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
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

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: «Рекомендації щодо технологій забезпечення інформаційної безпеки в хмарах»

Виконавець: студент IV курсу, групи КБ-41

_____ **Борис МАМІЧ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	Підпис
Керівник	Юрій ЩЕБЛАНІН	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

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
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-41** **Маміч Борис Васильович**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Рекомендації щодо технологій забезпечення інформаційної безпеки в хмарах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Хмарні технології, архітектура хмарних сервісів, забезпечення безпеки використання хмар

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією хмарних технологій, їх типовими розгортаннями та послугами, вразливостями з боку безпеки даних та технологіями захисту

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено рекомендації щодо забезпечення інформаційної безпеки хмарних технологій.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 01 листопада 2021 року

Завдання видав	_____	Юрій ЩЕБЛАНІН
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	Борис МАМІЧ
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки завдання	01.11.2021 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2022 – 11.02.2022	*виконано*
3	Розгляд принципів функціонування хмарних технологій	12.02.2022 – 24.02.2022	*виконано*
4	Дослідження загроз безпеки інформації	25.02.2022 – 24.03.2022	*виконано*
7	Дослідження методів і засобів вирішення проблем безпеки в хмарних технологіях	21.04.2022 – 05.05.2022	*виконано*
8	Оформлення пояснювальної записки	05.06.2022 – 06.06.2022	*виконано*
9	Підготовка до захисту	07.06.2022 – 13.06.2022	*виконано*

Завдання видав	_____	Юрій ЩЕБЛАНІН
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	Борис МАМІЧ
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Робота присвячена дослідженню проблем забезпечення інформаційної безпеки в хмарах.

Робота складається з трьох розділів, загальних висновків, списку використаних джерел і має 5 рисунків, 4 таблиці. Загальний обсяг роботи 49 сторінок.

Об'єкт дослідження – система забезпечення безпеки хмарних технологій.

Предмет дослідження – проблеми захисту інформації в хмарних технологіях.

Метою роботи є: надання рекомендацій щодо забезпечення інформаційної безпеки в хмарних технологіях, що використовуються підприємствами для обробки чи зберігання даних.

Методи дослідження – спостереження, аналогії, експерименту, розрахунково – аналітичний та ін.

Теоретична та практична цінність роботи полягає в тому, що розглянуто різновиди та принципи роботи хмарних технологій, системи безпеки, що використовуються для забезпечення цілісності периметру безпеки. В роботі розглянуто підходи до забезпечення інформаційної безпеки в хмарних технологіях, та надано рекомендації щодо існуючих методів безпеки, які можуть бути використані керівниками служб безпеки відповідних підприємств.

Практична цінність полягає у набутті автором практичних навичок і вмінь з інформаційного пошуку, аналітичного опрацювання літератури та узагальнення інформації.

Ключові слова: ХМАРНІ ТЕХНОЛОГІЇ, ЦЕНТРИ ОБРОБКИ ДАНИХ АВТОМАТИЗОВАНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМЕРЦІЙНА ТАЄМНИЦЯ ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 6

ВСТУП 7

РОЗДІЛ 1 ПРИНЦИПИ ФУНКЦІОНУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ 9

1.1. Поняття та визначення хмарних технологій 9

1.2. Український розвиток хмарних технологій 11

1.3. Поняття та класифікація загроз ІБ у хмарах 14

1.4. Методи забезпечення ІБ в хмарах 17

Висновки до першого розділу. 17

РОЗДІЛ 2 ДОСЛІДЖЕННЯ ПРОБЛЕМ БЕЗПЕКИ СУЧАСНИХ ХМАРНИХ ТЕХНОЛОГІЙ 18

2.1. Проблеми ІБ у хмарах і їх класифікація 18

2.2. Можливі атаки на хмари і рішення щодо протидії 19

2.3. Вимоги до безпеки на основі аналізу технології HDFS 24

2.4. Модель захисту даних 25

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРНИХ ТЕХНОЛОГІЯХ 30

3.1. Системне вирішення проблем безпеки в хмарних технологіях 30

3.2. Тенденції розвитку новітніх засобів захисту ІБ в хмарних технологіях 40

Висновки до третього розділу 44

ВИСНОВКИ 45

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 47

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС	-	автоматизована система
ЗК	-	загальні критерії оцінки безпеки інформаційних технологій
ІБ	-	інформаційна безпека
ІС	-	інформаційна система
КСЗІ	-	комплексна система захисту інформації
СУІБ	-	система управління інформаційною безпекою
ЦОД	-	центр обробки даних
ХТ	-	хмарні технології

ВСТУП

Використання хмарних сервісів, є перспективним напрямком розвитку IT-технологій. Більшість компаній та стартапів, що з’являються щорічно (близько 60 тис.) використовують саме хмарні технології для обробки та зберігання інформації.

Ми живемо в епоху інформаційного суспільства, коли інформаційні та телекомунікаційні технології охопили майже всі сфери життєдіяльності при цьому стали об'єктом злочинних посягань (кібернетична злочинність), де інформаційна безпека підприємства також входить до об'єктів вищезазначених технологій – слід неабияку увагу приділяти захисту даних. За даними Інтерполу кібернетична злочинність за своїм розвитком, вже входить до списку найбільш серйозних загроз, з якими доводилося зустрічатися правоохоронній системі.

Для попередження та запобігання даному виду злочинності кожного року створюються та оновлюються системи та методи захисту інформації від різних видів вторгнення в інформаційну систему, на що витрачається величезні ресурси [1, 2].

Актуальність роботи полягає в тому, що інформаційна безпека будь-якого підприємства займає одне з найважливіших місць в складовій цілісної системи безпеки. Як зазначалось раніше, більшість підприємств використовує хмарні технології, а саме центри обробки даних, при цьому в більшості випадків використовують готові рішення, і не обов’язково розробляють їх самі. У світі існує багато компаній, що дозволяють використовувати свої потужності хмарних технологій, наприклад пакет Microsoft Azure чи Amazon AWS Activate.

Погіршення таких параметрів інформації на підприємстві, як конфіденційність, цілісність, доступність, може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами та інших критично важливих систем; розголошення відомостей, що становлять комерційну та інші види таємниці; несанкціонований доступ до персональних даних фізичних осіб тощо.

Наслідком цього може бути: погіршення ділових відносин з партнерами; зрив переговорів; невиконання договорів; необхідність додаткового дослідження ринку; фінансові втрати, пов'язані з новими розробками; втрата ділової репутації; труднощі з постачанням та закупівлею обладнання тощо.

Метою роботи є надання рекомендацій щодо забезпечення інформаційної безпеки в хмарних технологіях, що використовуються підприємствами для обробки чи зберігання даних.

Об’єкт дослідження – система забезпечення безпеки хмарних технологій.

Предмет дослідження – проблеми захисту інформації в хмарних технологіях.

Галузь застосування. Рекомендації можуть використовуватися керівниками підприємств для підвищення їх конкурентоспроможності, рентабельності, інвестиційної привабливості та ін.

РОЗДІЛ 1.
ПРИНЦИПИ ФУНКЦІОНУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

1.1. Поняття та визначення хмарних технологій

Хмарні обчислення визначаються як динамічно масштабований безкоштовний спосіб доступу до зовнішніх обчислювальних інформаційних ресурсів у вигляді послуг, що надаються через Інтернет. Термін вперше був використаний в 1997 році в лекції Рамната Челлаппи.

Але термін «хмарні технології» активно почав використовуватися лише в 2008 році, коли генеральний директор Google Ерік Шмідт почав використовувати його в презентаціях. Компанія Salesforce.com в 1999 році, далі були у 2002 році веб-сервіси Amazon.

Запропонована технологія забезпечувала збереження інформації та проводити розрахунки. У 2006 році Amazon презентував службу забезпечував своїх користувачів використанням власного програмного забезпечення. Тоді ж Google почав впроваджувати сервіси SaaS під назвою «Google Apps» професійних розробників (PDC) 2008 року, яка стала значним поштовхом до хмарних технологій.

Послуги, які ми можемо отримувати за допомогою хмарних технологій [1-2]:

1. Користувач може використовувати програмне забезпечення (Software as a Service (SaaS));
2. Технологія, платформа як сервіс (Platform as a Service (PaaS)) — забезпечує доступ до спеціалізованої платформи призначеної для розробки, та тестування програмних рішень;
3. Технологія Infrastructure as a Service (IaaS) — забезпечує представлення IT - інфраструктури у вигляді віртуалізації, до складу якої входять операційні системи, спеціалізоване програмне забезпечення, та апаратне забезпечення;
4. Послуга віртуального робочого місця (Desktop as a Service (DaaS)) – надає користувачам можливість налаштування свого робочого місця та створення набору програмного забезпечення, що використовується в роботі.

Хмарні технології мають як плюси, так і мінуси. Це досить економно і підходить для використання в різних компаніях тощо. Не потребує нарощувати потужності пристрою (будь то КПК, планшет, смартфон, комп'ютер), в той же час висуваються більш жорсткі вимоги до каналів зв'язку. Це означає, що користувачам потрібно мати безперебійний високошвидкісний Інтернет. Наступним недоліком є випадки, коли сервіс знаходиться в режимі офлайн, тоді доступ до ресурсів компанії відсутній.

Як показує практика, відповідно до потреб сучасних умов роботи зручніше, ніж локальне редагування документа, помістити потрібний файл у хмарне сховище, доступ до якого може бути диференційований для ролей конкретних користувачів. Деякі користувачі можуть редагувати файл, інші можуть лише читати та переглядати зміни. Загалом, використання таких хмарних сервісів просте у використанні і не вимагає спеціальних налаштувань. Ідея створення онлайн-редактора документів існує вже давно: перші такі продукти з'явилися в 2005 році і представляли собою базовий функціонал текстових процесорів і електронних таблиць, перенесених у веб-інтерфейс.

Сьогодні хмарні технології є потужною концепцією, яка включає багато різних концепцій. Це інфраструктурна складова, програмна, платформи, дані, робочі місця і т. ін. Розглянемо найбільш істотні переваги використання хмарних сервісів у бізнесі.

Однією з головних переваг хмарних технологій є можливість заощадити компанії на дорогому програмно-апаратному забезпеченні. Адже не обов'язково встановлювати на кожне автоматизоване робоче місце ліцензоване програмне забезпечення. Крім усього іншого, хмарні сервіси в змозі забезпечити співробітників компанії використовувати лише одну операційну систему, а доступ до робочих місць здійснюється через набагато дешевші термінали.

В той же час, наявність зазначених переваг хмарних технологій їх концепція зазнає критики. Основні претензії в першу чергу стосуються безпеки, оскільки не всі вважають, що зберігати інформацію з обмеженим доступом на віддаленому сервері є безпечно.

1.2. Український розвиток хмарних технологій

Перспективи швидкого розвитку хмарних сервісів в Україні спонукають ближче поглянути на досвід їх використання на більш «зрілих» ринках. Очевидно, що навіть у порівнянні з грід-системами, не кажучи вже про «провідно-апаратні» мережі попереднього покоління, архітектура хмарного сервісу.

Хмарні технології забезпечують значне скорочення капітальних витрат на будівництво дата-центрів, закупівлю серверного та мережевого обладнання, апаратно-програмних рішень тощо. «Левову частку» цих витрат поглинає постачальник хмарних послуг. Крім того, їхній клієнт економить на обслуговуванні IT-персоналу, адмініструванні тощо. По-друге, хмарні технології дають можливість надзвичайно швидко змінювати конфігурацію корпоративної IT-інфраструктури залежно від поточних потреб, споживаючи (і купуючи) саме стільки ресурсів, скільки потрібно на даний момент.

Хмарних ресурсів зазвичай достатньо для замовлення віртуального «суперкомп'ютера» чи інфраструктури для великої корпорації, а також немає проблем з оновленням програмного забезпечення (завжди доступні останні версії), сумісністю різних операційних систем тощо. По-третє, хмарні сервіси забезпечують працівникам компанії високу мобільність до робочого місця. По-четверте, спектр послуг, які пропонують виробники та постачальники хмарних рішень, постійно розширюється.

Все це лише найвагоміші технологічні переваги хмарних сервісів, список яких можна суттєво продовжити. В той же час виробникам та провайдерам хмарних сервісів сформували гнучку та адекватну систему надання послуг [5-9]:

- Private cloud (Приватна хмара). Хмарна інфраструктура, яка обслуговує окремі організації. Управління здійснюватися як самою організацією так і сторонніми компаніями.
- Community cloud (Спільна хмара). Рішення впроваджується і використовується рядом організацій, які дотримуються однакових принципів при розробці IT-інфраструктури (вимог до безпеки, регламентів і т.ін).

- Public cloud (Публічна (громадська) хмара). Публічна хмара є загальнодоступною технологією і створена для використання великим колом користувачів.

- Hybrid cloud (Гібридна хмара). Технологія, що є поєднанням трьох попередніх моделей.

До суттєвих недоліків технології та ризиків її використання для споживачів та організацій, слід віднести наступне [8-12]:

- Залежність хмарних технологій від підключення до мережі Інтернет.

Безпеку інформації в хмарах забезпечує:

- сертифіковані фахівці: компанії та організації, наймають спеціалістів у галузі безпеки інформації для забезпечення безпеки в хмарі;

- централізоване управління, налаштування та аудит системи безпеки;

- стабільність платформи: апаратне та програмне забезпечення платформи, на якій хмара розгорнута більш рівномірно, ніж у більшості традиційних центрів обробки даних, що дозволяє краще автоматизувати захист, тестування та налагодження компонентів платформи;

- доступність ресурсів: можливість динамічного масштабування системних ресурсів, а також резервування та аварійне відновлення, які можуть бути використані для підвищення стійкості системи проти атак «відмову в обслуговуванні», а також швидкого відновлення після великих інцидентів;

- резервне копіювання та відновлення: постачальник хмарних послуг може дозволити більш високий рівень резервного копіювання;

- мобільність кінцевого користувача: завдяки хмарній архітектурі клієнти можуть використовувати різноманітні портативні пристрої, з низькою обчислювальною потужністю, доступом до Інтернету, браузером та/або кількома встановленими додатками для доступу до основних обчислювальних ресурсів.

До недоліків використання хмарних обчислень з точки зору безпеки інформації відносять [10-15]:

- Складність системи: загальна хмара є надзвичайно складним технічним рішенням порівняно з класичним центром обробки даних. Значна кількість компонентів, з яких складається хмара, дозволяє проводити атаки. Окрім засобів для віртуальних моніторів машини, гістьових віртуальних машин, зберігання даних є також компоненти, які включають в себе елементи управління: самообслуговування, ресурс обліку, управління квотами, реплікація даних і відновлення, моніторинг рівня сервісу, управління робочим навантаженням.
- Загальне багатокористувальницьке середовище: поділяють з користувачами, які їм не відомі на логічному рівні, що дозволяє зловмиснику, використовуючи вразливості всередині хмари, подолати механізм розподілу ресурсів між користувачами та отримати несанкціонований доступ до ресурсів.
- Типовий набір програмного та апаратного складу платформи означає, що типовий недолік буде проявлятися у всьому хмарному рішенні.

Слід зауважити, що в контексті «буму» хмарних технологій в Україні питання правового регулювання цієї сфери набувають неабиякої актуальності. Однак чинна редакція вітчизняного закону «Про захист персональних даних» не лише не регулює їх захист у cloud-середовищі, але у низці положень прямо конфліктує з практиками хмарних сервісів і, по суті, забороняє їх.

Але є очевидним, що при використанні хмарних сервісів (а надто – серверів крупних провайдерів з глобальним охопленням) встановити реальне місцезнаходження бази даних є неможливим в зв’язку з автоматичною міграцією серверів в залежності від завантаження. Так само, неможливо (керуючись їх визначенням в Законі) встановити «третіх осіб», у яких перебувають персональні дані володільця під час їх міграції, чи – тим більше – надати інформацію щодо транскордонної передачі.

Однією з регуляторних проблем, яка виникає разом з розвитком хмарного ринку в Україні є недосконаліть національного нормативно-правового забезпечення використання та впровадження хмарних сервісів. Актуальність цих питань обумовлюється і тим фактом, що в Україні вже існують проекти переходу на

хмарні технології IT-інфраструктур державних органів – наприклад, Національного банку України.

1.3. Поняття та класифікація загроз ІБ у хмарах

Інформаційна безпека – це стан захищеності інформаційного середовища, захист інформації – це діяльність щодо запобігання витоку захищеної інформації, несанкціонованого та ненавмисного впливу на захищену інформацію, тобто процес, спрямований на досягнення цього стану. Метою інформаційної безпеки будь-якого об'єкта є побудова системи інформаційної безпеки об'єкта.

СЗІБ - організована сукупність спеціальних органів, служб, засобів, методів і заходів, які орієнтовані на забезпечення захисту життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз.

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, забезпечення його формування, використання та розвитку в інтересах громадян, організацій», правомірним є виявлення загроз інформаційній безпеці, джерел цих загроз, способів реалізації. і мета, та інші умови та дії. порушують безпеку. При цьому, звісно, слід продумати заходи щодо захисту інформації від протиправних дій, які призводять до шкоди.

Загроза - сукупність факторів і умов, що виникають у процесі взаємодії об'єкта безпеки з іншими об'єктами, а також його компонентами та між собою і можуть мати на нього негативний вплив. Він слугує можливістю вирішити протиріччя у взаємодії об’єкта безпеки з іншими об’єктами, складовими об’єкта безпеки, що перебувають у стані дисгармонії чи конфлікту, шляхом примусової зміни у бік погіршення властивостей об’єкта безпеки або його компонентів, тобто пошкодженням.

Між загрозою і небезпекою заподіяння шкоди завжди існує зв'язок заподіяння, який визначається як обумовлений сутністю взаємодіючих об'єктів, елементів системи зв'язок між явищами, в яких одне явище, назване причиною, за певних умов

неминуче породжує ще одне явище, яке називається розслідуванням. Загрози інформаційній безпеці - це дії або події, що можуть призвести до порушень ІБ.

Якщо розглядати загрози інформації більш детально, то їх можна поділити на загрози місцям розміщення (розташування) носіїв конфіденційної інформації, загрози безпосередньо носіям інформації з обмеженим доступом, а також каналам передачі (системам інформаційного обміну).

Виходячи з вище написаного, можна зробити висновок, що загрози ІБ направлені на створення каналів витоку інформації.

При розробці необхідних засобів, методів і заходів для забезпечення захисту інформації необхідно враховувати велику кількість різноманітних факторів. Інформація, будучи предметом захисту, може бути представлена на різних технічних носіях. Його носіями можуть бути люди з числа користувачів і обслуговуючий персонал. Інформація може оброблятися в комп’ютерних системах, передаватися по каналах зв’язку та відображатися різними пристроями. Він може відрізнятися за значенням. Об'єктами охорони, на яких може бути розміщена інформація, є не тільки комп'ютери та канали зв'язку, а й приміщення, будівлі та прилегла територія. Кваліфікація порушників може суттєво відрізнятися, а також способи та канали несанкціонованого доступу до інформації.

Основними принципами забезпечення інформаційної безпеки хмарних технологій є:

- Системність.
- Комплексність.
- Безперервність захисту.
- Розумна достатність.
- Гнучкості управління і застосування.
- Відкритість алгоритмів і механізмів захисту.
- Простота застосування захисних заходів і засобів.

Способи забезпечення безпеки комп'ютерних систем є:

- нормативно-правові (законодавчі);
- морально-етичні;

- організаційно-адміністративні заходи;
- фізичні рішення;
- програмно- апаратні.

Правові заходи щодо захисту інформації включають діючі в країні закони, укази, постанови, інструкції та інші нормативні акти, які регулюють правила поводження з інформацією обмеженого використання та відповідальність за їх порушення. Таким чином вони запобігають несанкціонованому використанню інформації та є стримуючим фактором для потенційних порушників.

До морально-етичних заходів протидії належать усілякі норми поведінки, які традиційно склалися або розвиваються в суспільстві в міру поширення комп'ютерів у країні. Ці норми є як неписаними (загальноприйняті норми чесності, патріотизму тощо), так і оформлені в набір правил чи норм.

Організаційно-адміністративні заходи захисту регулюють функціонування ІВ (інформаційних систем); використання ресурсів ІР; діяльність персоналу інформаційної служби на підприємстві; порядок взаємодії користувачів із системою, щоб максимально ускладнити або зробити неможливим реалізацію загроз безпеки.

Заходи фізичного захисту включають різні механічні, електро- та електромеханічні пристрої або конструкції, спеціально призначені для створення фізичних перешкод для можливого проникнення та доступу порушників (турнікети, колючий дріт, кодові замки, системи пожежної сигналізації тощо).

Апаратно-програмні засоби захисту включають апаратні засоби та спеціальне програмне забезпечення, які реалізують самостійно або в поєднанні з іншими засобами наступні способи захисту в хмарах:

- ідентифікацію і аутентифікацію суб'єктів ІС;
- розмежування доступу до ресурсів ІС;
- контроль цілісності даних;
- забезпечення конфіденційності даних;
- аудит подій;
- резервування.

Таким чином можна стверджувати, що безпеку ресурсів може забезпечити тільки комплексна система захисту інформації. Вона має спиратися на систему видів

власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

1.4. Методи забезпечення ІБ в хмарах

Найбільш ефективні способи захисту в галузі безпеки хмар в наш час опублікувала організація Cloud Security Alliance (CSA):

1. Збереження даних. (Шифрування).

Шшифрування – є ефективним способом захисту даних. Надавач послуг шифрує інформацію клієнта, що зберігається в ЦОД.

2. Захист даних.

3. Процес автентифікації.

4. Технологія ізоляції користувачів.

Використання окремої віртуальної машини та віртуальної мережі. Віртуальні мережі мають бути розгорнуті за допомогою таких технологій, як VPN (віртуальна приватна мережа), VLAN (віртуальна локальна мережа) і VPLS (сервіс віртуальної приватної локальної мережі).

Часто постачальники ізолюють дані користувачів один від одного, змінюючи дані коду в одному програмному середовищі. Однак цей підхід має ризики.

Висновки до першого розділу.

Сучасні підприємства постійно перебувають під впливом факторів, пов’язаних з розвитком технологій, які, з одного боку, спрощують роботу з великими обсягами інформації, але, з іншого боку, викликають проблеми, пов’язані насамперед з інформаційною безпекою.

Однією з таких технологій є хмарні сервіси (хмарні обчислення).

Багато IT-компаній створили основу для власних хмарних обчислень. У 2007 році Dell випустила свою версію хмарних сервісів, IBM запустила програмне забезпечення Blue Cloud. Пізніше з’явилися такі продукти, як MapReduce від Google, Windows Azure від Microsoftware, iCloud, Amazon CloudDrive тощо.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ ПРОБЛЕМ БЕЗПЕКИ СУЧАСНИХ ХМАРНИХ ТЕХНОЛОГІЙ

2.1. Проблеми ІБ у хмарах і їх класифікація

Хмарний контроль і керування є проблемою безпеки. Немає гарантій, що всі хмарні ресурси підраховані і в ній немає некерованих віртуальних машин, що не запускаються непотрібні процеси і не порушується взаємна конфігурація елементів хмари. Це високорівневий тип загрози, тому він пов’язаний з управлінням хмарами як єдиною інформаційною системою, і для неї загальний захист має будуватися окремо. Це вимагає використання моделі управління ризиками для хмарних інфраструктур.

Основою фізичної безпеки є суворий контроль фізичного доступу до серверів та мережевої інфраструктури. На відміну від фізичної безпеки, мережева безпека передусім полягає у створенні надійної моделі загроз, яка включає захист від вторгнень і брандмауер. Використовуйте брандмауер як роботу фільтра, щоб розрізняти внутрішні мережі центрів обробки даних у підмережах з різними рівнями довіри. Це можуть бути окремі сервери, доступні з Інтернету, або сервери з внутрішніх мереж. У хмарних обчисленнях найважливішу роль платформи відіграє технологія віртуалізації. Щоб зберегти цілісність даних і забезпечити захист, розглянемо основні відомі загрози для хмарних обчислень.

Вимоги до безпеки хмарних обчислень не відрізняються від вимог безпеки до центрів обробки даних. Однак, віртуалізація ЦОД і перехід до хмарних середовищ призводять до появи нових загроз. Доступ через Інтернет до управління обчислювальною потужністю є одним з ключових характеристик хмарних обчислень. У більшості традиційних ЦОД доступ інженерів до серверів контролюється на фізичному рівні, в хмарних середовищах вони працюють через

Інтернет. Розмежування контролю доступу та забезпечення прозорості змін на системному рівні є одним з головних критеріїв захисту.

Віртуальні машини динамічні. Створити нову машину, зупинити її, перезапустити, це можна зробити за короткий час. Вони клоновані і їх можна переміщати між фізичними серверами. Ця мінливість погано впливає на розвиток цілісності системи безпеки. Однак уразливості в операційній системі або програмах у віртуальному середовищі поширюються неконтрольовано і часто з'являються через довільний проміжок часу (наприклад, при відновленні з резервної копії). У середовищах хмарних обчислень важливо надійно фіксувати стан захисту системи, і він не повинен залежати від її стану та розташування.

Хмарні сервери та локальні сервери використовують одні й ті ж операційні системи та програми. Для хмарних систем високий ризик віддаленого злому або зараження шкідливим програмним забезпеченням.

Коли віртуальна машина вимкнена, вона піддається зараженню. Достатньо мережевого доступу до сховища образів віртуальної машини. Запустити захисне програмне забезпечення на вимкненій віртуальній машині категорично неможливо. При цьому захист має бути реалізований не лише всередині кожної віртуальної машини, а й на рівні гіпервізора.

Щоб розрізняти сегменти з різними рівнями довіри до хмари, віртуальні машини повинні забезпечити собі захист, перемістивши периметр мережі до самої віртуальної машини.

2.2. Можливі атаки на хмари і рішення щодо протидії

1. Атаки на програмне забезпечення.

Традиційними загрозами є вразливості операційних систем, модульних компонентів, мережевих протоколів тощо, для захисту від яких достатньо встановити брандмауер, брандмауер, антивірус, IPS та інші компоненти, здатні вирішити цю проблему. Важливо, щоб ці засоби захисту працювали ефективно в середовищі віртуалізації.

2. Атаки на елементи хмар.

Цей тип атаки пов'язаний з багатошаровою хмарою, загальним принципом безпеки. У статті про небезпеку хмар запропоновано таке рішення: Для захисту від функціональних атак для кожна частина хмари має використовувати такі засоби захисту: для проксі - ефективний захист від DoS-атак, для веб-сервера - контроль цілісності сторінки, для сервера додатків - екран рівня програми, для СУБД - захист від SQL-ін'єкцій, для системи зберігання - коректне резервне копіювання (резервне копіювання), розмежування доступу. Кожен із цих механізмів захисту вже створено окремо, але вони не збираються разом для комплексного хмарного захисту, тому при створенні хмари необхідно вирішувати завдання їх інтеграції в єдину систему.

3. Атаки на клієнта.

Більшість користувачів підключаються до хмари за допомогою браузера. Це включає такі атаки, як міжсайтові сценарії, крадіжка паролів, перехоплення веб-сеансів, посередник тощо. Єдиним захистом від цього типу атаки є належна аутентифікація та використання зашифрованого з’єднання (SSL) із взаємною автентифікацією. Однак ці методи захисту не дуже зручні та дуже марнотратні для творців хмар. У цій сфері інформаційної безпеки залишається багато невирішених питань.

4. Атаки орієнтовані на гіпервізор.

Ключовим елементом віртуальної системи є гіпервізор. Його основна функція — розподіл ресурсів між віртуальними машинами. Атака на гіпервізор може призвести до того, що одна віртуальна машина зможе отримати доступ до пам’яті та ресурсів іншої. Він також зможе перехоплювати мережевий трафік, вибирати фізичні ресурси і навіть витісняти віртуальну машину з сервера.

В якості стандартних методів захисту рекомендується використовувати спеціалізовані продукти для віртуальних середовищ, інтеграцію хост-серверів з Active Directory, використання політики складності та застаріння паролів, а також стандартизацію процедур доступу до хосту. інструменти керування сервером, застосувати вбудований брандмауер хоста віртуалізації. Ви також можете вимкнути

служби, які часто не використовуються, наприклад веб-доступ до сервера віртуалізації.

5. Атаки на системи управління хмарами.

Для забезпечення потреб користувачів у хмарах розгортається велика кількість віртуальних машин. Втручання в систему управління може призвести до появи віртуальних машин - невидимок, здатних блокувати одні віртуальні машини і підставляти інші.

Інформаційна безпека підприємства — це захист інформації, що є власністю підприємства, від несанкціонованого доступу, знищення, модифікації, розголошення та затримки в отриманні. Крім того, інформаційна безпека означає захист інформації та її допоміжної інфраструктури від будь-яких випадкових або зловмисних дій, які можуть призвести до шкоди самій інформації, її власникам або допоміжній інфраструктурі. Архітектура ІС охоплює процеси, людей, технології, різні види інформації, адаптуючись до них, враховує складність і мінливість сучасного підприємства. Іншими словами, він описує бажану структуру інфраструктури безпеки організації та інших компонентів та інтерфейсів інформаційної безпеки.

Метою системи безпеки є [11-15]:

- захист прав підприємства (установи), його структурних підрозділів і співробітників;
- збереження й ефективне використання інформаційних, матеріальних і фінансових ресурсів;
- підвищення іміджу системи за рахунок забезпечення якості послуг щодо інформаційної безпеки.

Хмарні технології динамічно розподіляють обчислювальні ресурси у відповідь на запити користувача на резервування ресурсів і, відповідно, на певні стандарти якості обслуговування клієнтів.

Хмарні обчислення – це технологія розподіленої обробки даних, при якій комп’ютерні ресурси та потужності надаються користувачам як Інтернет-сервіс. Хмарний сервіс – це спеціальна клієнт-серверна технологія, яка передбачає використання клієнтом ресурсів (процесорний час, оперативна пам’ять, дисковий

простір, мережеві канали, спеціалізовані контролери, програмне забезпечення тощо) групи серверів у мережі, які взаємодіють наступним чином:

- для клієнта вся група виглядає як єдиний віртуальний сервер;
- клієнт може прозоро та гнучко змінювати обсяги споживання ресурсів у разі зміни своїх потреб (збільшувати/зменшувати потужність сервера з відповідною зміною оплати).

Завдяки постачальникам хмарних рішень ви можете орендувати обчислювальну потужність і дисковий простір через Інтернет. Хмарні сервіси змінюють підхід користувача до роботи з інформацією та програмами. Хмарні системи дозволяють отримувати доступ до інформації та серверів з будь-якої точки світу, позбавляючи користувачів від необхідності мати настільний комп'ютер і полегшуючи спільну роботу багатьом людям, які можуть перебувати в різних місцях. Amazon була першою компанією, яка повністю реалізувала комерційний потенціал технологій віртуалізації. Якщо до 2006 року віртуалізація розумілася як можливість розгорнути необхідну кількість віртуальних серверів на власному обладнанні, то завдяки Elastic Computing Cloud від Amazon ідея оренди віртуальних серверів на чужому обладнанні була втілена в життя. У цьому суть хмарних пропозицій класу «інфраструктура як послуга» (Infrastructure as a Service – IaaS).

Основні моделі надання послуг за допомогою «хмар» відображено в Табл.2.1:

У разі операційних ризиків проблема інформаційної безпеки в системі хмарних обчислень стає критичним елементом системи. Розглянемо деякі аспекти інформаційної безпеки «хмар». Керування безпекою віртуальної пам'яті. І для IBM Blue Cloud, і для Microsoft Windows Azure технологія віртуальних машин розглядається як платформа для основних компонентів хмарних обчислень, а різниця між Cloud Blue і Windows Azure полягає в тому, що віртуальна машина працює на Linux або Microsoft Windows.

Технологія віртуальних машин демонструє очевидні переваги, вона сприяє роботі сервера, що залежить не від фізичного пристрою, а від віртуальних серверів. У віртуальних машинах зміна фізичних параметрів або їх переміщення не впливає на послуги, які надає провайдер. Якщо користувачеві потрібно більше послуг,

постачальник може задовольнити потреби користувачів, не втручаючись у роботу обладнання. Традиційний центр обробки даних і безпеки пов'язаний з межами апаратної платформи, тоді як хмарні обчислення можуть належати серверу з числа віртуальних серверів; віртуальний сервер може приєднуватися до різних груп логічних серверів. Тому існує ймовірність взаємної атаки, що загрожує захисту віртуальних серверів.

Таблиця 2.1.

Основні моделі надання послуг за допомогою «хмар»

Послуга	Приклади
Програмне забезпечення (SaaS)	Сервіси Gmail та Google Docs
Платформа (PaaS)	Google Apps надає додатки для бізнесу в режимі онлайн; ПЗ і дані зберігаються на серверах Google
Інфраструктура (IaaS)	Надання провайдером клієнтові різноманітної комп’ютерної інфраструктури: сервісів, систем зберігання даних, мережевого обладнання, ПЗ для керування цими ресурсами

Хмарне середовище — це динамічний простір, в якому дані користувача передаються від центру обробки даних до клієнта користувача. Для системи дані користувача постійно змінюються. Можливість читання та запису даних залежить від ідентичності автентифікації користувача та налаштувань доступу. Віртуальна машина може містити різні дані користувача, які необхідно чітко контролювати. У хмарних обчисленнях актуальна схема єдиного входу та корпоративної безпеки. У цьому випадку система зв’язується зі службою контролю доступу для аутентифікації запиту до веб-служби. Веб-сервіс не реалізує власну схему аутентифікації, а делегує

це завдання зовнішньому серверу. Після отримання підтвердження автентичності веб-сервіс взаємодіє зі сховищем даних для надання інформації.

Концепція хмарних обчислень заснована на новій конфігурації. Нова конфігурація складається з безлічі нових технологій, таких як Hadoop (програмна платформа), Hbase (тип нереляційної бази даних) сімейства Apache, що підвищує продуктивність системи хмарних обчислень, але в той же час може призводять до ризику. У середовищі хмарних обчислень користувачі створюють багато динамічних віртуальних організацій, які в основному засновані на довірі між цими організаціями. Ризики часто виникають на інтерактивних вузлах між віртуальними машинами і є динамічним, непередбачуваним процесом. Середовище хмарних обчислень дозволяє користувачеві «купити» повний доступ до ресурсів, що також підвищує ризик загроз безпеці.

2.3. Вимоги до безпеки на основі аналізу технології HDFS

HDFS (HadoopDistributed File System) є відомою поширеною технологією хмарних обчислень, яка використовується у великомасштабних хмарних обчисленнях у типовій конфігурації розподіленої файлової системи. HDFS схожа на існуючу розподілену файлову систему, таку як GFS (Google File System); вони мають ідентичні цілі, продуктивність, доступність і стабільність. HDFS спочатку використовувалася в мережевій пошуковій системі Apache Nutch і стала основою проекту Apache Hadoop.

Також необхідно враховувати й інші можливості, а саме: контроль доступу, шифрування файлів тощо. Принципи захисту даних Уся процедура захисту даних побудована на конфіденційності, цілісності та доступності. Конфіденційність належить до так званої прихованої функції фактичних даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки. У випадку хмарних обчислень дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші. Цілісність даних у будь-якому вигляді не відіграє значної ролі для гарантії несанкціонованого видалення, зміни або

пошкодження. Доступність даних означає, що користувачі можуть використовувати дані за рахунок використання потенціальних можливостей хмарних технологій.

2.4. Модель захисту даних

У моделі використовується тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях «хмари».

- Перший шар відповідає за автентифікацію користувачів цифрових сертифікатів, виданих відповідними органами; управляє кодами доступу користувачів.
- Другий шар відповідальний за шифрування даних користувача, а також захист конфіденційності користувачів у певний спосіб.
- Третій шар – використання даних користувача для швидкого відновлення.

Загальносистемний захист — останній рівень даних користувача. При трирівневій структурі аутентифікація користувача використовується для забезпечення цілісності даних. Якщо відбувається незаконне вторгнення в систему аутентифікації користувачів і входить небезпечний користувач, шифрування файлів і захист конфіденційності можуть забезпечити такий рівень захисту. На цьому рівні дані користувача шифруються, якщо ключ доступу був введений незаконно. Через функцію захисту конфіденційності небезпечний користувач не зможе отримати повний доступ до інформації, що дуже важливо для захисту комерційної таємниці бізнес-користувачів у середовищі хмарних обчислень. Нарешті, швидке відновлення файлового рівня за допомогою алгоритму відновлення дозволяє швидко відновлювати дані користувача навіть у разі серйозного пошкодження.

Перехід на хмарні технології потребує значного підвищення вимог до якості надання послуг доступу до Інтернету, які стають критично важливими. Найбільше в цьому плані розвинулися американські провайдери. В американській практиці прийнято детально публікувати детальні зобов'язання щодо дотримання якості

обслуговування, які прописані в угодах про рівень обслуговування (Service Level Agreements). Якщо оператор не виконує свої зобов'язання, він несе матеріальну відповідальність. Перегляд законодавства став платформою для розподілених додатків: компанія може вести конфіденційний внутрішній документообіг на сторонніх об'єктах, уклавши контракт із стороннім постачальником SaaS, який, у свою чергу, оброблятиме дані на обчислювальній потужності інших IaaS та/або Провайдери PaaS. Існуюче законодавство (як закордонне, так і вітчизняне) таких ситуацій майже не передбачає.

Регулювання відносин у сфері хмарних технологій є складним завданням ще й тому, що інтереси користувачів, зацікавлених у збереженні контролю над своїми даними, та інтереси провайдерів хмарних послуг, зацікавлених у максимальній свободі у роботі та розвитку своїх сервісів, розходяться в протилежні сторони. Майбутнє хмарних технологій багато в чому залежатиме від розумного компромісу між двома сторонами. У роботі The Economics of the Cloud експерти Microsoft стверджують, що сьогоднішні юридичні проблеми є типовими для будь-якої нової технології і що юридичні бар'єри для хмарних обчислень більше не існуватимуть просто через природний розвиток ринку. NIST запропонував набір з десяти основних принципів безпеки для хмарних обчислень (табл. 2.2).

Таблиця 2.2.

Базові принципи безпеки для хмарних обчислень

№ з/п	Принципи	Коротка характеристика принципів
1.	Прозорість	Компанії-провайдери розкривають внутрішні правила обробки інформації, а також відомості про діяльність.
2.	Обмеження за сферами використання	Компанії не претендують на володіння даними замовників і можуть використовувати їх лише в тих цілях, для яких вони були отримані від замовників.

3.	Розкриття	Компанії розкривають дані замовників лише у випадку, якщо це потрібно самим замовникам або передбачено законом, і повинні в такому разі попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів у тій частині, наскільки це дозволяє законодавство.
4.	Система управління безпекою	Компанії володіють потужною системою захисту даних, що відповідає міжнародним стандартам (таким, як ISO 27002).
5.	Додаткові можливості у сфері безпеки	Компанії зобов'язуються пропонувати замовникам додаткові можливості щодо захисту їх даних
6.	Розміщення даних	Компанії надають замовникам список країн, в яких розміщуються пов'язані з ними дані
7.	Повідомлення про витоки інформації	Компанії оперативно повідомляють замовників про всі відомі витоки, які ставлять під загрозу конфіденційність або цілісність даних
8.	Аудит	Компанії звертаються до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпекою відповідає вимогам відповідних стандартів
9.	Переносимість даних	Компанії надають замовникам можливість вивантаження даних у стандартному форматі, придатному для передавання через Інтернет
10.	Звітність	Компанії співпрацюють із замовниками в адекватному розподілі обов'язків під час складання звітності «Про приватність і безпеку»

Хоча ці пропозиції не отримали широкої підтримки з боку учасників галузі, цілком імовірно, що в майбутньому обговорення призведе до розробки загальногалузевих правил – спочатку в США та Європі, пізніше і, можливо, одночасно в інших країнах. Це допоможе врегулювати інтереси користувачів і постачальників хмарних послуг. Українське законодавство поки не приділяє особливої уваги хмарним технологіям. По-перше, між двома сторонами немає розробленої угоди, яка б регулювала відносини між користувачем і провайдером, який надає хмарні можливості, тоді як в Європі процес оновлення законодавства у цій сфері йде досить активно.

Хмарні можливості дозволяють вирішувати бізнес-проблеми та надавати послуги користувачам у короткі терміни. Центри обробки даних можуть надавати свої послуги більшій кількості користувачів. Розробники можуть думати про нові покоління своїх продуктів. Передбачається, що масової міграції комерційних структур у публічні «хмари» не буде, повної відмови від власних дата-центрів також не очікується – хмарні сервіси прийдуть до гібридної моделі, де залишаться обидва елементи. Програмні додатки майбутнього будуть мати частину, яка працює на комп'ютері користувача, і частину, яка працює в хмарі, а загальна частина хмари повинна швидко розширюватися, щоб працювати з тисячами серверів за потреби, а також скоротитися до однієї віртуальної машини. .

Поки що необхідно не тільки розробити правову модель використання нової технології, а й розподілити взаємовідносини між користувачами та постачальниками, забезпечивши максимально розумний баланс між їхніми інтересами. Питання інформаційної безпеки технології хмарних сервісів потребують значного вдосконалення, а багато в чому – перших розробок і розробок.

Висновки до другого розділу

Інформаційна безпека підприємства — це захист інформації, що є власністю підприємства, від несанкціонованого доступу, знищення, модифікації, розголошення та затримки в отриманні. Крім того, інформаційна безпека означає захист інформації та її допоміжної інфраструктури від будь-яких випадкових або зловмисних дій, які

можуть призвести до шкоди самій інформації, її власникам або допоміжній інфраструктурі. Основним стримуючим фактором при роботі з «хмарними» ресурсами є безпека – відсутність контролю над серверами, обчислювальними процесами, можливість витоку критичної інформації. Серед інших обмежень – сумніви щодо якості хмарних сервісів, невелика кількість пропозицій, відсутність методик вимірювання продуктивності та небажання змінювати підходи до IT-стратегій.

РОЗДІЛ 3.
РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРНИХ ТЕХНОЛОГІЯХ

3.1. Системне вирішення проблем безпеки в хмарних технологіях

У комп’ютерних системах, які працюють через Інтернет, надзвичайно важлива безпека даних і програм. На збереження безпеки програм і обробки даних світові розробники сервісів та надавачі послуг виділяють значні ресурси для попередження несанкціонового доступу до даних.

У сучасному світі великі корпорації у більшості випадків використовують схожі методи та засоби забезпечення безпеки в своїх дата-центрах. Дані зберігаються в закодованому форматі, оптимізованому для роботи, а не в традиційній файловій системі чи базі даних. Дані розподілено на низці фізичних і логічних томів, що гарантує резервне збереження та раціональний доступ і, відповідно, запобігає зміненню даних чи незаконному втручанню.

Хмарні обчислення – це нова, перспективна технологія, яка поєднує обчислювальну потужність для підтримки програмних послуг. На відміну від класичних обчислювальних моделей, хмарна модель складається з сервісів, клієнтів, централізовано керованого вмісту та віртуальних машин. Різні установи покладаються переважно на власні програмні та апаратні ресурси. Хмарні обчислення є важливим напрямком у розвитку сучасних інформаційних технологій. Вони є ефективним рішенням для підтримки обчислювальної інфраструктури для багатьох користувачів. Крім того, вони надають рішення для управління даними багатьом державним установам і корпоративним клієнтам без необхідності повного адміністрування програмного та апаратного забезпечення. «Хмарне» сховище, як складова вищевказаної технології, також має багато переваг перед традиційним сховищем.

В США інститутом стандартів і технологій розроблено характеристики хмарних сервісів:

- користувач сам визначає і підбирає обчислювальні потужності, такі як серверний час, швидкості доступу та обробки даних, об’єм збережених даних без контактів з постачальником сервісу;
- універсальний доступ до мережі: послуги доступні споживачам через мережу передачі даних незалежно від використовуваного термінального пристрою;
- об'єднання ресурсів, тобто постачальник послуг об'єднує ресурси для обслуговування великої кількості споживачів в єдиний пул для динамічного перерозподілу потужностей між споживачами в умовах постійно мінливого попиту на потужність; споживачі контролюють лише основні параметри послуги (наприклад, обсяг даних, швидкість доступу), але фактичний розподіл ресурсів, що надаються споживачеві, здійснюється провайдером (у деяких випадках споживачі все ще можуть контролювати деякі фізичні параметри перерозподілу, наприклад, вкажіть потрібний центр обробки даних з причин географічної близькості);
- еластичність: послуги можна надавати, розширювати, звужувати в будь-який час, без додаткових витрат на взаємодію з постачальником, як правило, автоматично;
- облік споживання постачальних послуг автоматично розраховує споживані ресурси на певному рівні абстракції (наприклад, обсяг збережених даних, пропускна здатність, кількість користувачів, кількість транзакцій), і на основі цих даних оцінює обсяг послуг, що надається споживачам.

Служби зберігання демонструють різноманітні трансформації архітектур управління даними. Експерти прогнозують, що багато майбутніх програм, орієнтованих на дані, будуть покладатися на хмарні сервіси даних.

У хмарних середовищах контроль є особливо важливою якістю. У порівнянні з традиційними системами, досягнення високого рівня контролю в хмарних середовищах ускладнюється трьома факторами: обмеженим втручанням людини, значним діапазоном робочих навантажень і різноманітністю спільних інфраструктур. У переважній більшості випадків не буде адміністраторів баз даних

або системних адміністраторів, які могли б допомогти розробникам у створенні додатків на основі хмарних сервісів; адміністрування платформи здебільшого має здійснюватися автоматично.

Системи завжди важко налаштувати за наявності змішаних робочих навантажень, які в цьому контексті можуть неминуче виникнути. З часом навантаження навіть одного і того ж споживача може істотно змінитися: гнучке надання хмарних сервісів робить ці послуги економічно ефективними для користувачів, яким за короткий проміжок часу може знадобитися значно більше ресурсів, ніж зазвичай. У цьому випадку можливість налаштування сервісів залежить від методу «віртуалізації» спільної інфраструктури. Це вимагатиме перегляду традиційних ролей і розподілу відповідальності за багаторівневе управління ресурсами. Окрема проблема — абсолютні масштаби «хмарних обчислень».

На сьогоднішній день існують такі типи хмар: - приватні хмари, що обслуговують одну організацію, які підтримуються нею або сторонньою компанією і розташовані всередині або за межами організації. Передплатниками є корпоративні офіси та відділи, ділові партнери, постачальники сировини, посередники, учасники виробничого ланцюга та інші організації. Хмарно захищені хмари не виходять за межі закритої внутрішньої мережі, завдяки чому забезпечується більш високий рівень захисту; групові хмари, розподілені між кількома організаціями, об'єднаними спільними інтересами (за сервісом і розташуванням не відрізняються від приватних хмар); загальнодоступні або загальнодоступні хмари (public) надаються організаціям або окремим особам на базі інфраструктури провайдера хмари. Абонентом пропонованих послуг може стати будь-яка компанія та індивідуальний користувач. Пропонуйте сховище, а також простий і доступний спосіб розгортання веб-сайтів або інформаційних систем з великою масштабованістю, яка була б недоступна в інших рішеннях; гібридні хмари поєднують перераховані вище функції вищевказаних хмар.

Також можна класифікувати хмари за базовою версією моделі надання послуг: - Програмне забезпечення як послуга (SaaS) засноване на наданні додатків

кінцевому користувачеві у вигляді послуги «на вимогу» замість завантаження за адресою на конкретному робочому місці або на власному сервері; - Платформа як послуга (PaaS) - надає платформу та/або проміжне (з'єднувальне) програмне забезпечення у вигляді сервісу, на якому можлива розробка та розгортання користувацьких додатків.

Типовими рішеннями такого типу є інтерфейси прикладного програмування (API) та інструменти, а також бази даних і системи керування робочими процесами, інтегровані засоби безпеки. Ці рішення дозволяють розробникам створювати програми та запускати їх в інфраструктурі, що належить і підтримується постачальником хмарних послуг. Інфраструктура як послуга (IaaS) охоплює обладнання та технології для комп'ютерних обчислень і зберігання, операційні системи та іншу інфраструктуру, що надається не як локальні ресурси, а опосередковано через доступ до послуг, розміщених на стороні провайдера. Апаратна модель також відома як сервіс (Hardware as a Service, HaaS), але це скоріше підтип моделі IaaS. Кожна з цих категорій (сервісних моделей) може використовуватися самостійно або в поєднанні з іншими варіантами сервісних блоків. Пропонується ще один базовий варіант моделі надання послуг: аналітика як сервіс (за аналогією з попередніми візьмемо назву як Сервіс, скорочено DMaaS) — дані, які аналізує користувач, «трансформуються» у мікрокуб на «хмара». Крім того, пропонується трансформувати не тільки дані, внесені в таблицю, а й будь-які дані підприємства, яке в цьому випадку оплачує витрати на перетворення та аналізує дані.

Інфраструктура як послуга недостатньо гнучка, щоб задовольнити різноманітні вимоги споживача щодо складу та якості послуг. За словами керівників Amazon, «хмара більше не розкладається на чітко визначені шари». У майбутньому багато додатків будуть збирати різні сервіси з різних місць і об’єднувати їх разом. Важко сказати, що прийде на зміну трирівневій моделі хмарних обчислень, але аналітики Gartner вважають, що в кінцевому підсумку хмарні обчислення призведуть до концепції «Все як послуга», наприклад: Computing as a Service

(Compute aaS) , пам'ять як послуга (Storage aaS), дані як служба (Data aaS), база даних як послуга (Data base aaS) тощо (рис.3.1).

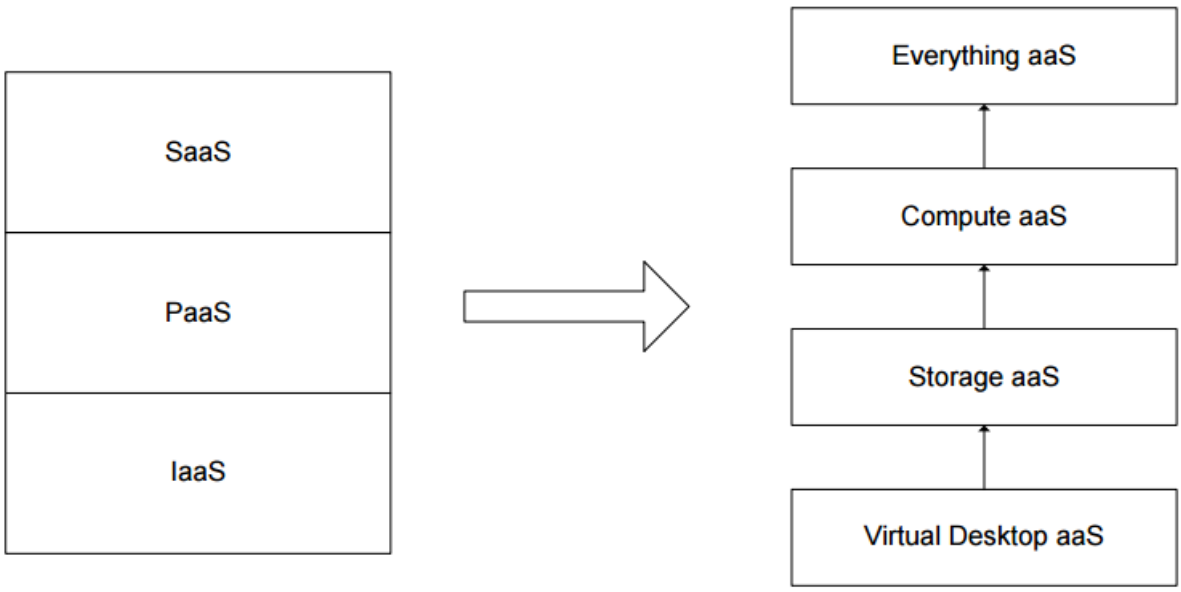

Рисунок 3.1 – Схема переходу від трирівневої моделі до моделі «Все як Послуга»

У таблиці 3.1 наведено перелік організацій та напрямів діяльності у сфері хмарних стандартів. Хмарні послуги надаються окремими операційними компаніями і мають дуже малу взаємодію. Для створення та захисту інтероперабельності необхідно створити міжнародні стандарти, які покращують мобільність програми, включаючи розподіл ресурсів між провайдерами «хмарного» сервісу. Найсерйознішу ініціативу у сфері стандартизації хмарних обчислень виявила міжнародна організація IEEE у сфері переліку стандартів і специфікацій, необхідних для створення загальних хмарних систем, а також базової інформації та рекомендацій щодо сумісності та портативності в хмарні обчислення.

Хмарне сховище — це модель онлайн-сховища, в якій дані зберігаються на численних мережевих серверах, які надаються клієнтам, переважно третьою стороною. Дані зберігаються та обробляються в хмарі, яка, з точки зору клієнта, є одним великим віртуальним сервером. Фізично такі сервери можуть бути розташовані на великій відстані один від одного географічно, аж до розташування на різних континентах. Сучасні системи баз даних, орієнтовані на SQL, не можуть

масштабуватися до тисяч вузлів, якщо вони розміщені в хмарному контексті. У сфері зберігання даних ці обмеження слід обійти за допомогою нових методів реалізації транзакційності, або за допомогою нової семантики зберігання даних, або й того й іншого.

Таблиця 3.1.

Організації та область їх діяльності у сфері стандартизації

Організація	Область діяльності
ISO/IEC JTC/SC 27 & Cloud Security Alliance	Стандарти в сфері хмарної безпеки
Cloud Standards Customer Council	Розробка хмарних стандартів, які відображають інтереси користувачів хмарних обчислень
Distributed Management Task Force (DTMF)	Стандарти управління корпоративними і хмарними обчисленнями
IEEE	Стандарти в області інтер-операбельності і практичного впровадження хмарних систем
OASIS	Актуалізація стандартів WS, SAML, XACML, KMIP
Open Cloud Consortium (OCC)	Розробка стандартів у сфері хмарних обчислень та їх сумісності
Робоча група з хмарним обчисленням у складі Open Group	Стандартизовані моделі, які дозволяють уникнути залежності від постачальника

При спільному використанні фізичних ресурсів у хмарній інфраструктурі необхідно забезпечити безпеку та конфіденційність даних, які неможливо гарантувати через фізичне розділення машин або мереж. Таким чином, хмарні

сервіси створюють міцну основу для зусиль по консолідації та прискоренню досліджень, що проводяться спільнотою баз даних у цих сферах. Ключем до успіху тут є зосередженість на конкретних сценаріях використання хмарних сервісів на основі практичних економічних стимулів для постачальників послуг і споживачів. Крім того, прогнозується поява фреймворкових додатків, які можуть вільно переміщатися між гетерогенними «хмарними» середовищами, як наслідок, зниження ролі ОС, оскільки велика частина функцій (наприклад, інформаційна безпека бере на себе ОС) користувача. отримуватиме з «хмар».

Значний інтерес до захищеності SSL-з'єднань викликаний, зокрема, розвитком хмарних технологій. Все більше число компаній і домашніх користувачів використовують хмарні сервіси для зберігання і обробки важливої інформації, а підключення до таких служб в більшості випадків здійснюється через веб-браузер з використанням технології SSL.

Якщо протокол SSL використовує один ключ для шифрування, то необхідно використовувати інший ключ для розшифрування. У цій ситуації ви можете отримувати захищені повідомлення, опублікувавши відкритий ключ і зберігаючи секретний ключ у секреті.

Резюмуючи міркування експертів, можна виділити низку обов’язкових умов, що необхідні для досягнення прийнятного (хоча й не стовідсоткового) рівня безпеки сучасного хмарного сервісу для користувача. Сьогодні це можливо за наявності таких обов’язкових складових:

1. Апаратна (фізична, хардверна) складова:

а) обладнання, на якому реалізована хмарна IT-інфраструктура, повинне знаходитися в захищеному приміщенні, з клімат-контролем, безперебійним живленням, ефективним протипожежним захистом;

б) має бути забезпечене цілодобове обслуговування усієї інфраструктури;

в) необхідним є фізичне розділення ресурсів, наприклад, інфраструктура, в якій обробляються критично важливі і конфіденційні дані, фізично повинна розташовуватися окремо від загальної інфраструктури, посилена безпека якої не передбачається.

2. Адміністративно-нормативна складова:

а) пропускний режим в приміщеннях дата-центру (аж до біометричного контролю доступу), максимальна обмеженість, регламентація та облік доступу до інформації, що зберігається в спеціалізованих сховищах і базах даних;

б) автентифікація користувачів за логіном і паролем з обов'язковим шифруванням цього процесу;

в) запровадження системи статусів користувачів з відповідною диверсифікацією прав та рівнів доступу до ресурсів інфраструктури;

г) чітке дотримання провайдером норм діючого законодавства (в аспекті безпеки українського користувача – насамперед Закону України «Про захист персональних даних»).

3. Програмна (софтверна) складова:

а) повномасштабний антивірусний захист, особливо у разі користування такими сервісами як SaaS (програмне забезпечення як послуга) і PaaS (платформа як послуга);

б) наявність спеціальних налагоджених мережевих екранів (брандмауерів, файрволів) для віртуальних машин, а також для усіх операційних систем, що задіяні в інфраструктурі;

в) захист систем та програм в частині хоча б найпоширеніших вразливостей;

г) обов'язкове шифрування принаймні важливої і конфіденційної інформації, розташованої в хмарі.

Щоб звести до мінімуму перерви в обслуговуванні через апаратні збої, стихійні лиха чи інші катастрофи, у всіх своїх центрах обробки даних слід використовувати комплексну програму післяаварійного відновлення роботи. Ця програма є багатокомпонентною, що виключає ситуації, коли відмова одного компонента призводить до відмови всієї системи. Складові перелічено нижче.

- Реплікація даних. Для забезпечення доступу в разі стихійного лиха дані, збережені в розподіленій файловій системі, реплікуються в окремі системи в різних центрах обробки даних.

- Географічне розподілення центрів обробки даних. Слід використовувати територіально розподілені центри обробки даних, що дає змогу запобігати перервам у роботі в разі стихійного лиха чи інших інцидентів в окремому регіоні. Високошвидкісний зв'язок між центрами обробки даних допомагає забезпечити швидкий перехід на інший ресурс. Керування центрами обробки даних є також розподіленим, що дає змогу забезпечити цілодобове системне адміністрування незалежно від місцеположення.

- Гнучка інфраструктура з можливістю резервування. Обчислювальні кластери сучасних дата-центрів надзвичайно відмовостійкі та підтримують резервування. Це допомагає звести до мінімуму відмови всієї системи через збій окремих компонентів, відмови обладнання й екологічні ризики. Для резервування даних використовуються здвоєні схеми, комутатори, мережі й інші пристрої. Додаткове обладнання в центрах обробки даних є надійним, стійким до відмов і може обслуговуватися без перерв у роботі.

Під час вибору провайдера дата-центру слід звертати увагу на [12-17]:

- Місцезнаходження дата-центру. Важливу роль відіграє як і юрисдикція, в якій фізично знаходиться дата-центр, так і географічне положення. Від географічного положення залежить клімат а також вірогідність стихійного лиха, що може фізично нашкодити апаратному забезпеченню дата-центра.

- Обладнання, що використовується. Слід особливу увагу звернути на апаратну складову дата-центра, бо існує ймовірність того, що на обладнанні, яке працювало великий період часу майже не зупиняючись, у будь-який момент може трапитись інцидент зносу жорстких дисків чи комутаційного обладнання.

- Кількість клієнтів дата-центру. В більшості випадків адміністрація дата-центру не зможе вам назвати що саме за компанії використовують ті самі сервери, що й ви. Існує ймовірність, що там можуть знаходитись файли та програми, що можуть фізично нашкодити вашій інформації, що знаходиться на тих самих носіях.

У стандартній моделі ЦОД, можна виділити наступні функціональні підсистеми:

- Підсистема серверів, яка надає обчислювальні ресурси для роботи корпоративних додатків;
- Підсистема селевої взаємодії, яка забезпечує надійний транспорт інформаційних потоків між компонентами ЦОД і об'єднання з магістральною мережею передачі даних;
- Підсистема зберігання даних;
- Підсистема інформаційної надійності;
- Підсистема управління та моніторингу, яка здійснює управління, моніторинг, діагностику та локалізацію невиправностей програмно-апаратного комплексу.

Окрім захисту ЦОД слід пам’ятати про канал передачі даних, який використовується. Окрім фізичного захисту каналу можна використовувати програмний захист каналу, завдяки VPN.

VPN мережа створюється поверх інших мереж або віртуальних каналах інших мереж (Інтернет). Безпека передачі пакетів через загальнодоступні мережі може бути реалізована за допомогою шифрування, в результаті чого канал зв'язку третьої сторони закривається. VPN дозволяє об'єднати, наприклад, кілька територіально віддалених мереж організації в одну мережу, використовуючи неконтрольовані канали для зв'язку між ними.

Інформаційна безпека в розумінні VPN включає шифрування, аутентифікацію та контроль доступу. Шифрування передбачає шифрування інформації, що передається через VPN. Тільки власник ключа шифру може прочитати всі отримані дані. Найбільш часто використовуваними алгоритмами шифрування в рішеннях VPN сьогодні є DES, Triple DES і різні реалізації AES.

Ступінь захищеності алгоритмів, підходи до вибору найбільш оптимального з них - це також окрема тема, обговорювати яку ми не в змозі. Аутентифікація передбачає перевірку цілісності даних та ідентифікацію осіб та об’єктів, залучених до VPN. Перший гарантує, що дані надійшли до одержувача саме в тому вигляді, в якому вони були надіслані. Найпопулярнішими сьогодні алгоритмами перевірки цілісності даних є MD5 і SHA1. Контроль трафіку передбачає визначення та

керування пріоритетами використання пропускної здатності VPN. З його допомогою ми можемо встановлювати різні пропускні здатності для мережевих програм і служб залежно від їх важливості.

3.2. Тенденції розвитку новітніх засобів захисту ІБ в хмарних технологіях

За прогнозами провідних фахівців, швидке вдосконалення та поширення хмарних технологій (хмарних обчислень) зараз є однією з ключових тенденцій, яка в найближчі 5-8 років суттєво вплине на глобальний розвиток не тільки IT-індустрії, а й бізнес, фінансову сферу, державне управління, медицину, освіту та багато інших сфер людського життя. Враховуючи прогресивний розвиток ІКТ та наступний спад у світовій економіці, технологія, яка дозволяє організаціям та іншим суб'єктам уникати значних витрат на власну IT-інфраструктуру і при цьому отримувати усі необхідних IT-ресурси онлайн, вважається перспективною. Досить сказати, що, за підрахунками авторитетної Міжнародної корпорації даних (IDC), ще у 2015 році, до 60% всіх людських даних зберігалося в хмарах. У найбільш розвинених регіонах світу вже прийняті стратегічні рішення та плани дій щодо системного та комплексного розвитку хмарних сервісів, розпочато відповідну роботу.

У глобальному масштабі хмарний ринок стає полем дедалі жорсткішої конкуренції між провідними світовими IT-корпораціями (Google, Yahoo, Amazon, Microsoft, Zoho, Cisco, Symantec, Fujitsu та багатьма іншими). Великі бізнес-гравці, які ще не мають «частки» на цьому ринку, готуються завоювати його найближчим часом. Така ситуація ще більше посилює технічну та технологічну гонку, тому нові апаратні рішення, стартапи, програмне забезпечення розробляються та просуваються в хмарному секторі дійсно швидшими темпами.

Ведеться активна робота над міжнародною стандартизацією хмарних обчислень. Два технічні підкомітети Спільного технічного комітету №1 Міжнародної організації зі стандартизації (ISO) працюють над групою стандартів і технічних звітів щодо хмарних технологій.

Викладене наочно свідчить, що хмарні технології вже є одним із значущих факторів міжнародного розвитку, вплив якого в найближчі роки зросте в рази. Як держава, глибоко інтегрована у світові інформаційно-комунікаційні процеси, Україна не може залишатися поза цим впливом.

Згідно зі зібраною статистикою споживання, хмарний ринок України, як і сусідні (Угорщина, більшість країн СНД), перебуває на етапі формування попиту та накопичення початкового досвіду споживання хмарних рішень. Про це свідчить мінімальний рівень знань кінцевих користувачів про хмарні обчислення та низький рівень проникнення технологій. Так, 47% опитаних IT-сервісів вважають свою обізнаність з хмарними рішеннями поверхневою, а 88% опитаних керівників не знайомі з хмарними сервісами.

Якщо попросити IT-фахівця зобразити карту інфраструктури компанії, якою він її бачить років через п'ять – замість схеми напевно отримаєте розповідь про потенційне співробітництво з провайдерами. Але докладного відповіді про інфраструктуру не доб'єтеся.

Вже сьогодні хмарні програми нерідко використовуються для автоматизації бізнесу за допомогою CRM, ERP, PSA і HR-систем, що зберігаються на віддалених серверах. Люди все більше використовують хмарні інструменти для спільної роботи з документами, обробки текстів і організації відеоконференцій. Багато організації переносять найбільш важливі дані в хмарні сховища, поступово відмовляючись від дорогих серверів і систем резервного копіювання. Що вже говорити, якщо навіть телефонні системи переїжджають в хмари.

Всі ці тенденції з кожним роком лише посилюються, і в майбутньому програмне забезпечення буде знаходитися десь «далеко за горизонтом», а інформація від нього — проходити через кілька фільтрів, перед тим як почати взаємодіяти з користувальницьким комп'ютером. З цієї ж причини додатки, створені на платформі як послугу, будуть абсолютно не вимогливі до можливостей комп'ютерного обладнання.

Складність і розміри окремих програм ростуть не по днях, а по годинах. У той же час, багато компаній прагнуть знижувати витрати, розбиваючи IT-інфраструктуру на окремі компоненти. Крім того, багато вимагають від розробників передбачати можливість додавання нових функцій, які не повинні позначатися на працездатності діючих програм. У зв'язку з цим, основний упор в процесі розробки програмного забезпечення буде зроблений на модулі, завдяки яким можна встановлювати динамічні частини програми, не зупиняючи і не перезавантажуючи його. Як наслідок, хмарні технології потребуватимуть нового системного мислення, і розробку програмного забезпечення доведеться обмірковувати з різних сторін. Особливо якщо врахувати, що в недалекому майбутньому додатки зможуть зберігатися не просто в хмарі: вони будуть складатися з багатьох модулів, розташованих на серверах різних хмарних сервісів. Адже плату за користування хмарними сервісами ніхто не відміняв, і розміщення окремих компонентів програм у різних сховищах може бути одним зі способів зниження вартості програмного забезпечення.

Іншими словами, різні частини додатків стане вигідніше зберігати у різних постачальників послуг. І написати програму тепер виявиться недостатньо — в найближчому майбутньому доведеться забезпечувати надійні угоди з обслуговування програмних пакетів між провайдерами.

Вже сьогодні на ринку доступні малопотужні чіпи, які дозволяють використовувати для обробки даних процесори з низьким споживанням енергії. Цілком ймовірно, що через п'ять-шість років малопотужні чіпи будуть скрізь, навіть в мікрохвильових печах. Все це призведе до серйозного зниження витрат на електроенергію, і за долар можна буде зробити набагато більше корисної роботи, ніж сьогодні.

В результаті хмарні провайдери добре заощадять на оплату електроенергії і поділяться частиною економії з розробниками: за даними IDC, ринок, а відповідно і конкуренція між хмарними сервісами, буде рости на 25-30% щорічно протягом

наступних п'яти років, що змусить постачальників послуг знижувати ціну настільки, наскільки це можливо.

За результатами щорічних досліджень компанії Gigaom, в найближчі два роки до 70% найбільших IT-компаній перенесуть основне програмне забезпечення в хмари. І всі вони потребуватимуть надійних гарантій безпеки для своїх даних.

Сьогодні розробники зайняті тим, щоб довести людям, що за хмарними технологіями майбутнє і незабаром програми, платформи та послуги будуть розміщуватися тільки в хмарах. Через п'ять-сім років це питання відпаде сам собою, і експерти зможуть сконцентруватися на питаннях захисту хмарних технологій, що використовуються для вирішення складних проблем і обробки великої кількості інформації, замість того, щоб переконувати користувачів у перевагах хмар.

Безсумнівно, фізична безпека центрів обробки даних також важлива, як надійне шифрування інформації. В недалекому майбутньому мінімальні вимоги до нинішнього протоколу SSL будуть серйозно змінено: напевно доведеться забути про нинішніх 256 біт, як забули про шифрування 56 — та 60-бітового шифрування. У зв'язку з постійно зростаючими вимогами до безпеки, фізичний доступ до ЦОД також буде серйозно обмежений, і для входу в охоронюване приміщення знадобиться не тільки електронний ключ, але і процедура біометричного сканування. Системи сигналізації, існуючі сьогодні, також зміняться (вони в принципі удосконалюються кожен рік).

На додаток до фізичної безпеки даних будуть вдосконалені технології VPN, щоб захистити передачу даних. Вже сьогодні тенденції розвитку архітектури VPN дозволяють забезпечувати захист не тільки текстових даних, але і відеододатків, голосової інформації. У найближчі два-три роки кількість нових рішень щодо удосконалення безпеки тільки зросте. Нові політики брандмауера обмежать VPN-трафік на конкретні IP-адреси і порти, а з оновленою прошивкою хмарні сервери будуть захищені в рази надійніше, ніж сьогодні.

Світ не стоїть на місці, а розвивається з такою швидкістю, що вже почалися проблеми з IP-адресами. Проте до того моменту, коли хмара стане стандартом для всіх додатків і інтернет охопить все навколо, поки далеченько. Багато бізнесменів і

раніше використовують потужні комп'ютери для обробки даних. Але незабаром хмари сильно розвантажать комп'ютери і забезпечать доступ до даних скрізь, де є інтернет.

З плином часу програмне забезпечення стає все більш стандартизованим: провідні компанії працюють над сумісністю веб-додатків; щоб відкрити файл у форматі PDF, вже необов'язково встановлювати Acrobat, а Word 2013 і зовсім здатний працювати з файлами десятка різних типів. Брайан Поузі (Brien Posey), не раз визнавався Microsoft MVP, вважає, що формати програмного забезпечення будуть стандартизовані, як були стандартизовані роз'єми для мобільних.

Це дозволить компаніям легко взаємодіяти один з одним. А в кінцевому підсумку хмарні обчислення призведуть до змін виробничого циклу і зміцнять зв'язки в роботі різних компонентів, необхідних для створення кінцевого продукту. Все це змусить виробників випускати більш якісну продукцію за більш низькою ціною.

Висновки до третього розділу

За результатами щорічних досліджень компанії Gigaom, в найближчі два роки до 70% найбільших IT-компаній перенесуть основне програмне забезпечення в хмари. І всі вони потребуватимуть надійних гарантій безпеки для своїх даних.

Найбільш ефективні способи захисту в галузі безпеки хмар в наш час опублікувала організація Cloud Security Alliance (CSA), до них відносяться: шифрування, автентифікація, використання індивідуальних віртуальних машин і віртуальної мережі. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій, як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service).

Міжнародними організаціями та експертами ведуться роботи щодо розробки та впровадження стандартів та технічних регламентів стосовно використання хмарних технологій і забезпечення їх безпеки.

ВИСНОВКИ

Майбутнє хмарних обчислень — це шанс для величезного технологічного ривка компаній, що сьогодні використовують дану технологію. Вище описані лише деякі тенденції, пов'язані з розвитком хмарних обчислень. Проте вже через кілька років ми побачимо, що хмари принесуть світу набагато більше користі, ніж можна припустити зараз. Власникам компаній варто залишатися в курсі останніх подій у світі хмарних технологій, щоб зберігати конкурентні переваги. А користувачам — чекати, коли розвиток хмарних технологій позначиться на загальному рівні життя. Дуже скоро хмарні технології дозволять працювати швидше і ефективніше, ніж це відбувається сьогодні. І разом з їх поширенням буде прискорюватися наше життя.

Питання інформаційної безпеки технології хмарних сервісів потребують значного вдосконалення, а багато в чому – перших розробок і розробок.

Тому в сучасних умовах безпеку інформаційних ресурсів може забезпечити лише комплексна система захисту інформації. Комплексна система захисту інформації має бути: безперервною, плановою, цілеспрямованою, конкретною, активною та надійною. Система захисту інформації має базуватися на системі видів власної підтримки, здатної реалізувати своє функціонування не лише в повсякденних умовах, а й у критичних ситуаціях.

У будь-якому випадку інформаційна безпека відіграє на підприємстві важливу роль, і слід звертати на це увагу. Для забезпечення безпеки документообігу, корпоративних розрахунків та планування слід використовувати хмарні технології, що більш економічно вигідно для підприємства, ніж нове та потужне обладнання.

В наш час ще не сталося революційної зміни підходу до захисту інформації в хмарах: як і раніше, інформація на сервері (в дата-центрі) має бути зашифрована за допомогою останніх розробок в області криптографії. Під час з’єднання клієнта за сервером мають використовуватись безпечні протоколи передачі даних, такі як HTTPS та SSL.

Сучасні хмарні технології (хмарні обчислення) є прогресивним і перспективним рішенням, одним із елементів революційної «третьої IT-платформи». Їх швидке поширення зараз є однією з ключових тенденцій, яка суттєво вплине на глобальний розвиток у найближчі 5-8 років. У найбільш розвинених регіонах світу (США, ЄС) вже прийняті стратегічні рішення та плани дій щодо системного та комплексного розвитку хмарних сервісів, розпочато відповідну роботу.

Використання хмарних технологій пов’язане не тільки з величезним скороченням та інтенсифікацією витрат, але й зі значними ризиками для споживачів (особливо ризиками зберігання та передачі даних). З іншого боку, (а) хмарні рішення постійно вдосконалюються, і (б) постачальник хмар сьогодні може досягти прийнятного рівня безпеки, ретельно дотримуючись ряду умов.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Угрозы облачных вычислений и методы их защиты» [Електронний ресурс]. - Режим доступу : http://habrahabr.ru/post/183168/.

2. «Хмарні обчислення» [Електронний ресурс]. - Режим доступу : http://uk.wikipedia.org/wiki/Хмарні_обчислення.

3. GfK Ukraine. De Novo и GfK Ukraine измерили облачный потенциал Украины. [Електронний ресурс]. - Режим доступу : http://www.gfk.ua/public_relations/partners_news/materials/010936/index.ua.html.

4. Волокита А., Мухін В., Стешин В. Специфіка інформаційних систем на основі технології cloud computing [Електронний ресурс]. - Режим доступу : http://archive.nbuv.gov.ua/portal/natural/vcndtu/2011_53/29.htm.

5. С.Л. Гнатюк «Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики". Аналітична записка [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1191/.

6. А.М.Кух «Кому потрібні хмарні технології» [Електронний ресурс]. – Режим доступу: http://kukh.ho.ua/kurs/KITON/H1.pdf/.

7. Биков В.Ю. Технології хмарних обчислень, ІКТ-аутсорсинг та нові функції ІКТ-підрозділів навчальних закладів і наукових установ / В.Ю.Биков // Інформаційні технології в освіті. –2011. – № 10. – С. 8 – 23.

8. Коптелов А., Беркович В. Вопросы информационной безопасности при аутсорсинге IT-процессов компании [Електронний ресурс]. – 15.05.2007. – Режим доступа: http://citcity.ru/15815.

9. IBM Cloud Academy. [Электронный ресурс]: (портал компании IBM) http://www.ibm.com/solutions/education/cloudacademy/us/en – Заголовок з екрана.

10. Justin Reich, Thomas Daccord, Alan November. Best Ideas for Teaching with Technology: A Practical Guide for Teachers, by Teachers. New York: M.E. Sharpe, 2008. – 291 p.

11. Michael Miller. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online. Que Publishing, 2008. – 312 p.

12. Microsoft Operations Framework [Електронний ресурс]: (портал компанії Microsoft). – 2010. Режим доступу: http://www.microsoft.com/mof.

13. «Угрозы облачных вычислений и методы их защиты» [Електронний ресурс]. - Режим доступу : http://habrahabr.ru/post/183168/.

14. «Елементи розвитку та перспективи досліджень технології хмарних обчислень» [Електронний ресурс]. - Режим доступу (www.dnu.dp.ua) : http://www.kpi.kharkov.ua/archive/1154825.pdf.

15. 4. Бодрук О.С. Структура воєнної безпеки: національний та міжнародний аспекти. — К.: Національний ін-т проблем міжнародної безпеки, 2001. - 299 (ej.kherson.ua) с.

16. Голубев В.О.. Гавловський ВД., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використаная комп'ютерних технологій // За заг. ред. д.ю.н. Калюжного Р.А. — Запоріжжя: Просвіта, 2001. — 252 с.

17. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. - 2003. - № 5. - С. 2-3