що дозволяють доставляти все, від простих хмарних додатків до складних корпоративних програм із підтримкою хмар. Ви купуєте потрібні вам ресурси у постачальника хмарних послуг і отримуєте доступ до них через захищене Інтернет-з'єднання. За цієї моделі провайдер надає розробникам фреймворк, на основі якого вони можуть створювати кастомізовані додатки. Провайдер контролює сервери, системи зберігання даних та мережі, тоді як розробники працюють з програмами та підтримують їх.

Як і IaaS, PaaS включає інфраструктурні сервери, сховища та мережі, також проміжне програмне забезпечення, засоби розробки, послуги бізнес-аналітики, системи управління базами даних тощо. PaaS розроблений для підтримки повного життєвого циклу веб-додатків: створення, тестування, розгортання, управління та оновлення.

PaaS дозволяє уникнути витрат та складностей придбання та управління ліцензіями на програмне забезпечення, базової інфраструктури програм та проміжного програмного забезпечення, організаторів контейнерів, засобів розробки та інших ресурсів. Ви керуєте програмами та послугами, які розробляєте, а постачальник хмарних послуг зазвичай керує усім іншим.

Організації зазвичай використовують PaaS для таких сценаріїв:

- Структура розвитку. PaaS забезпечує структуру, на якій розробники можуть спиратися на розробку або налаштування хмарних додатків. PaaS дозволяє розробникам створювати програми за допомогою вбудованих програмних компонентів. Включені такі хмарні функції, як масштабованість, висока доступність та можливості робити з декількома клієнтами, що зменшує кількість кодування, яке повинні робити розробники.

- Аналітика або бізнес-аналітика. Інструменти, що надаються як послуга з PaaS, дозволяють організаціям аналізувати та видобувати свої дані, знаходити статистичні дані та закономірності, прогнозувати результати для поліпшення прогнозування, прийняття рішень щодо проектування продукції, віддачі інвестицій та інших бізнес-рішень.

- Додаткові послуги. Постачальники PaaS можуть пропонувати інші послуги, що покращують програми, такі як робочий процес, каталог, безпека та планування.

Надаючи інфраструктуру як послугу, PaaS пропонує ті самі переваги, що і IaaS. Але додаткові функції - проміжне програмне забезпечення, засоби розробки та інші бізнес-інструменти - дають вам більше переваг:

- Скоротіть час кодування. Засоби розробки PaaS можуть скоротити час, необхідний для кодування нових програм за допомогою попередньо закодованих компонентів додатків, вбудованих у платформу, таких як робочий процес, служби каталогів, функції безпеки, пошук тощо.

- Додайте можливості розвитку без додавання персоналу. Платформа як сервісні компоненти можуть надати вашій команді розробників нові можливості без необхідності додавати персонал, який має необхідні навички.

- Розробка для багатьох платформ. Деякі постачальники послуг надають вам варіанти розробки для декількох платформ, таких як комп'ютери, мобільні пристрої та браузери, що робить крос-платформні програми швидшими та легшими в розробці.

- Використовуйте складні інструменти за доступною ціною. Дає можливість приватним особам або організаціям використовувати складне програмне

забезпечення для розробки та інструменти бізнес-аналітики та аналітики, які вони не могли дозволити собі придбати самостійно.

- Підтримка географічно розподілених команд розробників. Оскільки доступ до середовища розробки здійснюється через Інтернет, команди розробників можуть працювати разом над проектами, навіть коли члени команди знаходяться у віддалених місцях.

- Ефективне управління життєвим циклом програми. PaaS надає всі можливості, необхідні для підтримки повного життєвого циклу веб-програми: побудова, тестування, розгортання, управління та оновлення в одному інтегрованому середовищі.

2.3.3 Програмне забезпечення як послуга (SaaS)

Програмне забезпечення як послуга дозволяє користувачам підключатися та використовувати хмарні програми через Інтернет. Поширеними прикладами є електронна пошта, календар та офісні інструменти. SaaS надає повне програмне рішення. Ви берете в користування додаток для своєї організації, а користувачі підключаються до нього через Інтернет, як правило, за допомогою веб-браузера. Вся основна інфраструктура, проміжне програмне забезпечення, програмне забезпечення додатків та дані додатків знаходяться в центрі обробки даних постачальника послуг. Постачальник послуг керує апаратним та програмним забезпеченням, а відповідно до угоди про надання послуг також забезпечить доступність та безпеку програми та ваших даних. SaaS дозволяє вашій організації швидко розпочати роботу з додатком за мінімальних початкових витрат.

Поширені сценарії SaaS:

- Ніяких носіїв, драйверів і встановлень. Створюєте обліковий запис і працюєте з текстом, таблицями та презентаціями прямо в браузері. Причому в документах одночасно з вами можуть працювати і інші колеги. Виїхавши у відрядження, можна зайти в свій обліковий запис з будь-якого пристрою і

продовжити друкувати потрібний документ. При цьому зберігати потрібно тільки зміну налаштувань, інші дані зберігаються автоматично.

- Для організаційного використання ви можете орендувати додатки для підвищення продуктивності, такі як електронна пошта, календар та складні бізнес-додатки, такі як управління взаємовідносинами з клієнтами (CRM), планування корпоративних ресурсів (ERP) та управління документами. Ви платите за використання цих програм за передплатою або відповідно до рівня використання.

Переваги SaaS:

- Отримуєте доступ до складних програм. Щоб надавати користувачам додатки SaaS, вам не потрібно купувати, встановлювати, оновлювати чи обслуговувати будь-яке обладнання, проміжне чи програмне забезпечення. SaaS робить навіть складні корпоративні програми, такі як ERP та CRM, доступними для організацій, яким бракує ресурсів для самостійного придбання, розгортання та управління необхідною інфраструктурою та програмним забезпеченням.

- Платіть лише за те, що ви використовуєте. Ви також економите гроші, оскільки послуга SaaS автоматично масштабується вгору та вниз відповідно до рівня використання.

- Використовуйте безкоштовне клієнтське програмне забезпечення. Користувачі можуть запускати більшість програм SaaS безпосередньо зі свого веб-браузера, не вимагаючи завантаження та встановлення будь-якого програмного забезпечення, хоча деякі програми вимагають плагінів. Це означає, що вам не потрібно купувати та встановлювати спеціальне програмне забезпечення для своїх користувачів.

- Легко мобілізуйте свою робочу силу. SaaS дозволяє легко “мобілізувати” свою робочу силу, оскільки користувачі можуть отримати доступ до програм та даних SaaS з будь-якого підключеного до Інтернету комп’ютера чи мобільного пристрою. Вам не потрібно турбуватися про розробку програм для запуску на різних типах комп’ютерів і пристроїв, оскільки це вже зробив постачальник послуг. Крім того, вам не потрібно мати на борту спеціальні знання для управління проблемами безпеки, притаманними мобільним обчисленням. Ретельно підібраний постачальник

послуг забезпечить безпеку ваших даних, незалежно від типу пристрою, який їх споживає.

- Доступ до даних програми з будь-якого місця. За допомогою даних, що зберігаються в хмарі, користувачі можуть отримати доступ до своєї інформації з будь-якого підключеного до Інтернету комп'ютера чи мобільного пристрою. І коли дані програми зберігаються в хмарі, дані не втрачаються, якщо комп'ютер або пристрій користувача виходять з ладу.

2.3.4 Відмінність між сервісними моделями

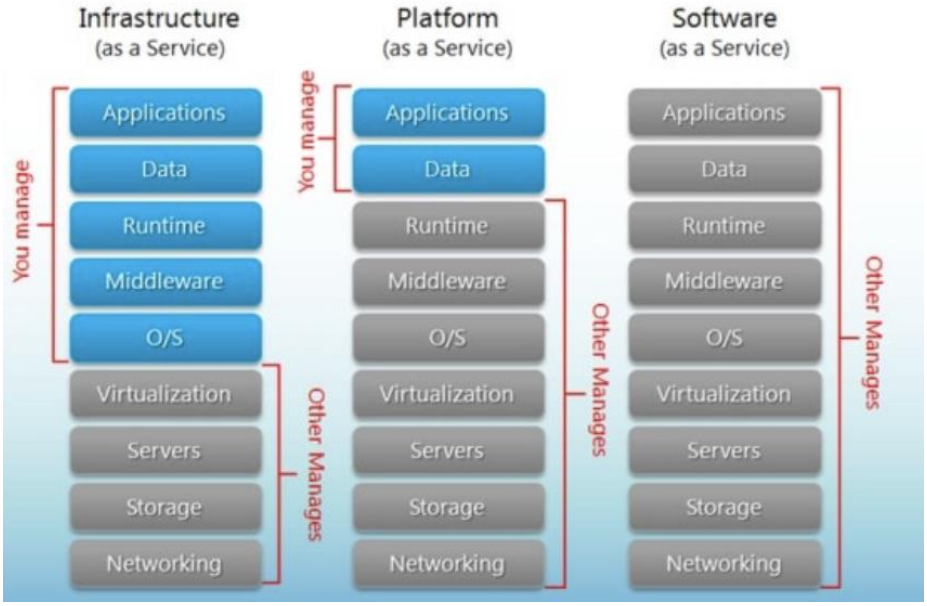

Рисунок №1 Відмінність між сервісними моделями

You manage – ви керуєте;

Other manage – керує постачальник хмарних сервісів;

Applications – програми;

Data – дані;

Runtime – час виконання;

Middleware – проміжне програмне забезпечення;

O/S – операційна система;

Virtualization – віртуалізація;

Servers – сервери;

Storage – сховища;

Networking - мережа.

2.4 Основні характеристики

З точки зору споживача, ці характеристики дозволяють отримати послуги з високим рівнем доступності і низькими ризиками непрацездатності, забезпечити швидке масштабування обчислювальної системи завдяки еластичності без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури.

Нижче наведено характеристики хмарних обчислень:

Об’єднання ресурсів

Це означає, що хмарний провайдер залучив обчислювальні ресурси для надання послуг багатьом клієнтам за допомогою багатокористувацької моделі. Постачальник послуг об'єднує ресурси для обслуговування великої кількості споживачів в єдиний пул для динамічного перерозподілу потужностей між споживачами в умовах постійної зміни попиту на потужності. При цьому споживачі контролюють тільки основні параметри послуги (наприклад, обсяг даних, швидкість доступу), але фактичний розподіл ресурсів, що надаються споживачеві, здійснює постачальник.

Самообслуговування на вимогу

Самообслуговування на вимогу означає, що споживач може запитувати та отримувати доступ до послуг без адміністратора або якогось допоміжного персоналу, який повинен виконувати запит вручну. Процеси запитів та процеси виконання автоматизовані. Це дає переваги як для постачальника, так і для споживача послуги.

Впровадження самообслуговування користувачів дозволяє клієнтам швидко виконувати запит та отримувати доступ до послуг, які вони хочуть. Це дуже

приваблива особливість хмари. Це робить необхідні ресурси дуже швидкими та простими. У традиційних середовищах запити часто виконувались днями чи тижнями, що спричиняло затримки в роботі. Вам не потрібно турбуватися про це в хмарному середовищі.

Самообслуговування користувачів також зменшує адміністративне навантаження на постачальника. Адміністратори звільняються від повсякденних дій щодо створення користувачів та управління запитами користувачів. Це дозволяє IT-співробітникам організації зосередитись на інших більш важливих питаннях.

Впровадження самообслуговування може бути важким для побудови, але для хмарних провайдерів вони безумовно коштують витрачених грошей та часу.

Простота обслуговування

Автоматичне оновлення програмного забезпечення. Усі послуги, доступ до яких відбувається через хмару, як правило, оновлюються. Це дозволяє користувачам отримувати доступ до найновіших функцій без необхідності самостійно підтримувати систему.

Широкий доступ до мережі

Однією з важливих характеристик хмарних обчислень є широкий доступ до мережі. Користувачі мають можливість отримати необхідну інформацію з будь-якого місця та з будь-якого пристрою. Користувачі можуть отримати цю інформацію незалежно від їх поточного місцезнаходження та типу пристрою, який вони використовують.

Доступність

Доступність - це нефункціональна вимога, яка визначається як відсоток часу доступності системи чи послуги. Цей відсоток визначає допустимий загальний час простою для будь-якої послуги. Висока доступність - це сувора вимога, яка дозволяє максимум, приблизно, п’ять хвилин простою на рік, включаючи відключення через планове технічне обслуговування та модернізацію. Доступність є однією з основних проблем хмари.

Автоматизована система

Хмарна автоматизація відноситься до програмних рішень, які автоматизують процес встановлення, конфігурації та управління хмарними обчислювальними послугами. Іншими словами, автоматизація хмар - це використання технології для зменшення ручних зусиль повторюваних завдань у хмарі.

Для більшості організацій хмарні ресурси просто надто складні, щоб люди могли обробляти та керувати ними в режимі реального часу. У міру масштабу хмарних операцій потреба в автоматизованих процесах стає надзвичайно важливою. Справжнє значення автоматизації полягає в тому, щоб зробити завдання управління хмарою максимально ефективними та зручним.

Плата

У хмарних обчисленнях користувач повинен платити лише за послугу або простір, який він використав. Немає жодної прихованої або додаткової плати, яку потрібно сплатити. Більшість часу деякі послуги відводяться безкоштовно. Це, безумовно, вигідно для користувачів.

Хмарні обчислення надають наступні економічні переваги:

- знижує капітальні витрати на інфраструктуру;
- знімає витрати на обслуговування;
- знімає адміністративні витрати.

Існує три різні стратегії ціноутворення, які запроваджуються в хмарних обчисленнях: багаторівневе ціноутворення, ціна за одиницю та ціна на основі підписки.

Багаторівневе ціноутворення:

Багаторівневе ціноутворення - це модель ціноутворення, в якій вартість базується на рівні послуг, обраному клієнтом. Вартість кожного рівня зростає, що визначається такими факторами, як особливості та обмеження використання, включені до будь-якого даного плану. Простіше кажучи, багаторівневе ціноутворення передбачає об’єднання ваших послуг в окремі плани. Потім клієнти прив'язуються до свого плану на певний період, часто отримуючи знижку за вибір довгострокового плану.

Ціна за одиницю:

Концепція цінової одиниці, згідно з якою ціна дається за певну одиничну абстракцію, яка називається «одиниця ресурсу», наприклад, гігабайт сховища чи віртуальна машина. Ця концепція існує вже давно в IT, і хмарні обчислення швидко її пристосували. Однак через підвищену складність послуг, що надаються, і множення можливих одиниць, концепція вже не є інтуїтивною та прозорою.

Ціна за підпискою:

У моделі, що базується на підписці, хмарні клієнти зазвичай платять авансом до отримання доступу до хмарних служб. Ціни часто базуються на тривалості передплати, і довша підписка часто призводить до нижчої вартості.

Безпека

Загрози безпеці постійно розвиваються і стають все більш досконалими.

Хмарні обчислення не менше ризикують, ніж локальне середовище. З цієї причини важливо співпрацювати з хмарним провайдером, який пропонує найкращий у своєму класі захист, який було налаштовано для вашої інфраструктури.

Хмарна безпека пропонує багато переваг, серед яких:

- Централізована безпека. Подібно до того, як хмарні обчислення централізують програми та дані, хмарна безпека централізує захист. Хмарні бізнес-мережі складаються з численних пристроїв і кінцевих точок, якими важко управляти. Централізоване управління покращує аналіз трафіку та веб-фільтрацію, впорядковує моніторинг мережевих подій і призводить до зменшення кількості програмного забезпечення та оновлень політики. Плани ліквідації наслідків стихійних лих також можна легко реалізовувати та реагувати на них, якщо ними керувати в одному місці.

- Зниження витрат. Однією з переваг використання хмарного сховища та безпеки є те, що це позбавляє від необхідності інвестувати у спеціальне обладнання. Це не тільки зменшує капітальні витрати, але й зменшує адміністративні накладні витрати. Колись IT-команди реагували на проблеми безпеки. Зараз хмарна безпека забезпечує активні функції безпеки, які забезпечують захист цілодобово та без вихідних, практично без участі людей.

- Зменшене адміністрування. Коли ви вибираєте надійного постачальника хмарних послуг або хмарну платформу безпеки, можна забути про ручні конфігурації безпеки та майже постійні оновлення безпеки. Усе адміністрування безпеки відбувається в одному місці і повністю управляється від вашого імені.

- Надійність. Послуги хмарних обчислень забезпечують максимальну надійність. За допомогою відповідних заходів безпеки в хмарі користувачі можуть безпечно отримувати доступ до даних та програм у хмарі, незалежно від того, де вони перебувають або яким пристроєм вони користуються.

Дуже важливо, щоб клієнти мали повну впевненість у своїй безпеці хмарних обчислень та щоб усі дані, системи та додатки були захищені від викрадення даних, витоків, пошкодження та видалення.

Усі хмарні моделі сприйнятливі до загроз. IT-відділи переносять критично важливі системи до хмари, і дуже важливо, щоб були введені правильні положення безпеки, незалежно від того, використовуєте ви приватну хмару, гібридну чи будь-яку іншу. Хмарна безпека пропонує всі функціональні можливості традиційної IT-безпеки та дозволяє клієнтам використовувати багато переваг хмарних обчислень, зберігаючи при цьому безпеку, а також забезпечувати дотримання вимог щодо конфіденційності даних та відповідності.

Вимірюване обслуговування

Хмарні системи автоматично контролюють і оптимізують використання ресурсів, використовуючи можливості вимірювання на певному рівні абстракції, що відповідає типу послуги (наприклад, зберігання, обробка, пропускна здатність та активні облікові записи користувачів). Використанні ресурси можна контролювати, складати звіти та повідомляти, забезпечуючи прозорість як для постачальника, так і для споживача послуги.

2.5 Референтна архітектура хмарних обчислень NIST

Референтна архітектура хмарних обчислень NIST дозволяє визначити основних діючих осіб, їх функції та діяльність. Ця архітектура була розроблена для

полегшення розуміння вимог, використання, специфікацій і стандартів хмарних обчислень.

Референта архітектура NIST включає п’ять суб’єктів, а саме: хмарний споживач, хмарний провайдер, хмарний оператор, хмарний аудитор та хмарний брокер. Кожен з яких бере участь в процесі або виконує певну задачу в хмарних обчисленнях. У таблиці №1 перераховані суб’єкти та їх визначення.

На рисунку №2 показано взаємодію між суб’єктами. Хмарні споживачі можуть запитувати послуги безпосередньо у хмарного провайдера або хмарних брокерів. А хмарні аудитори проводять незалежні перевірки та можуть зв'язуватися з іншими суб’єктами для збору необхідної інформації.

Таблиця №1 Суб’єкти та їх визначення

Суб’єкти	Визначення
Хмарний споживач	Людина або організація, яка підтримує бізнес стосунки та використовує послугу від хмарних постачальників.
Хмарний провайдер	Особа чи організація, відповідальна за надання послуг зацікавленим сторонам.
Хмарний аудитор	Сторона, яка проводить незалежну оцінку хмарних сервісів, функціонування інформаційної системи, продуктивності та впровадження безпеки хмари.
Хмарний брокер	Суб'єкт господарювання, який управляє використанням, продуктивністю та веде переговори про відносини між хмарним постачальником та хмарним споживачем.
Хмарний оператор	Посередник, який забезпечує зв'язок та доставку хмарних послуг від хмарних провайдерів до хмарних споживачів.

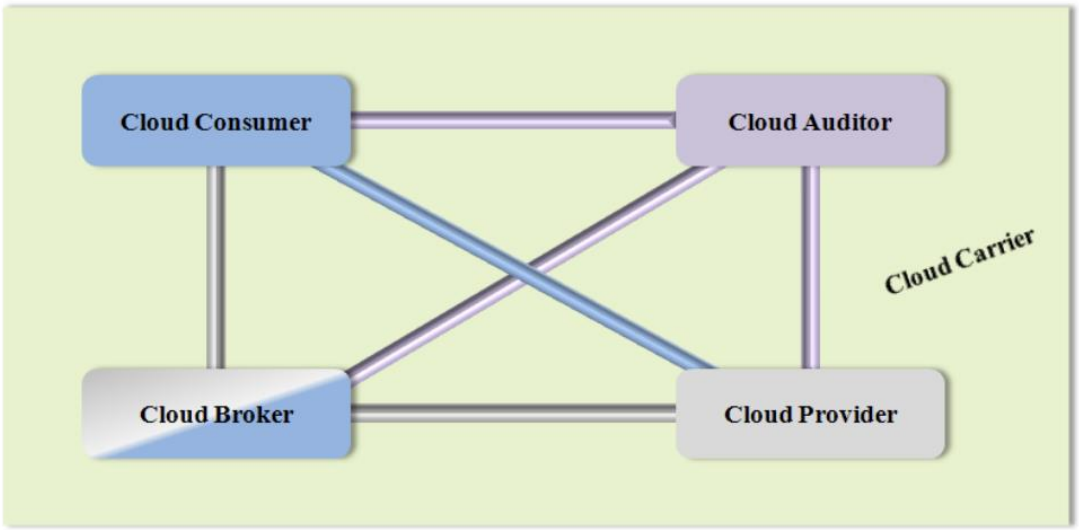

Рисунок №2 Взаємодія між суб’єктами хмарних обчислень

2.5.1 Сценарії використання

Сценарій використання №1.

Хмарний споживач може звернутися до хмарного брокера за послугами, замість звернення до хмарного постачальника. Якщо немає послуги, яка задовольняє вимоги споживача. То брокер може поєднати декілька послуг в одну або вдосконалити існуючу. У цьому сценарії використання постачальник невидимий для споживача. Адже усі комунікації відбуваються між брокером та споживачем.

Рисунок №3 Сценарій використання хмарних брокерів

Сценарій використання №2

Хмарні оператори відповідають за доставку послуг та зв'язок між хмарним провайдером та хмарним споживачем. Як показано на рисунку №4, провайдер бере участь у двох унікальних угодах про рівень обслуговування (SLA). Перша використовується для зв'язку з оператором (SLA2), а друга для зв'язку з споживачем

(SLA1). Провайдеру знадобиться виділене зашифроване з'єднання для укладення угоди про рівень обслуговування (SLA) з оператором, щоб забезпечити доступність хмарних послуг на стабільному рівні відповідно до угоди зі споживачем послуг. У цьому випадку постачальник може вказати свою функціональність, гнучкість і функціональні вимоги в SLA2 для задоволення необхідних вимог SLA1.

Рисунок №4 Сценарій використання хмарних операторів

Сценарій використання №3

Хмарний аудитор проводить незалежну оцінку роботи та безпеки впровадженої хмарної служби. Аудит може передбачати взаємодію як із споживачем хмарних послуг, так і з хмарним провайдером.

Рисунок №5 Сценарій використання хмарних аудиторів

2.5.2 Актори референтної архітектури

Хмарні споживачі

Хмарні споживачі зацікавленні в отриманні якісних хмарних послуг. Хмарний споживач – це особа або організація, яка використовує хмарні послуги, що надає провайдер. Спочатку споживач обирає необхідну послугу, встановлює контакт на обслуговування з провайдером та використовує надану послугу.

Споживачі хмарних сервісів потребують SLA для визначення технічних вимог продуктів, що виконуються хмарними провайдерами. SLA включає в себе умови, пов'язані з якістю обслуговування, безпекою та функціями безпеки. Провайдери також можуть включати свої вимоги в угодах про рівень обслуговування, а саме обмеження і зобов'язання, які повинні приймати хмарні споживачі. Споживачі можуть обирати будь-якого провайдера, який їх влаштовує більше. Політика цін і угоди про рівень обслуговування хмарних провайдерів, як правило, не підлягають обговоренню. Виняток, однак, полягає в тому, що клієнт очікує інтенсивно використовувати сервіси і може домовитися з хмарним провайдером про більш вигідні умови. Послуги в різних провайдерах можуть відрізнятися.

Хмарний провайдер

Хмарний провайдер - це організація, яка відповідає за за надання послуг зацікавленим сторонам. Хмарний постачальник набуває та управляє необхідною для цього обчислювальною інфраструктурою надаючи послуги, запускає хмарне програмне забезпечення, яке надає послуги, і домовляється надавати хмарні послуги хмарним споживачам через мережевий доступ.

Хмарний аудитор

Хмарний аудитор - це сторона, яка проводить незалежну перевірку контролю хмарних сервісів і дає висновок про безпеку, продуктивність і т.д.

Аудит перевіряє відповідність стандартів, оцінює якість наданих послуг.

Цей тест допоможе дотримуватися застосовних законів і правил. Аудит забезпечує конфіденційність, цілісність і доступність персональних даних споживача на кожному етапі розробки та експлуатації.

Хмарний брокер

З розвитком хмарних обчислень споживачу все складніше управляти послугами. Хмарний споживач може звернутися до хмарного брокера за послугами, замість звернення до хмарного постачальника.

Хмарний брокер - це організація, яка управляє використанням, продуктивністю та доставкою хмарних послуг та веде переговори про відносини між хмарними провайдерами та хмарними споживачами.

Хмарний брокер може надавати послуги у трьох категоріях:

- Посередництво у послугах. Хмарний брокер покращує надану послугу.

- Агрегація послуг. Хмарний брокер поєднує та інтегрує кілька служб в одну або кілька нових послуг.

- Арбітраж послуг. Сервісний арбітраж означає, що брокер має можливість вибору послуги від кількох постачальників.

Хмарний оператор

Хмарні оператори виступають в якості посередників, які забезпечують зв'язок і надання хмарних послуг між споживачами послуг і провайдерами. Хмарні оператори дозволяють споживачам отримувати доступ через мережу, телекомунікації та інші пристрої доступу. Поширення хмарних сервісів зазвичай здійснюється через мережу операторами мобільного зв'язку або хмарним оператором. Хмарний оператор безпосередньо стосується організації, яка займається фізичним транспортуванням носіїв, таких як жорсткі диски великої ємності.

Хмарний провайдер встановлює SLA з хмарним оператором для надання послуг, що відповідають рівню SLA, які пропонуються хмарним споживачам. Хмарний провайдер в праві вимагати від хмарного оператора надання спеціальних та безпечних засобів зв’язку між споживачами та провайдерами.

Висновки за розділом 2

В другому розділі під назвою побудова та структура хмарних обчислень та сервісів я детально розглянув наступні питання:

- моделі розгортання хмарних;

- сервісні моделі хмарних обчислень (навів їх переваги та для чого вони використовуються);

- надав основні характеристики хмарних обчислень та розповів для чого вони потрібні;

- розповів про референтну архітектуру хмарних обчислень NIST (про її суб’єктів та можливі сценарії використання).

РОЗДІЛ 3
ЗАГРОЗИ ТА РЕКОМЕНДАЦІЇ ЩОДО ХМАРНИХ СЕРВІСІВ

3.1 Модель загроз хмарних сервісів

Потенційні можливості порушника дозволили розробити модель загроз відносно хмарних сервісів. Детальний опис моделі загроз наведений в таблиці №2. В ній на основі рисунка №6 вказується об’єкт, для якого реалізується загроза, мета порушника, ймовірність загрози та мета здійснення захисту.

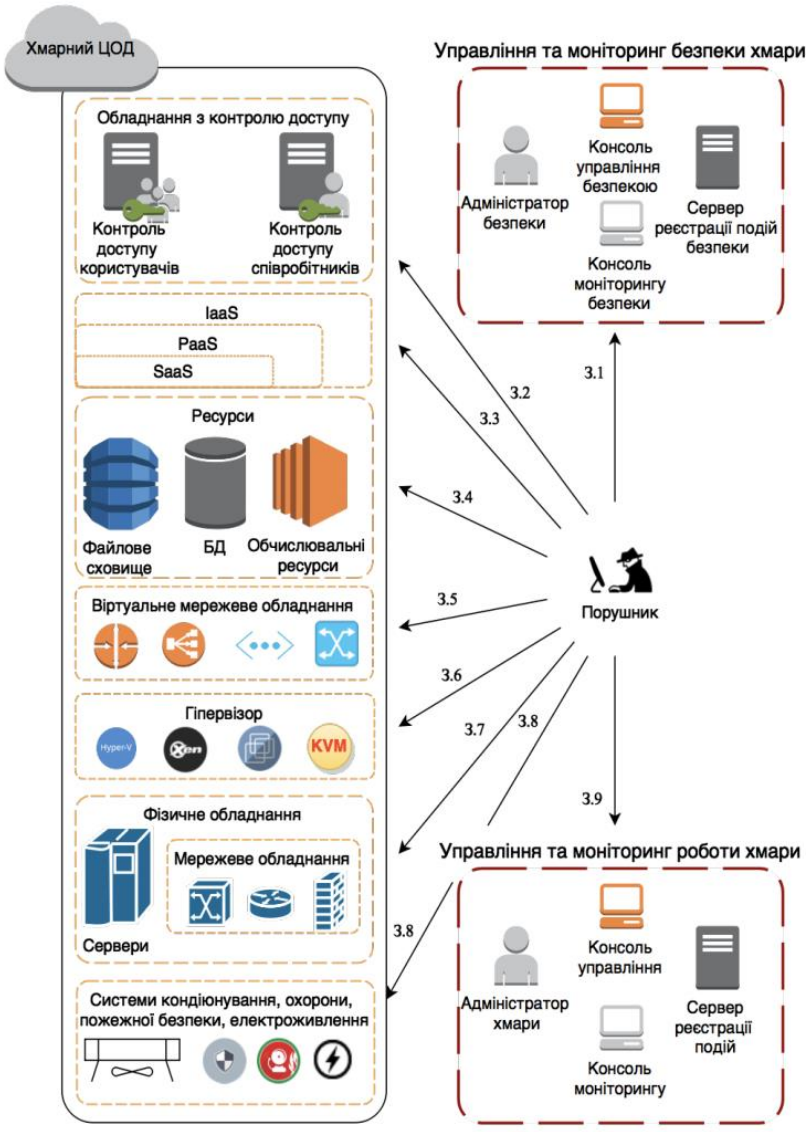

Рисунок №6 Модель загроз

Найбільшу ймовірність мають загрози, що здійснюються на компоненти хмарної інфраструктури, які мають інтерфейси доступу із зовні або знаходяться в віртуалізованому середовищі. Аналіз моделі загроз, зображеної на рис. 6, показав, що найбільшу небезпеку становлять загрози управління хмарою та її безпекою, а також загрози гіпервізору.

Незалежно від моделі розгортання хмари та моделі надання послуг найнебезпечнішими порушниками в ІТС хмари є адміністратори хмари та адміністратори безпеки хмари.

3.2 Порівняння безпеки різних хмарних провайдерів

За даними аналітики Canalys лідерами ринку є:

- Amazon Web Services;
- Microsoft Azure;
- Google Cloud.

Тому порівнювати буду саме ці три хмарні провайдери.

Потрібно враховувати три важливі аспекти:

- Фізична безпека, наприклад захист фізичних активів у географічному розташуванні.
- Захист інфраструктури, такий як забезпечення якнайшвидшого оновлення виправлень безпеки, сканування портів на наявність ненормальної поведінки тощо.
- Захист даних та доступу, наприклад, шифрування даних, контроль прав користувача тощо.

Той факт, що користувачі хмарних служб несуть значну відповідальність за компонент безпеки, відомий як модель спільної відповідальності.

За цим сценарієм: «Клієнт зобов’язаний забезпечити, щоб він і надалі відповідав вимогам безпеки, управління та дотримання вимог. Наприклад, CSP може захистити від грубих спроб входу, але відповідальність замовника полягає в тому, щоб співробітники використовували унікальні та безпечні паролі для всіх хмарних служб, щоб мінімізувати ризик компрометації облікового запису ".

AWS

AWS - найстаріший та великий хмарний постачальник. Це і добре, і погано, оскільки деякі їх варіанти на рівні підприємства в основному були об'єднані з базових служб і не були спроектовані для масштабів сучасних хмарних розгортань.

Найбільша перевага AWS полягає в тому, що, як провідний постачальник, існує багато знань та інструментів. Отримати відповіді, знайти допомогу та знайти підтримувані інструменти простіше простого. Це відповідає загальній зрілості та обсягу платформи. AWS також досить добре виконує роботу за замовчуванням для захисту конфігурацій. Наприклад, коли ви розгортаєте екземпляр на VPC, доступ до мережі обмежений.

Ізоляція – це головне в AWS. Служби навіть не можуть отримати доступ до інших служб, якщо ви прямо не дозволите доступ. Основним елементом в AWS є облікові записи повністю ізольовані один від одного, поки ви не відкриєте доступ. Ви можете зв'язати всі свої облікові записи разом, якщо хочете, але все одно можна обмежити центральний доступ.

Доступні більшість основних функцій безпеки - від надійного моніторингу активності API до базової інформації про загрози (Guard Duty), WAF, DLP (Macie), оцінки вразливостей (інспектор) та тригерів подій безпеки для автоматизації. Є методики заповнення залишившихся прогалин. Дві найкращі функції безпеки AWS - це їх відмінна реалізація груп безпеки (брандмауери) та детальний IAM.

Але всі ці переваги мають і темну сторону. Ізоляція ускладнює управління масштабами підприємства. Навіть в межах одного облікового запису важко збирати дані безпеки та керувати ними в різних регіонах. Наприклад, ви можете створити концентратор подій безпеки, але він може збирати події лише у своєму регіоні. Центр безпеки - це їх новий продукт, який поєднує свої інструменти безпеки, так і сторонніх виробників. Хоч він і може працювати в усіх облікових записах, він все ще обмежений регіонами.

Управління IAM у масштабі може бути важкою задачею, особливо якщо ви ввімкнете більш розширені функції, такі як межі дозволів та умовні позначення.

Знову ж таки, це в основному пов’язано з ізоляцією між обліковими записами, оскільки немає єдиного місця для управління доступом для всіх них.

Незважаючи на ці обмеження, сьогодні AWS, як правило, найкраща хмара для початку, де ви стикаєтеся з найменшою кількістю проблем безпеки.

Microsoft Azure

Azure час від часу може зводити з розуму через непослідовність та погану документацію. Багато служб використовують за замовчуванням менш безпечні конфігурації. Наприклад, якщо ви створюєте нову віртуальну мережу та нову віртуальну машину на ній, усі порти та протоколи відкриті. AWS та GCP завжди починаються із заборони за замовчуванням, але Azure починається із дозволу за замовчуванням.

Azure має деякі переваги, які можуть бути значними для підприємств. Azure Active Directory - єдине джерело достовірної інформації для авторизації та управління дозволами. На відміну від AWS - де вам потрібно налаштувати користувачів та доступ для кожного облікового запису окремо. Azure дозволяє керувати всім цим з одного каталогу. Це і добре, і погано - управління простіше і послідовніше, але середовище (підписки) менш ізольовані та захищені одне від одного. Під час оцінки однієї із найпоширеніших проблем є надлишкове відділення ресурсів.

Azure має ще дві інші центральні функції, які особливо приваблюють корпоративних користувачів:

- Журнали активності охоплюють консоль та активність API для всього орендаря (організації) за замовчуванням у різних регіонах. Немає потреби створювати власні функції для переміщення подій між регіонами або іншими складностями, які ми бачимо на AWS. Журнали активності набагато більш своєчасні.

- Центр безпеки Azure також охоплює всього орендаря (з належним ліцензуванням) і може бути обмежений, щоб дозволити доступ на рівні підписки, щоб місцеві команди могли управляти власними сповіщеннями. Але ASC може звести з розуму через відсутність прозорості та обмежень щодо оцінки. Головне

зрозуміти, що він робить добре, що робить нормально (наприклад, деякі сканування загроз проводяться щодня), а що погано (оцінки відповідності мають дивні прогалини).

Як і в випадку з AWS, ви можете робити майже все, що вам потрібно в Azure, але як тільки ви перейдете на Azure AD, журнали активності та центр безпеки Azure, то в порівнянні з Azure решта інших провайдерів буде більш складніше налаштовувати. Наприклад, є два різні типи груп безпеки (мережа та програми), якими керують по-різному, і одна навіть не відображається на порталі, коли ви дивитесь на свої мережі. Підтримка API всюди, хоча ви можете робити більшість речей у PowerShell, SDK та інших інструментах.

Azure також має реальні проблеми з послідовністю, доступністю та документацією. Наприклад, деякі служби розгортають кінцеву точку у віртуальній мережі, але не підтримують її групи безпеки мережі. Схоже що ви захищені, але натомість порти або пункти призначення доступні в Інтернеті - і це не те, що клієнт може змінити! Були клієнти, які повідомляли про різні види ідіосинкратичної поведінки та про такі, що не відповідають документації. Що стосується підтримки, поширеною скаргою є те, що клієнти задають одне питання, а потім отримують 5 різних відповідей від 3-х різних консультантів Microsoft або представників служби підтримки.

Ви можете бути в безпеці на Azure, але потрібно бути дуже обережним та перевіряти все.

Google

В одному GCP дуже молодий, а в іншому дуже старий. Він побудований на вражаючих довгострокових інженерних та глобальних операціях Google, які шалено вражають.

Як і Azure, GCP краще централізований, оскільки багато можливостей планувалось із самого початку - порівняно з функцією AWS, яку було додано лише кілька років тому. У вашому обліковому записі проекти ізольовані один від одного, за винятком випадків, коли ви підключаєте послуги. Загалом GCP не настільки

зрілий, як AWS, але деякі служби - зокрема управління контейнерами та AI - є лідером класу.

GCP пропонує ведення журнала для всієї організації, але охоплення не є повним. Він має більш детальний IAM, яким можна простіше управляти централізовано, але деякі аспекти політик все ще перебувають у бета-версії. Це все лише питання часу. Зазвичай GCP за замовчуванням захищає конфігурації, але не завжди має такий самий спектр функцій безпеки, як AWS.

GCP включає деякі вражаючі вбудовані засоби захисту. Командний центр Cloud Security - це їх версія центру безпеки. Stackdriver Logging чудово працює, і Google пропонує відкритий код Forseti для управління конфігураціями безпеки.

Недоліком є дуже мала кількість експертів з безпеки з глибоким досвідом роботи з GCP та менш надійне співтовариство та інструментарій. Знову ж цього можна очікувати від молодшої служби - такий тип розширення знань вимагає часу.

3.3 Рекомендації щодо захисту хмарних сервісів

Я хочу чітко пояснити, що клієнти будуть в безпеці використовуючи будь-яку компанію з вище перерахованих - за допомогою правильних конфігурацій, знань та інструментів.

Однак хмарні провайдери мало контролюють захист даних та доступ. Натомість безпека на рівні додатків, як правило, відповідальність користувачів. Близько 80% порушень відбувається, оскільки ця частина не дуже добре забезпечена.

Щоб зменшити ризики запропоновано наступні рекомендації:

- Шифрувати дані та бази даних (шифрування даних використовується для того, щоб уникнути зловмисних або недбалих сторін від доступу до конфіденційних даних. Шифрування є важливою лінією захисту в архітектурі кібербезпеки, максимально ускладнює використання перехоплених даних. Шифрування може застосовуватися до всіх видів даних, починаючи від секретної державної інформації

та закінчуючи операціями з особистими кредитними картками. В хмарних обчисленнях дуже важливо шифрувати дані для входу);

- Забезпечувати правильність прав користувача (Велику загрозу для безпеки інформації в хмарі становлять користувачі, які мають привілегійований доступ до функцій системи або адміністратори хмарних сервісів, тому для зменшення ризику можливих деструктивних дій з їх боку, доцільно вести незалежний нагляд та контроль за їх діями в хмарі. Як показує статистика саме на внутрішніх користувачів припадає найбільша кількість порушень безпеки);

- Розгортати такі функції, як сканери кібербезпеки (сканери вразливостей - цінні інструменти, які шукають і повідомляють про те, які відомі вразливості присутні в IT-інфраструктурі організації. Використання сканера вразливостей - це проста, але надзвичайно важлива практика безпеки, якою може скористатися кожна організація.

Ці сканування можуть дати організації уявлення про те, з якими загрозами безпеки вони можуть зіткнутися, даючи уявлення про потенційні слабкі місця в безпеці, що існують в їхньому середовищі. Можна використовувати кілька сканерів вразливості, щоб забезпечити повне охоплення кожного об’єкта, створюючи повну картину. Протягом багатьох років було розроблено багато різних сканерів, що надають безліч різних опцій та функцій);

-Прийняття міжнародних стандартів у галузі;

-Введення контролю з боку держави;

-Використання незалежних експертів у цій галузі;

-Використовувати алгоритми цифрового підпису (цифровий підпис - це математична схема для перевірки справжності цифрових повідомлень або документів. Дійсний цифровий підпис, коли передумови виконані, дає одержувачу дуже вагомі підстави вважати, що повідомлення було створене авторизованим відправником і що повідомлення не було змінено під час передачі);

-Використовувати методи багатофакторної автентифікації (багатофакторна автентифікація - це електронний метод автентифікації, при якому користувач

пристрою отримує доступ до веб-сайту або програми лише після успішного представлення двох або більше доказів);

-Потрібно щоб була відповідність законів у сфері обробки, передачі, збереження та захисту інформації різних держав. Вирішення цієї проблеми є ключовим фактором для можливості фізичного розміщення серверів постачальника хмарних сервісів у різних країнах та регіонах, а також використанням користувачами з різних країн одного постачальника послуг.

-Потрібно проводити аудити безпеки постачальника хмарних послуг та перевірки відповідності його системи безпеки міжнародним вимогам до захисту інформації, що сформульовані в міжнародних стандартах.

-Відстеження діяльності кінцевих користувачів за допомогою автоматизованих рішень для виявлення зловмисників. Моніторинг у реальному часі та аналіз діяльності кінцевих користувачів може допомогти виявити порушення, що відхиляються від звичайних схем використання, наприклад, увійти з раніше невідомої IP-адреси або пристроїв. Ці ненормальні дії можуть свідчити про порушення у вашій системі, тому їх своєчасне виявлення може зупинити хакерів і дозволити вам виправити проблеми безпеки, перш ніж вони спричинять хаос. Є багато рішень, які можуть у цьому допомогти, починаючи з автоматизованого цілодобового моніторингу та управління мережею та переходячи до передових рішень з кібербезпеки.

-Коли працівники залишають компанію, переконайтеся, що вони більше не матимуть доступу до хмарного сховища, систем, даних, інформації про клієнтів і т.д. Це найважливіша відповідальність за безпеку, яку часто відкидають через кілька днів чи тижнів після того, як хтось пішов. Оскільки кожен співробітник, швидше за все, мав доступ до багатьох різних хмарних додатків та платформ, потрібен систематизований процес виведення з ладу, щоб гарантувати, що всі права доступу для кожного працівника, що звільнилися, анульовані.

-Забезпечити регулярне навчання працівників з питань фішингу. Хакери можуть отримати доступ до захищеної інформації, викрадаючи реєстраційні дані співробітників, використовуючи такі технології соціальної інженерії, як фішинг,

підробка веб-сайтів та шпигунство в соціальних мережах. Проведення постійних тренінгів - найкращий спосіб запобігти тому, щоб співробітники не стали жертвами цих шахрайств та не порушили конфіденційність компанії.

Висновки за розділом 3

В третьому розділі під назвою загрози та рекомендації щодо захисту хмарних сервісів я детально розглянув наступні питання:

- навів загрози хмарних сервісів, їх мету та методи вирішення;
- порівняв безпеку найпопулярніших хмарних провайдерів;
- на основі аналізу запропонував рекомендації захисту щодо хмарних сервісів.

ВИСНОВКИ

У дипломній роботі було проаналізовано основні положення нормативно-правового забезпечення з інформаційної безпеки в хмарних обчисленнях, досліджено принципи побудови хмарних сервісів, найпоширеніші загрози безпеці та методи їх запобігання.

На основі аналізу було запропоновано рекомендації інформаційної безпеки хмарних обчислень. Для досягнення поставленої мети роботи було використано аналіз захищеності найпопулярніших хмарних провайдерів, літератури, стандартів та структури хмарних сервісів.

Практичне значення роботи полягає у поєднанні різних методів захисту хмарних сервісів та формування рекомендацій, які можуть бути успішно впроваджені.

Мету роботи досягнуто, поставлені задачі виконано.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Haeberlen, T. Cloud Computing Benefits, risks and recommendations for information security T. Haeberlen, L. Dupré [Електронний ресурс]. - Режим доступу: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file;

2. Jansen, W. Cloud Hooks: Security and Privacy Issues in Cloud Computing W. Jansen 44th Hawaii International Conference on System Sciences (HICSS) – 2011. - с.1–10;

3. Jansen, W. Guidelines on Security and Privacy in Public Cloud Computing. W. Jansen, F. Grance, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf [Електронний ресурс].- Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf;

4. Hashizume, K. An analysis of security issues for cloud computing / K. Hashizume, D. Rosado, E. Fernández-Medina, E. Fernandez. Journal of Internet Services and Application – 2013. – с. 15–28;

5. Chandramouli, R. Analysis of Protection Options for Virtualized Infrastructures in Infrastructure as a Service Cloud. R. Chandramouli. Fifth International Conference on Cloud Computing, GRIDs, and Virtualization, Venice, Italy, 2014. – с. 37–43;

6. Chandramouli, R. NIST Cryptographic Key Management Issues & Challenges in Cloud Services. R. Chandramoli, S. Chokhani, M. Iorga. – National Institute of Standards and Technology, 2013. – с. 31-43;

7. Luna, J. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards J. Luna, N. Suri, M. Iorga and A. Karmel // IEEE Cloud Computing. – 2015. – с. 32–40;

8. Choo, K. A Cloud Security Risk-Management Strategy K. Choo // IEEE Cloud Computing, 2014. - с. 52-56;

9. Зикратов, И. А. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода. И. А. Зикратов, С. В. Одегов // Научно-технический вестник информационных технологий, механики и оптики, 2012. –

с. 121–126;

10. Juliadotter, N. Cloud Attack and Risk Assessment Taxonomy. N. Juliadotter, K. Choo // IEEE Cloud Computing, 2015. – с. 14-20;

11. Аулов, І. Ф. Аналіз формальної модели безпеки хмари NIST: Всеукр. межвед. науч.-техн. сб. І. Ф. Аулов, І. Д. Горбенко // Радиотехника, 2014. – с. 131–137;

12. Gillam, Lee. Cloud Computing: Principles, Systems and Applications. Nick Antonopoulos, Lee Gillam, 2010. — с. 355-379;

13. Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0. Technical report, Cloud Security Alliance, 2011 [Електронний ресурс]. - Режим доступу: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf;

14. Cloud computing use cases whitepaper August, 2009 [Електронний ресурс]. - Режим доступу: http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper;

15. The European Union Agency for Cybersecurity [Електронний ресурс]. - Режим доступу: http://www.enisa.europa.eu/;

16. Wikipedia [Електронний ресурс]. - Режим доступу: https://www.wikipedia.org/;

17. International Organization for Standardization [Електронний ресурс]. - Режим доступу: https://www.iso.org/home.html;

18. National Institute of Standards and Technology [Електронний ресурс]. - Режим доступу: https://www.nist.gov/;

19. Cloud Security Alliance [Електронний ресурс]. - Режим доступу: https://cloudsecurityalliance.org/;

20. Google Cloud [Електронний ресурс]. - Режим доступу: https://cloud.google.com/;

21. Microsoft Azure[Електронний ресурс]. - Режим доступу: https://azure.microsoft.com/;

22. Amazon Web Services [Електронний ресурс]. - Режим доступу: https://aws.amazon.com/;

23. Global Privacy & Security, Francoise Gilbert, 2009 – с. 27-35;

24. Web Services API Developer's Guide [Електронний ресурс]. – Режим доступу: http://www.salesforce.com/us/developer/docs/api/index.htm;

25. Few Good Information Security Metrics, By Scott Berinato, July 2005 [Електронний ресурс]. – Режим доступу: http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

26. Cloud-computing-information-assurance-framework Wayne Jansen, Timothy Grance Guidelines on Security. – с. 51-63;

27. Cloud Computing Security Risk Assessment. Technical report, D. Catteddu and G. Hogben. – с. 14-17;

28. Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0. Technical report, Cloud Security Alliance, 2011 [Електронний ресурс]. – Режим доступу: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf;

29. Ярочкин В.И. Информационная безопасность: Учеб. пособие для студ. непрофильных вузов. – М., 2000. Новицька Н.Б. Правове забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави, 2009. – с. 44-47;

30. Cloud Security and Privacy – An Enterprise perspective on Risks and Compliance from O'Reilly [Електронний ресурс]. – Режим доступу: http://oreilly.com/catalog/9780596802776/;

31. Cloud Storage Strategy, Steve Lesem, July 19, 2009 [Електронний ресурс]. – Режим доступу: http://www.cloudstoragestrategy.com/2009/07/cloud-storage-and-the-innovators-dilemma.html;

32. The Institute of Internal Auditors, Critical Infrastructure Assurance Project,

"Information Security Governance: What Directors Need to Know", 2001. – с. 77-84;

ДОДАТОК А

Таблиця №2 Загрози хмарних обчислень

Загроза	Об’єкт для якого реалізується загроза	Мета	Ймовірність загрози	Методи захисту
3.1	Управління та моніторинг безпеки хмари	Отримання несанкціонованого доступу до хмари	низька	Використання систем з контролю доступу, політики безпеки, атестація персоналу
3.2	Обладнання з контролю доступу	Отримання несанкціонованого доступу до хмарних ресурсів чи управління хмарою	висока	Використання захищених носіїв ключа для автентифікації
3.3	Середовище хмари: сервіси, додатки та інфраструктура	Порушення сервісами, додатками та об’єктами інфраструктури прав доступу. Несанкціонований доступ до функцій управління інфраструктурою, даних сервісів та додатків користувача хмари. Зараження шпигунським ПЗ	висока	Використання технологій розмежування та обмеження доступу, контроль над цілісністю об’єктів та їх моніторинг

		та вірусами		
3.4	Ресурси хмари	Отримання несанкціонованого доступу до файлів, записів БД або використання обчислювальних ресурсів	висока	Впровадження механізмів обмеження доступу, шифрування даних, моніторинг роботи
3.5	Віртуальні мережі в межах хмарної інфраструктури	Прослуховування трафіку, порушення цілісності, доступності, організація атак DDoS, несанкціоноване підключення до мережі	висока	Використання засобів захисту даних в мережі, систем виявлення та протидії мережевим атакам, моніторинг роботи
3.6	Гіпервізор	Повний контроль над розгорнутим віртуальним середовищем	низька	Захист гіпервізора та контроль доступу до його налаштувань
3.7	Фізичне обладнання	Встановлення засобів несанкціонованого доступу, модифікації та знищення інформації.	низька	Використання систем контролю доступу, політики безпеки, атестація персоналу. Встановлення контрольованої

				зони
3.8	Допоміжні системи (живлення, охорони, безпеки, охолодження)	Встановлення засобів несанкціонованого доступу, модифікації та знищення інформації.	низька	Використання систем контролю доступу, політики безпеки, атестація персоналу. Встановлення контрольованої зони
3.9	Управління та моніторинг роботи хмари	Отримання несанкціонованого доступу до налаштувань хмари	середня	Використання технологій розмежування та обмеження доступу, моніторинг дій адміністраторів
3.10	Зв’язки між хмарними ЦОД	Порушення доступності ЦОД, отримання несанкціонованого доступу до інформації, що передається мережею	низька	Використання надійних протоколів з стійкими криптограф. алгоритмами