ТЕХНІЧНІ НАУКИ

DOI: https://doi.org/10.32839/2304-5809/2021-7-95-1
УДК 004.75

Андрощук О.В., Голобородько М.Ю., Головченко О.В.
Національний університет оборони України імені Івана Черняховського
Миронюк А.Б.
Міністерство оборони України

ТЕОРЕТИЧНІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЦЕНТРІВ ОБРОБКИ ДАНИХ В ПРИВАТНИХ ХМАРАХ: ВИМОГИ ПОБУДОВИ, ВИДИ, ПЕРЕВАГИ ТА НЕДОЛІКИ, НАДІЙНІСТЬ

Анотація. У статті було проаналізовано та визначено поняття "приватних хмар", загальні принципи використання центру обробки даних (далі ЦОД) у "приватних хмарах", визначено поняття ЦОД, історію його зародження та розвитку. Проаналізовано усі недоліки і переваги існуючих ЦОД порівняно з локальними аналогами. Також було розглянуто питання інформаційної безпеки ЦОД у "приватних хмарах" та захисту даних. Особливу увагу приділено особливостям застосування даної технології в організаціях, а також в якості основи розроблюваних систем інформаційної інфраструктури. Виокремлені актуальні проблеми, які виникають під час експлуатації ЦОД. Проаналізовано приклади зарубіжного досвіду успішного використання ЦОД у "приватних хмарах".

Ключові слова: ЦОД, центр обробки даних, бази-даних, сервери, приватна хмара, сервіс, хмарні технології.

Androshchuk Olha, Holoborodko Maksym, Golovchenko Oleksandr
The National Defence University of Ukraine named after Ivan Cherniakhovskyi
Myroniuk Andrii
Ministry of Defence Ukraine

THEORETICAL PECULIARITIES OF USING DATA PROCESSING CENTERS IN PRIVATE CLOUDS: CONSTRUCTION REQUIREMENTS, TYPES, ADVANTAGES AND DISADVANTAGES, RELIABILITY

Summary. The article analyzes and defines the concept of "private clouds", general principles of using data center (hereinafter data center) in "private clouds", defines concept of data center, history of its origin and development. All the disadvantages and advantages of existing data centers compared to local counterparts are analyzed. Issues of information security data centers in "private clouds" and data protection were also considered. Particular attention is paid to the application of this technology in organizations, as well as a basis for development information infrastructure systems. The current problems that arise during operation of the data center are highlighted. Examples of foreign experience successful use data centers in "private clouds" are analyzed. To solve the problems of the Concept, it is necessary to attract human and material resources, and the achievement of expected results depends on a reasonable determination of ways of information technology development – management technologies and data processing using computer technology, as well as organizational and technical integration of human, technical, software, computing and telecommunication resources for the provision of information services (services) in the relevant information infrastructure, taking into account the specifics of the military. With the use of "cloud technology", information consumers can significantly reduce the cost of building data centers, purchasing server and network equipment, hardware and software solutions to ensure continuity and performance, as these costs are absorbed by the cloud service provider. In addition, the long construction and commissioning of large IT facilities and their high initial cost limit the ability of consumers to respond flexibly to market demands, while cloud technology provides the ability to respond almost instantly to increasing demand for computing power.

Keywords: data center, data processing center, databases, servers, private cloud, service, cloud technologies.

Постановка проблеми. Концепцією Національної програми інформатизації [1] визначено, що інформатизація Збройних Сил України є складовою частиною інформатизації держави. Вона включає процеси створення, впровадження і застосування в різних сферах їх діяльності у мирний та воєнний час сучасних методів, систем і засобів одержання, оброблення, зберігання, передавання та використання інформації.

Для вирішення завдань Концепції, необхідне залучення людських і матеріальних ресурсів, а досягнення очікуваних результатів залежить від обґрунтованого визначення шляхів розвитку інформаційних технологій – технологій управління та обробки даних з використанням обчислювальної техніки, а також організаційно-технічного об'єднання людських, технічних, програмних, обчислювальних та телекомунікаційних ресурсів для надання інформаційних послуг (сервісів) у відповідну інформаційну інфраструктуру з врахуванням військової специфіки.

У зв'язку з відносною новизною "хмарних технологій", в питанні доцільності їх впровадження, виникає безліч суперечок і дискусій на тему здатності організовувати єдиний інформаційний простір. Прийняття ефективних рішень, щодо

впровадження розсіяних обчислень, вимагає повного аналізу середовища, для якого планується розгорнути, так звані, робочі столи на "хмарах".

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень показав, що інформаційна безпека організацій постійно посилюються процесами технічних засобів обробки та передачі даних і, перш за все, обчислювальних систем [1; 2]. Про актуальність проблеми свідчать дослідження В. Домарева, І. Конеєва, А. Беляєва, А. Савченко, В. Василенко, О. Колісника, Т. Халявкіної, Б. Корнієнко, Л. Галати та ін. [1–5]. Зокрема у праці А. Савченко, В. Василенко, О. Колісника, Т. Халявкіної [3] розглядаються методи моніторингу та управління інфраструктурою ЦОД, для забезпечення високої надійності та інформаційної безпеки. Вчені Б. Корнієнко та Л. Галата у своїх роботах [4] запропонували метод дослідження математичної моделі системи інформаційної безпеки в комп'ютерній мережі, в тому числі ЦОД. В ній вони оцінили пропускну здатність мережі та її компонентів, визначили "вузькі" місця в структурі обчислювальної системи; порівняно різні варіанти організації мережі, здійснили перспективний прогноз розвитку системи та передбачили майбутні вимоги відносно пропускної здатності мережі.

Однак, у розглянутих дослідженнях невисвітленим лишилось питання забезпечення надійності та оптимізації інфраструктури ЦОД.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на всі теоретичні та практичні дослідження ЦОД у світі, вони досі інтенсивно розвиваються і впроваджуються в багатьох сферах державного сектору. Використання ЦОД у "приватних хмарах" під час створення інформаційної інфраструктури потребує всебічного дослідження шляхів його виконання. Дослідженню перспектив використання ЦОД у "приватних хмарах" для створення інформаційної інфраструктури Міністерства оборони України присвячена дійсна робота.

Мета статті. Метою даного дослідження є аналіз та систематизація теоретичних та практичних аспектів використання ЦОД у "приватних хмарах". Відповідно до поставленої мети, завданнями статті було визначення загальних принципів ЦОД, історії їх зародження та розвитку. Аналіз недоліків і переваг існуючих ЦОД у "приватних хмарах" порівняно з локальними аналогами. Питання інформаційної безпеки ЦОД та захисту даних у приватній хмарі.

Викладення основного матеріалу дослідження. За останні кілька років роль інформаційних систем і технологій суттєво зросла. Впровадження інформаційних систем стало необхідною умовою підвищення мобільності, гнучкості та ефективності системи управління організацією.

Хмарні обчислення (англ. Cloudcomputing) – технологія розподіленої обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс. Суть концепції хмарних обчислень полягає в наданні кінцевим користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів і додатків (включаючи операційні системи і інфраструктури) через Інтернет. Розвиток сфери хостингу було обумовлено виниклою потребою в програмному забезпеченні і цифрових послугах, якими можна було б управляти зсередини, але які були б при цьому більш економічними і ефективними за рахунок економії d масштабі [6].

Одним з основних підходів в основі хмарних технологій стоїть сервіс, до назв варіантів надання послуг прийнято додавати словосполучення "as a service", що в перекладі означає "у вигляді сервісу". SaaS (Software as a service), або програми у вигляді сервісів – варіант, при якому пропонується використовувати конкретне ПО, наприклад, корпоративну систему, у вигляді сервісу з підпискою. [6] Одним з варіантів використання SaaS є "приватна хмара".

Приватна хмара – це пул комп'ютерних ресурсів, що надаються як стандартний набір служб, який визначається, проектується і контролюється конкретним підприємством. Наприклад, банки та урядові установи мають проблеми з безпекою даних, які можуть перешкоджати використанню наявних служб "публічної хмари". Існують такі різновиди "приватних хмар":

– самостійно розміщена приватна хмара забезпечує контроль над архітектурою і операціями, використовуючи наявні інвестиції в персонал і устаткування, забезпечує виділене локальне середовище, яке проектується, розміщується і управляється всередині компанії;

– розміщена приватна хмара – це виділене середовище, яке проєктується всередині компанії, а розміщується і управляється за її межами. У ній поєднуються переваги управління службою та архітектурним проєктом з перевагами аутсорсингу;

– приватна хмара на основі пристрою – це виділене середовище, яке закуповується у постачальника та проєктується їм з орієнтиром на постачальника послуг і ринок функцій і контролем над архітектурою. Це середовище розміщується всередині організації і має внутрішнє або зовнішнє управління. В ньому поєднуються переваги використання попередньо налаштованої архітектури і низькими ризиками при розгортанні, з перевагами внутрішньої системи безпеки і контролю [7].

Історія розвитку дата-центрів починається з величезних комп'ютерних кімнат часів зародження комп'ютерної індустрії. Тоді комп'ютерні системи були складніше в управлінні і вимагали забезпечення особливих умов для роботи. Так як вони займали багато місця і вимагали безлічі проводів для підключення різних компонентів, в комп'ютерних кімнатах стали застосовувати стандартні серверні стійки, фальшполи і кабельні канали (прокладені по стелі або під фальшполом). Крім того, такі системи споживали багато енергії і потребували постійного охолодження, щоб устаткування не перегрівалося. Не менш важливою була безпека – обладнання досить дороге і часто використовувалося для військових потреб. Тому були розроблені основні конструкційні принципи по контролю доступу в серверні.

В наш час проєктування і побудова дата-центрів суворо регламентована стандартами, які встановлюють вимоги для проектування дата-центрів. Але все ж залишилося ще багато невирішених завдань в методах роботи, а також будівництві дата-центрів, які не завдають шкоди навколишньому середовищу.

Серед вимог до Центру обробки даних (ЦОД) можна виділити цілодобовий режим роботи

та моніторингу, високу відмовостійкість, надмірність (резервування), безпеку, контроль параметрів середовища, пожежну безпеку, можливість швидкого розгортання та зміни конфігурації, підключення до територіальних, глобальних мереж або Internet [8; 9].

Дата-центр (від англ. *data center*), або центр (зберігання і) обробки даних (ЦОД/ЦХОД) – це спеціалізована будівля для розміщення (хостингу) серверного і мережевого устаткування і підключення абонентів до каналів мережі Інтернет.

Дата-центр виконує функції обробки, зберігання і розповсюдження інформації, як правило, в інтересах корпоративних клієнтів – він орієнтований на вирішення бізнес-завдань шляхом надання інформаційних послуг. Консолідація обчислювальних ресурсів і засобів зберігання даних в ЦОД дозволяє скоротити сукупну вартість володіння IT-інфраструктурою за рахунок можливості ефективного використання технічних засобів, наприклад, перерозподілу навантажень, а також за рахунок скорочення витрат на адміністрування.

Дата-центри зазвичай розташовані в межах або в безпосередній близькості від вузла зв'язку або точки присутності якого-небудь одного або декількох операторів зв'язку. Основним критерієм оцінки якості роботи будь-якого дата-центру є час доступності сервера (аптайм) [10].

Центр обробки даних (ЦОД) – це комплекс потужних серверів, дискових сховищ і технічних рішень, призначених для автоматизації та безперебійної роботи комерційних процесів.

Якість і надійність – два основних критерії при виборі дата-центру. Якісний ЦОД повинен відповідати наступним вимогам:

– розміщення обладнання повинно бути надійно захищене від впливу навколишнього середовища;

– безперебійне постачання електроенергії;

– якісна система вентилювання повітря і відведення тепла;

– розвинена і багаторівнева система охорони: обгороджена територія, контрольно-пропускна система з доглядом, відеоспостереження, управління доступом;

– обізнані співробітники, які обслуговують інфраструктуру ЦОД і клієнтське обладнання.

Типи ЦОД:

– корпоративні (основні та резервні). Використовуються звичайними та інтернет-компаніями для зберігання власної актуальної інформації, а також забезпечуються функціонуванням віртуальних сервісів;

– комерційні (хостингові). Орієнтовані на зберігання і обробку даних сторонніх користувачів (клієнтів) з метою підвищення ефективності повсякденної економічної діяльності;

– використовуючі технологію Web 2.0.

Принципи роботи ЦОД:

– віртуалізація. Рішення, що дозволяє зменшити кількість використовуваного обладнання, що призводить до економії часу, коштів і площ; необхідних для створення центру обробки даних.

– кластеризация. Установка програмах зв'язків між декількома серверами з метою їх об'єднання для координації роботи та перерозподілу навантажень;

– масштабування. Передбачені можливості збільшення потужності ЦОД за рахунок додавання нових модулів або поступового збільшення продуктивності наявного обладнання;

– резервування. Створення умов для безперебійної роботи ЦОД за допомогою перерозподілу функцій між окремими підсистемами.

Першочерговим завданням дата-центрів є створення сприятливих і захищених умов для доступу конкретної компанії до власних даних і їх закриття від сторонніх користувачів.

Досягнення основної мети забезпечується за допомогою:

– зберігання та аналізу великих обсягів інформації;

– забезпечення безпеки і безвідмовності високотехнологічних систем;

– забезпечення максимальної доступності даних;

– об'єднання окремих складових IT-систем.

Унікальні можливості ЦОД гарантують ефективність і безперебійність роботи будь-якої організації, допомагаючи вирішувати більшість проблем, властивих будь-якому виду бізнесу.

Багатокомпонентні системи забезпечують:

– високу надійність зберігання інформації по цілком обґрунтованої вартості;

– значну економію коштів за рахунок варіативного вибору послуг і можливостей, що особливо актуально при реалізації нових IT-проектів;

– скорочення витрат на оренду приміщень, сервісне обслуговування обладнання та оплату електроенергії;

– створення умов для безперебійної роботи і взаємодії головного офісу і мережі філій;

– можливість організовувати резервний офіс у разі необхідності.

Основний показник роботи ЦОД – відмовостійкість; також важлива вартість експлуатації, показники енергоспоживання і регулювання температурного режиму.

Наприклад, стандарт TIA-942 передбачає чотири рівні надійності дата-центрів:

Рівень 1 (N) – відмови устаткування або проведення ремонтних робіт призводять до зупинки роботи всього дата-центру;

Рівень 2 (N+1) – є невеликий рівень резервування;

Рівень 3 (2N) – є можливість проведення ремонтних робіт (включаючи заміну компонентів системи, додавання і видалення вийшло з ладу) без зупинки роботи дата-центру;

Рівень 4 (2(N+1)) – є можливість проведення будь-яких робіт без зупинки роботи дата-центру.

Чотири рівня надійності також відображені і в стандарті Tier (відповідно Tier I, II, III і IV). Цей стандарт найбільш часто фігурує в сертифікатах Цодов.

IBS DataFort надає замовникам в користування промисловий віртуальний центр обробки даних (ВЦОД), який на відміну від власного дата-центру не потребує витрат на апаратне забезпечення, утримання, обслуговування і модернізацію. Ви отримуєте інфраструктуру як сервіс (IaaS) з можливістю самостійного управління і моніторингу через спеціальний портал.

Рішення включає в себе обчислювальні ресурси, дисковий простір, засоби управління і моніторингу, сервіси інформаційної безпеки і доступу до інфраструктури. Віртуальний ЦОД IBS DataFort може використовуватися як основна або резервна площадка [11].

Переваги сервісу:

Економічна ефективність Відсутність капітальних витрат і оптимізація операційних, оплата за фактично використані ресурси.	*Безпека* Ефективні засоби захисту інформації, цілодобовий моніторинг, швидка реакція на інциденти, захист конфіденційних даних від витоків
Швидке впровадження та модернізація Повністю готовий до роботи сервіс надається протягом одного робочого дня, впровадження нових систем в залежності від складності займає кілька годин	*Безперервність бізнесу* Високий рівень доступності сервісу, безперервність критичних IT-процесів
Збереження даних Фізична безпека в ЦОД Tier III, відмовостійкість на рівні системи зберігання та інших компонентів хмарної інфраструктури	*Надійність і продуктивність* Сучасні промислові рішення провідних світових вендорів: Cisco, Arista, HPE, Pure Storage, VMware, Microsoft, Veeam

Створення дата-центру зазвичай – це виділення окремого відділу в конкретній компанії, якщо відповідні послуги не надаються ззовні на комерційних умовах.

Приміщення, де знаходиться ЦОД має розташовуватися в безпосередній близькості від зовнішніх транспортних і електричних мереж. В обов'язковому порядку дотримуються найжорстокіші нормативи відповідно площі приміщення, електричного навантаження його перекриттів, особливостям електроживлення і кондиціонування.

Склад ЦОД:

– технічні компоненти (серверний комплекс, системи зберігання та резервного копіювання даних, мережева інфраструктура, системи інженерної експлуатації та безпеки дата-центру);

– програмне забезпечення (операційні системи серверів, робочих станцій, програмне забезпечення баз даних, засоби адміністрування серверів і робочих станцій, резервного копіювання, кластеризації і інвентаризації, програми пристроїв зберігання даних, браузери та клієнти електронної пошти);

– організаційне середовище, що забезпечує функціональність процесів, пов'язаних з наданням IT-послуг.

Основні етапи створення ЦОД:

– планування (розробка технічного завдання та плану реалізації);

– узгодження обраної концепції і її адаптація до реальних умов експлуатації дата-центру;

– безпосередня реалізація проекту;

– експлуатація центру обробки даних;

– модернізація дата-центру.

Будівництво безпечного і надійного ЦОД можливо тільки при дотриманні вимог і нормативів, які стосуються характеристик приміщення, де буде розташовуватися обладнання. Від фактичного стану майданчика залежить не тільки належне функціонування ЦОД, а й вартість його облаштування.

Висновки і пропозиції. Отже, при використанні "хмарних технологій" споживачі інформації можуть значно знизити витрати на побудову центрів обробки даних, закупівлю серверного та мережевого обладнання, апаратного і програмного рішення щодо забезпечення безперервності і працездатності, так як ці витрати поглинаються провайдером хмарних послуг. Крім того, тривалий час побудови і введення в експлуатацію великих об'єктів інфраструктури інформаційних технологій і висока їх початкова вартість обмежують здатність споживачів гнучко реагувати на вимоги ринку, тоді як хмарні технології забезпечують можливість практично миттєво реагувати на збільшення попиту на обчислювальні потужності.

В даний час хмарні технології на українському ринку тільки починають розвиватися, але, судячи з динаміки, обіцяють незабаром наздогнати зарубіжних конкурентів. Створення інформаційної інфраструктури Міністерства оборони України без розвитку галузі інформаційних технологій з залученням хмарних моделей та технологій слід приділити значну увагу.

Список літератури:

1. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев, 2004. 992 с.
2. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. СПб., 2003. 354 с.
3. Savchenko A. S., Vasylenko V. A., Kolisnyk O. V., Holiavkina T. V. Computer networks monitoring and management methods. *Наукоємні технології.* 2018. Т. 39. № 3. С. 281–288. DOI: 10.18372/2310-5461.39.13075
4. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. *Наукоємні технології.* 2017. Т. 34. № 2. С. 114–118. DOI: 10.18372/2310-5461.34.11608
5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб. : Питер, 2016. 960 с.
6. Cloud Computing: Global (2010–2015). URL: http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html
7. Монахов Д. Н., Монахов Н. В., Прончев Г. Б., Кузьменков Д. А. Облачные Технологии. Теория и практика : книга. Москва : МАКС Пресс, МГУ, 2013. С. 128.
8. ANSI/TIA-942 STANDART Telecommunications Infrastructure Standard for Data Centers. URL: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf
9. Сюзанн Найлз. Стандартизация и модульность в Адаптивной Инженерной Инфраструктуре Центра обработки данных. Информационная статья № 116. *APC.* URL: https://www.apc.com/salestools/VAVR-626VPD/VAVR-626VPD_R0_RU.pdf

References:

1. Domarev V. V. (2004) Bezopasnost' informatsionnykh tekhnologiy. Sistemnyy podkhod [Information technology security. Systems approach]. Kyiv. (in Russian)
2. Koneyev I. R., Belyayev A. B. (2003) Informatsionnaya bezopasnost' predpriyatiya [Information security of the enterprise]. Sankt-Peterburg. (in Russian)
3. Savchenko A. S., Vasylenko V. A., Kolisnyk O. V., Holiavkina T. V. (2018) Metod monitorynhu ta upravlinnya suchasnymy komp″yuternymy merezhamy [A method of monitoring and managing modern computer networks]. *Naukoyemni tekhnolohiyi (Science-intensive technologies)* (electronic journal), vol. 39, no. 3, pp. 281–288.
4. Korniyenko B. Y., Galata L. P. (2017) Rozrobka i doslidzhennya matematychnoyi modeli systemy informatsiynoyi bezpeky v komp'yuterniy merezhi [Design and research of mathematical model for information security system in computer network]. *Naukoyemni tekhnolohiyi (Science-intensive technologies)* (electronic journal), vol. 34, no. 2, pp. 114–118.
5. Tanenbaum E., Uezeroll D. (2016) Komp'yuternyye seti [Computer networks]. Sankt-Peterburg. (in Russian)
6. Cloud Computing: Global (2010–2015). Available at: http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html
7. Monakhov D. N., Monakhov N. V., Pronchev G. B., Kuz'menkov D. A. (2013) Oblachnyye Tekhnologii. Teoriya i praktika kniga [Cloud Technologies. Theory and Practice book]. Moscow: MAKS Press, MGU.
8. ANSI/TIA-942 STANDART Telecommunications Infrastructure Standard for Data Centers. Available at: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf
9. Syuzann Naylz. Standartizatsiya i modul'nost' v Adaptivnoy Inzhenernoy Infrastrukture Tsentra obrabotki dannykh. Informatsionnaya stat'ya № 116. *ARS*. Available at: https://www.apc.com/salestools/VAVR-626VPD/VAVR-626VPD_R0_RU.pdf