УДК 004.89 **doi: 10.26906/SUNZ.2023.3.075**

В. Б. Важинський, В. М. Ткачов

Харківський національний університет радіоелектроніки, Харків

ПРОБЛЕМАТИКА БЕЗПЕКИ ТА КРИТЕРІЇ хНАДІЙНОСТІ МУЛЬТИХМАРНИХ СЕРЕДОВИЩ

Анотація. Мета статті – познайомитися з проблематикою безпеки мультихмарних середовищ і проаналізувавши причини виникнення цих проблем сформувати на їх основі власні критерії безпечної хмари. Викладені головні проблеми та критерії надійності мультихмарних середовищ для подальшого їх аналізу. Було освітлено пріоритетні міні-проблеми, які мають зв'язок з головними. **Завдання:** проаналізувати будь-які інформаційні джерела за напрямом та відповідною темою, окреслити проблеми та пов’язані з ними загрози і ризики в області хмарної безпеки, проаналізувати основних провайдерів хмарних послуг, розглянути перспективи і застосування на ринку, довести доцільність використання підходу мультихмарності, сформувати власні критерії безпечності хмарних систем. **Результати дослідження.** В цій статті при знайомстві з хмарним світом і історією його виникнення, а також при розгляді через призму розвитку популярності хмар в якості IT-тренду наведені існуючі ризики та загрози виникнення сучасних дірок безпеки в хмарному секторі, які сповільнюють подальший розвиток IT-індустрії. Описані фундаментальні проблемні моменти роботи хмарних обчислень в інфраструктурі. Проведено порівняльний аналіз найвигідніших сучасних хмарних систем, що задають темп іншим організаціям хмарного ринку. Досліджено доцільність та область використання хмарних середовищ. Запропоновані загальні критерії надійності виправленого хмарного продукту, на основі причин виникнення проблем мультихмарних середовищ. **Висновок**. Закладено основу для подальшого майбутніх досліджень хмарної безпеки, розробки рішення по забезпеченню надійності хмарних систем та вдосконаленню наявних компонентів хмарних технологій в IT-інфраструктурі.

Ключові слова: мультихмарне середовище, хмарна безпека, хмарні обчислення, мультихмарність, критерії надійності, кіберзлочинець, IT-інфраструктура.

Вступ

Постановка проблеми. Нарощування об'ємів цифрового кома відбувається в неконтрольованій геометричній прогресії, тому на сьогодні, ризиковано залишати важливі відомості на локальному носії, для цих випадків вже створений тип програмно-технічного середовища. Прикладом вищеописаного довкілля є хмара, її простий спосіб експлуатації та некоректно налаштований доступ до розташованих в ній об'єктів, становить загрозу надійності всієї системи. Також зі збільшенням кількості хмарних продуктів зростає складність їх інтеграції, контролю, розробки та забезпечення ефективної, стабільної та безпечної роботи. Перераховані міні-проблеми, якщо їх не вирішити або частково не зменшити їх негативний вплив, можуть перетворити надії та гарантії успішності роботи в хаос. У результаті, не релевантні методи забезпечення ефективного рівня безпеки або їх відсутність викликатимуть серйозні занепокоєння щодо втрати або витоку даних організації та її клієнтів. Зараз також в нашому сучасному світі, актуально захистити кожен збережений біт інформації і підібрати наявні підходи або у разі необхідності відновити вже втрачені файли. При бурхливому розвитку хмарних технологій та бажанні бізнесменів, швидко зробити власний продукт максимально легким та зручним, мало приділяли уваги до безпеки. Наразі ключовими факторами сповільнення вирішення питань безпеки все ще є людський фактор, не вигідні втрати продуктивності заради захисту продукту та складність комплаєнсу з урахуванням індивідуальних обмежень компанії в залежності від завдання. Хмари все більше вбудовуються в наше життя і тепер з кожним кроком їх розвитку, користувачі переконані що такий невиправданий темп пов'язаний з потребами жадібного ринку споживачів, які не дають шансу розробникам проектів або стартапів хоча б на середній рівень задовільнити вимоги до безпеки. Таким чином монопольні компанії в маркетинговій гонці за грошима будуть успішно втрачати репутацію, коли клієнти сконцентруються на більш вигідних унікальних рішеннях конкурентів. Зараз як ніколи це актуально, під час сурової конкуренції між технологічними-технічними компаніями, клієнт має максимальну вигоду за рахунок одночасної взаємодії різних хмарних сервісів з інфраструктурою та платформами серверів. Якщо ми кажемо про масштаби цілої організації, тоді не створюють з нуля нові рішення та відповідно їм додаткові перепони для бізнесу, завжди застосовують і вдосконалюють існуючи стратегії в IT-сфері, наприклад, мультихмарність. Завдяки хмарній інфраструктури, користувачі можуть, будь-де, при наявності доступу до хмари, в зручний час використовувати розподілені ресурси для дій при виконанні різнорідних завдань. Значить будь-яка вразлива частина або вузол, який був зламаний, IT-інфраструктури при задіянні декількох хмар може стати ризиковою системою №1. Окремо, хочеться наголосити, що додатковим економічним тягарем для юридичних та публічних обличь є складність забезпечення конфіденційності даних. В хмарних продуктах, при впровадженні хмарних обчислень співробітникам корпорацій не вистачає знань та досвіду, щоб перевірити, які елементи інфраструктури під безпекою. Звідси пішла необхідність більш детально досліджувати даний напрям з різних боків в плані безпеки та надійності хмар. На мою думку, чим більше якісних досліджень ми зробимо, тим швидше наші праці дадуть шанс вирішити поточні проблеми або зменшити поганий вплив на IT-сферу. Освітливши насущні проблеми надійності хмарного сектору і на основі

причин їх виникнення, необхідно знайти критерії безпечної хмари, щоб вони стали орієнтиром для знаходження або створення, у майбутньому, методу забезпечення надійності хмарних систем. Звісно необхідно врахувати роботу інших діячів для подальшого якісного та унікального дослідження. Не дивлячись на новизну технології, пов'язаною з хмарами, вони в подальшому обов'язково будуть незамінними ще декілька років та можливо стануть частиною нових винаходів, але без рішень сучасних проблем, хмарні перспективи залишаться нездійсненною мрією.

Аналіз останніх досліджень і публікацій. В веб-сайті [1] стисло проводена екскурсія по хмарному світу. Унікальні статистичні дані взяті з джерела [2] і там же вони детально описані. Наукова стаття [3] надає нам готовий результат аналізу різних хмарних продуктів нашого часу. Електронний ресурс [4] розповідає про актуальність та необхідність у використанні мультихмарності в бізнесі. Робота [5] показує наявні документи по хмарним питанням. В інтернеті [6] описаний окремий розділ комп'ютерної безпеки – безпека хмарних обчислень.

Мета статті – познайомитися з проблематикою безпеки мультихмарних середовищ і проаналізувавши причини виникнення цих проблем сформувати на їх основі власні критерії безпечної хмари.

Виклад основного матеріалу

Людство, після цифрової революції минулого сторіччя та реалізації концепції хмарних обчислень, настільки пришвидшила свій технологічний прогрес, що вийшла на новий рівень можливостей і паралельно з ними з'являються нові або погіршуються раніше невирішені проблеми надійності інформації. Наприклад: ефективність потужних мереж, низька вартість обладнання та пристроїв зберігання і обробки, а також необхідне масштабне вбудовування віртуалізації. Саме такі досягнення створили основу для проблем із-за пов'язаних з ними потенційних загроз та ризиків інформаційної безпеки, які будуть специфічними для хмар та обчислень. Варто згадати що, єдина перша складова навколишнього світу – це інформація, необмежений доступ до неї став ключовою подією у сучасній історії. Тому зараз, компанії усвідомлюють, що задіяння хмари – це геніальний шанс щоб, легко, швидко та за незначну вартість, отримати доступ до найкращих додатків у своїй галузі. Але із-за зросту конфіденційної інформації, яка розміщується в хмарі, починає зростати занепокоєння з приводу того, наскільки безпечним є це середовище.

Щоб повністю і точно розгледіти всю глибину проблем, потрібно хоча б поверхнево відповісти на ряд логічних питань:

1) З чого почалася ідея зі створення інформаційної хмари і як далі вона розвивалася в ідеал?

2) Наскільки зараз важливі хмарні технології для нас і яка область їх застосування на ринку IT-індустрії?

3) Хто є головними постачальниками хмарних середовищ?

4) Які існують плани, перспективи та шанси у подальшому для хмарного напряму?

Перед послідовної відповіддю на перераховані питання, краще почати з маленької історичної довідки та визначенням хмарних обчислень.

Згідно з визначенням Національного інституту стандартів і технології (NIST) США, Хмарні обчислення (від англ. Cloud Computing) — це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та вивільнені з мінімальними управлінськими затратами та зверненнями до провайдера [1]. Першим же кроком до втілення хмарних обчислень можна вважати появу ASP (Application service provider - провайдери послуг доступу до додатків) у другій половині 1990х років. ASP можна вважати одними із перших SaaS сервісів. Пальма першості належить сервісу електронної пошти від компанії Hotmail. Але відсутність на той час широких каналів інтернет та технологій віртуалізації стали на перепоні - за відсутності швидких та стабільних каналів інтернет користувачі не могли отримати якісні послуги, а без технологій віртуалізації неможливо було ефективно та гнучко розподіляти ресурси та масштабувати сервіси (рис. 1) [1].

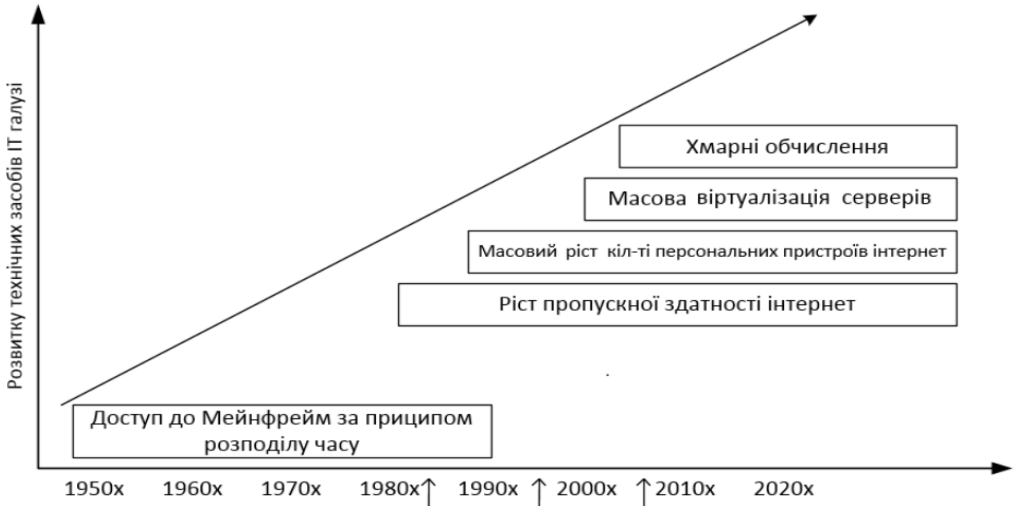

Рис. 1. Розвиток IT галузі (джерело: [1, С. 1])

В цей момент доцільно наголосити що хмарочки залишаються актуальними, тому що на сьогодення задовольняють запити більшості користувачів. Вони це довели не тільки в теорії, але і в своїй справі. У глобальному вимірі, хмарні сервіси розповсюджені у багатьох галузях. Відповідно, за галузевим розподілом перше місце посідає IT-сектор (50 %), друге – сфера фінансових послуг (14 %), третє – державний сектор (рис. 2) [2].

Рис. 2. Розповсюдженість хмарних сервісів за сферою використання (джерело: [2, С.3])

Для перерахуванням факторів виникнення проблем та їх самих з подальшим описом, важливо проаналізувати проблемні місця – хмарні продукти. За кожною хмарою стоїть свій провайдер, в такому ареалі не багато основних постачальників, згідно статистики приблизно дві третини ринку заняті проектами великих корпорацій такими як: Amazon Web Services, Microsoft Azure, Google Cloud Platform.

На їх прикладі, ми можемо побачити більшість сучасних проблем хмар, тому що ці компанії-виробники зараз задають темп розвитку хмар на ринку (табл. 1) [3].

Таблиця 1 – **Популярні послуги хмарних обчислень** (джерело: [3, С.4])

	Google Cloud Platform	Amazon Web Services	Microsoft Azure
Віртуальні машини	Compute Engine	EC2	Virtual Machines
Хостинг сайтів	App Engine	Elastic Beanstalk	Cloud Services
Системи контейнерів	Container Engine	EC2 Container Service	Container Service
Бази даних	Cloud Bigtable	DynamoDB	CosmosDB
Аналіз даних	BigQuery	Redshift	SQL Database
Обробка даних	Cloud Functions	Lambda	Functions
Бази даних	Cloud Datatastore	DynamoDB	Cosmos DB
Зберігання	Storage	S3	Blob Storage

Наприклад, нещодавнє дослідження State of the Cloud, проведене компанією Flexera, показало, що в 2019 році, принаймні на ринках економічно розвинутих країн, доля організацій, що використовують декілька хмарних послуг різних операторів, досягла 84%. Приблизно того ж висновку дійшли і аналітики Gartner — нещодавно проведене опитування представників експертного середовища продемонструвало, що 81% респондентів працюють з двома чи більше провайдерами. [4, С.1]

Загальна безпека. В якому місці надійніший захист для даних, в локальних пристроях або на віддалених серверах?

З одного боку, дані користувачів мають кращу безпеку при внутрішньому керуванні, з іншого боку, провайдери хмарних послуг вигідно зберігають стабільну довіру і для цього використовують найбільш доступний рівень безпеки. Важливо врахувати що інформація клієнта фізично знаходиться в різних куточках світу. Тому, перед застосуванням хмарних обчислень необхідно врахувати можливі загрози або ризики і для протидії їм, потрібно перевірити наявність механізмів хмарного захисту та контролю.

Недостатність ресурсів та досвіду. Не звертаючи увагу, на те що більшість IT працівників покращують свій досвід, компаніям складно знайти актуального та вагомого фахівця на ринку праці. В даній ситуації технології випереджають ринок, тому різниця в швидкості засвоєння нового стала значуща настільки, що справжні професіонали просто ще не встигли вирости в робочому плані. Високі вимоги по вирішенню та некоректна оцінка поставленого завдання знецінює будь-яку кількість наданих ресурсів. Спільне використання ресурсним потенціалом вірогідно надає тимчасовий доступ сторонньому користувачу у разі випадкового відкриття шляху до самих ресурсів.

Зайві витрати у хмарі. Деякі IT робітники, такі як розробники, вмикають хмарний сервіс з обмеженим часом дії і забувають його вчасно вимкнути. Окремим корпораціям заважає сміття та шум у хмарному трафіку, які не використовується. Бізнесмени інколи забувають, що хмарні проекти не обов'язково гарантують економію витрат, адже організації полюбляють робити зайві резервування або полінитися зробити моніторинг та автоматизацію процесів власних витрат.

Враховуючи популярність лідерів поставки хмарних послуг, варто не забувати що, в залежності від часу, немає такого місця куди не міг дістатися злодій або у нашу цифрову еру – кіберзлочинець. Лакомим шматочком для зловмисників є хмарні сервіси, які привертають увагу хакерів при наявності в них однієї із загроз та ризиків хмарної безпеки:

- втрата або витік даних;
- порушення цілісності системи;
- великі фінансові витрати;
- відсутність належного захисту;
- неправильне або некоректне налаштування хмарної системи безпеки;
- існує тільки частковий контроль та керування хмарним довкіллям;
- стихійні, фізичні, помилкові пошкодження;
- занадто велика небезпека використання привілейованого доступу до значущих частин роботи;
- відсутність правової міжнародної справедливості та підтримки у хмарних питаннях;
- схильність до різного виду хакерських атак.

Тепер можливо навести загальні критерії захищеної хмари, яку ми хочемо отримати в результаті успішної роботи майбутнього методу.

Для цього, ми, по пріоритету та с описом, наведемо, с різних сторін, критерії безпеки мультихмарних середовищ.

Наявні ліцензії хмар і її відповідність різним законам та нормам безпеки. Ліцензування це не тільки маркетинговій хід на якому можна заробити, також такий підхід виправдовує себе в плані безпеки. Вся відповідальність за якість продукту покладається на розробника або постачальника, якщо надається послуга. З'являється лояльне вирішення банальних хмарних питань у правовому полі та збільшується довіра до самого виробника або власника ідеї.

Аргументована доцільність використання і ефективно оптимізовані витрати на IT-інфраструктуру. Умовою коли потрібно заощадити завжди була обмеженість в ресурсах, потім клієнт шукає шляхи для економії і нажаль більшість жертвують хмарною безпекою системи заради її швидкодії та після атаки на інфраструктуру, розуміють що вони втратили більше ніж могли. Також вищеописане стосується працівників, коли рішення одного фахівця переважають кількісну перевагу в колективі. Це важливо для будь-якої компанії, які звикли планувати і прогнозувати свої витрати.

Надається більше контроль над продуктом для кращої його якості. Ідеальний той постачальник, який дозволяє контролювати найбільшу кількість процесів, засобів та даних в хмарі. Вільне володіння хмарою дасть можливість задовільнити різноманітні потреби, наприклад, завжди можна отримати повідомлення і вчасно на нього відреагувати, або детально налаштувати політику доступу до хмари.

Створено звід відкритих міжнародних стандартів та специфік по хмарним питання в області безпеки. Більшість провайдерів хмарних послуг мають у своєму «арсеналі» власний механізм для програмування, який може бути задокументованим, але така практика призводить до неможливості переходу користувача до іншого постачальника. Єдиним рішенням цього питання є розробка ефективних та унікальних стандартів і специфік.

У США асоціація Cloud Security Alliance випустила Cloud Controls Matrix. Цей документ являє собою перелік існуючих технологій інформаційної безпеки, які можуть бути використані в хмарних сервісах. Хоча деякі фахівці вважають, що для управління ІБ при побудові хмари SaaS можуть бути використані стандарти ISO 27001 та ISO 27002, все ж необхідна розробка спеціальних стандартів для хмарних обчислень [5].

Висновки

В даній науковій роботі ми поверхнево розкрили відповідну тематику і досягли поставленої мети за власним планом. Для цього робота була розділена на декілька частин, кожна з яких логічно та послідовно доповнювала попередню. Після мотивації, роз'ясненням сучасних проблемних обставин хмарної безпеки в IT-індустрії, ми трішки познайомили читачів історією та визначенням хмарних обчислень. Потім, як по нотам, нам вдалося через призму розвитку і статистику області застосування хмар, знайти проблеми в проаналізованих нами хмарних продуктах на наявність вагомих загроз та ризиків для хмарної безпеки.

Додатково навели відомості доцільності застосування стратегії мультихмарності на практиці. Відокремили фундаментальні проблеми та пов'язані з ними знайдені загрози та ризики, які потребують подальших ефективних і актуальних рішень. Наостанок розробили власні ознаки надійної хмари.

Список літератури

1. Хмарні обчислення. 2023. URL: http://surl.li/hdptk.
2. Рубцова М. Ю. Хмарні технології як інструмент поглиблення віртуалізації фінансового сектору. *Електронна економіка*, 2020, № 5. URL: http://www.economy.nayka.com.ua/pdf/5_2020/112.pdf.
3. Дідківська С.О. Платформи хмарних обчислень: порівняльний аналіз. Житомирський державний університет імені Івана Франка. *Semantic Scholar*, Corpus ID: 200208573, С. 131–136. URL: http://surl.li/kxurb.
4. Multicloud - перевага чи проблема. URL: https://denovo.ua/blog/multicloud-perevega-chi-problema-75.
5. Никишин Д.Д., Федюшин О.И. Ризики інформаційної безпеки в хмарних сервісах. *GLOBAL CYBER SECURITY FORUM 2019*: матеріали першого міжн. науково-практичного форуму. Харків: ХНУРЕ, 2019. С. 80–81. URL: http://surl.li/kxvhq.
6. Безпека хмарних обчислень. Матеріал з Вікіпедії — вільної енциклопедії. URL: http://surl.li/kxuvd.

Received (Надійшла) 11.07.2023
Accepted for publication (Прийнята до друку) 13.09.2023

Security issues and reliability criteria of multiple cloud environments

B. Vazhynskyi, V. Tkachov

Abstract. The purpose of the given work is to shed light on the critical and actual reliability problems of multi-cloud environments. In this scientific article, we outlined the main problems and reliability criteria of multi-cloud environments for their further analysis. For this purpose, priority mini-problems related to the main problems were highlighted. The work is divided into three small parts, each of which complements each other and fully reveals the subject of the article. In the first part, the problem of multiclouds is described in detail, what is its state, the causes of its occurrence, how relevant the problems are for users of any clouds and why they need to be solved in the near future, and note the considered possible consequences of ignoring them. Also, the connection of problems with practical and scientific tasks was drawn up in order to offer solutions in cases of a combination of cloud products from different providers in the IT infrastructure. In the second part, we got acquainted with the basics of the cloud world and the main providers of the cloud market, using their example, we listed various risks and threats of clouds that caused key reliability problems. In the final third part, the formed criteria of a secure cloud with multicloud are offered to your attention, which can become a guide for choosing a universal method for ensuring the reliability of multicloud or similar systems. Of course, for the uniqueness of the scientific work, a specific goal was given and the well-known works of other figures in the direction of this topic were analyzed. Further details and results can be seen in the conclusions section.

Keywords: multicloud environment, cloud security, cloud computing, multicloud, reliability criteria, cybercriminal, IT infrastructure.