ISSN 2786-4588 (Print)
ISSN 2786-4596 (Online)

Міністерство освіти і науки України
Херсонський державний аграрно-економічний університет

Таврійський науковий вісник

Технічні науки

Випуск 4

Видавничий дім
«Гельветика»
2021

ISSN 2786-4588 (Print)
ISSN 2786-4596 (Online)

Рекомендовано до друку вченою радою Херсонського державного аграрно-економічного університету (протокол № 3 від 03.11.2021 року)

Таврійський науковий вісник. Серія: Технічні науки / Херсонський державний аграрно-економічний університет. Херсон : Видавничий дім «Гельветика», 2021. Вип. 4. 92 с.

Журнал включено до міжнародної наукометричної бази Index Copernicus International (Республіка Польща)
Свідоцтво про державну реєстрацію: Серія КВ № 24810-14750ПР від 31.05.2021 року.

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

УДК 004.056
DOI https://doi.org/10.32851/tnv-tech.2021.4.3

ОСНОВНІ АСПЕКТИ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В УМОВАХ ПАНДЕМІЇ COVID-19

Худік Н.Д. *– старший викладач кафедри менеджменту*
та інформаційних технологій
Херсонського державного аграрно-економічного університету
ORCID ID*: 0000-0002-2310-799X*

У статті розкриваються основні проблеми дистанційної роботи в режимі обмеження, що пов'язані з пандемією COVID-19, з використанням доступних хмарних технологій. Визначені, проаналізовані та систематизовані проблеми кібербезпеки, пов'язані з додатками для дистанційної роботи. Поширившись по всьому світі, пандемія COVID-19 вплинула на глобальне обмеження суспільних зборів усіх типів, включаючи традиційне робоче місце. Сьогодні мільйони компаній стикаються з проблемою управління повністю віддаленою робочою силою за допомогою дистанційної роботи та пов'язаних з нею технологій. COVID-19 та масштабний перехід до віддаленої роботи забезпечили цифровий прорив та величезний культурний зсув у оперативному плані для кожної організації у всьому світі. Багато постачальників технологій уже скоригували свої відповідні інформаційні продукти та послуги, щоб забезпечити глобальне впровадження роботи на відстані. Так само організації у всіх секторах реалізують політику дистанційної роботи для своїх працівників відповідно до цієї тенденції. Технологічні корпорації Microsoft, Facebook, Amazon, Twitter, Google та багато інших оновили керівні принципи для своїх співробітників щодо віддаленої роботи та збалансування продуктивності. Водночас вони зосереджуються на ретельному виправленні потенційних недоліків зв'язку, які раніше існували у їхніх продуктах та послугах. Ризики кібербезпеки, пов'язані з недоліками у віддалених технологіях, не є особливо новими, але оскільки політика соціального дистанціювання через пандемію змушує співробітників працювати більше вдома, позаяк люди шукають нові способи залишатися на зв'язку, хакери у всьому світі також використовують нові підходи до шахрайства та кібератаки проти працівників та нової професійної активності в Інтернеті багатьох компаній. Успішні кібератаки призводять до втрати даних, псування репутації та технологічної апатії; потенційно підривають зусилля щодо стримування поширення COVID-19. Метою дослідження є вирішення завдань, які породжує робота на відстані, включаючи фактори ризику кібербезпеки, технологічну апатію та наслідки кібератак з використанням доступних хмарних технологій.

Ключові слова: *віддалена робота, хмарні технології, кібербезпека, COVID-19, дистанційна робота.*

Khudik N.D. Main aspects of safe use of cloud technologies in a COVID-19 pandemic

The article reveals the main problems of remote operation in the constraint mode associated with the COVID-19 pandemic using available cloud technologies. Identified, analyzed and systematized cybersecurity issues related to remote applications. Spreading around the world, the COVID-19 pandemic has affected global restrictions on public gatherings of all types, including the traditional workplace. Today millions of companies face the challenge of managing a completely remote workforce through remote work and related technologies. COVID-19 and the large-scale transition to teleworking have provided a digital breakthrough and a huge cultural shift in operational terms for every organization around the world. Many technology providers have already adjusted their respective information products and services to enable the global adoption of teleworking. Likewise, organizations across all sectors are implementing telecommuting policies for their employees in line with this trend. Likewise, organizations across all sectors are implementing telecommuting policies for their employees in line with this trend. Tech corporations Microsoft, Facebook, Amazon, Twitter, Google, and many others have updated guidelines for their employees to work remotely and balance productivity. At the same time, they focus on carefully tweaking potential connectivity disadvantages that previously existed in their products and services. Cybersecurity risks posed by weaknesses in remote technologies are not

particularly new, but as social distancing policies due to the pandemic force employees to work more from home and as people seek new ways to stay connected, hackers around the world are also using new ones approaches to fraud and cyberattacks against workers and new professional activities on the Internet of many companies. Successful cyberattacks result in data loss, damage to reputation and technological apathy; potentially undermine efforts to contain the spread of COVID-19. The aim of the study is to address the challenges posed by teleworking, including cybersecurity risk factors, technological apathy, and the consequences of cyber attacks using available cloud technologies.

Key words: *remote work, cloud technologies, cybersecurity, COVID-19, technology corporations.*

Впровадження хмарних обчислень, що дозволяє користувачам віддалено отримувати доступ до сховищ даних, обчислювальних ресурсів та програмних додатків, стало найбільш актуальним у контексті пандемії COVID-19.

Клієнти в хмарі можуть значно скоротити витрати на зберігання та обчислення, використовуючи загальнодоступне мережеве сховище та обчислювальні ресурси. Постачальник послуг повинен об'єднати ресурси для обслуговування широкого кола клієнтів у єдине ціле, щоб забезпечити динамічний та ефективний перерозподіл потужностей між замовниками, а не постійно змінювати попит на ємність.

Різноманітність пристроїв, що використовуються в хмарних обчисленнях, різко знижує витрати на використання обчислювальних ресурсів. Зниження вартості на розподілені обчислення, загальне сховище та сховище кардинально змінює економіку обробки даних та робить хмарні обчислення дуже привабливими для багатьох клієнтів.

Часто не помічається, що власник має невеликий контроль над своєю безпекою під час передачі даних у хмару, а постачальники послуг поступово беруть на себе відповідальність за їхню безпеку.

Основний акцент на інформаційну безпеку у хмарі приділено в роботах таких вітчизняних та зарубіжних дослідників, як: О.В. Олійник, С.В. Бєлай, Є.А. Ісаєв, В.В. Корнілов, C. Brenton, W. Jansen, T. Grance, J. Karhunen, T. Nyman, N. Asokan та інші. Подальші дослідження потребують розробки стратегії хмарної інформаційної безпеки.

Мета роботи – проаналізувати теоретичні та практичні аспекти безпеки віддаленої роботи співробітників із використанням доступних хмарних технологій у контексті пандемії COVID-19.

Робота на відстані – це технологічна практика віддаленої роботи або вдома за рахунок комбінованого використання систем зв'язку, підключених до Інтернету, електронної пошти, телефону та інших онлайн-цифрових програм. Це застосування комп'ютерного програмного забезпечення та високошвидкісних телекомунікаційних систем для дистанційного впровадження комунікації на робочому місці.

Компонент відеоконференцій – це форма віддаленої відеовзаємодії у реальному часі, коли учасники групуються у фіксованому місці, на відміну від індивідуальної участі у традиційній роботі на відстані. Однак інноваційна інтеграція сеансу відеоконференцій як представника одного учасника дистанційної роботи можлива там, де потрібна сегментація великих учасників з різних географічних місць.

Рішення для відеоконференцій можна використовувати для двостороннього спілкування в прямому ефірі з обмеженою взаємодією з аудиторією. Сфера застосування включає віртуальні зустрічі, онлайн-навчання, технічну підтримку, вебінари, ділові конференції, чати, обмін повідомленнями та обмін файлами,

а також багатоканальну сумісну роботу із загальним доступом до певних файлів та документів.

Нинішня хвиля роботи на дистанційному рівні зумовлена вимогами пандемії COVID-19, тому її можна назвати епізодичною або ситуативною, оскільки це не запланований вид роботи, а той, що був викликаний надзвичайною ситуацією. У результаті кожен важливий компонент дистанційної роботи створює унікальну проблему безпеки, яку необхідно або пом'якшити, або ретельно контролювати, щоб мінімізувати ймовірність кібератак хакерами та шахраями в Інтернеті [4].

«Хмара» – це інструмент, який може використовуватися великими та малими компаніями для покращення взаємозв'язку їхньої робочої сили. Переваги використання хмари включають більшу гнучкість зберігання, посилену співпрацю з будь-якої точки світу та підвищену безпеку.

Більшість компаній уже використовують хмарні сервіси у своїй діяльності. Дуже важливо, щоб кожен працівник знав, як користуватися хмарними службами і, що важливіше, як безпечно користуватися хмарними службами. Крім того, компанії повинні розуміти, що у них є варіанти вибору хмарних сервісів.

Три основні типи – це програмне забезпечення як послуга (SaaS), інфраструктура як послуга (IaaS) та платформа як послуга (PaaS), і ці послуги також варіюються залежно від постачальника хмарних послуг. Нині є змога для кожного бізнесу, малого та великого, розглянути можливість використання хмарного сервісу для підвищення ефективності та результативності своєї діяльності.

Перш ніж купувати хмарні послуги, керівники повинні уважно зрозуміти їхні конкретні потреби та знайти хмарний сервіс, який найкраще відповідає цим потребам. Особливо в унікальному віртуальному робочому середовищі COVID-19 попит на хмарні послуги різко зріс: Microsoft повідомила про зростання хмарного попиту на 775% [16].

Компанії, які розміщують ці ресурси, називаються постачальниками хмарних послуг – cloud service providers (CSP). Одними з найбільших постачальників послуг є Amazon Web Services, NetApp та Google Cloud.

Використовуючи CSP, клієнти, по суті, запозичують інфраструктуру для зберігання ресурсів. Це допомагає заощадити на IT-витратах та забезпечує більш швидке масштабування.

Великі та малі компанії можуть скористатися перевагами хмарних технологій, від електронної комерції для підприємств до місцевих кав'ярень. Розглянемо основні переваги хмарних технологій у контексті пандемії COVID-19.

1. Більш конкретні та прості інструменти для спільної роботи.

Тепер, коли дистанційна робота стала нормою, почалося зростання використання інструментів співпраці або продуктивності. У 2021 році люди продовжуватимуть працювати вдома, а інструменти співпраці матимуть вирішальне значення для продуктивності.

Відеоконференції, спільне використання екрана та чати стануть більш інтегрованими. Це полегшить спілкування між командами. Інші досягнення в галузі штучного інтелекту (ШІ), такі як придушення шуму та віртуальне тло, будуть продовжувати вдосконалюватися та застосовуватись ширше.

Інструменти для сумісної роботи також стають усе більш і більш нішевими. Зараз є програми, що спеціально розроблені для команд, починаючи від юридичних і закінчуючи інженерними.

2. Використання штучного інтелекту на робочому місці.

Штучний інтелект охоплює широкий спектр послуг, включаючи чат-боти, служби визначення місцезнаходження та цифрових помічників. Він спрямований на автоматизацію повторюваних завдань, що економить час та гроші.

Його зростання триватиме і цього року, очікується, що до 2024 року дохід на світовому ринку штучного інтелекту перевищить 300 мільярдів доларів.

Оскільки компанії прагнуть оптимізувати та раціоналізувати свій бізнес, ШІ стане ще більш актуальним на робочому місці. Це може бути реалізоване для автоматизації розрахунків заробітної плати, прогнозування бюджетів або покращення дотримання нормативних вимог. Співробітники також зможуть заощадити час на таких речах, як звіти про витрати, рахунки-фактури та аналіз даних.

Завдяки штучному інтелекту компанії зможуть позбутися більшості ручних завдань і замість цього зосередитися на інноваціях. Тому для підприємств з обмеженими ресурсами або обмеженими бюджетами такі технології, як ШІ, матимуть першочергове значення.

3. Хмарне сховище в охороні здоров'я.

Протягом останніх кількох років охорона здоров'я переходить у хмару і продовжиться в 2021 році. Насправді, прогнозується, що глобальний хмарний ринок охорони здоров'я зросте на 25,54 млрд доларів протягом 2020–2024 років.

Оскільки хмарне сховище дозволяє системам охорони здоров'я зберігати дані в Інтернеті, це відкрило двері для телездоров'я. Пацієнти можуть отримати медичну допомогу без відвідування лікарні та пройти багато планових оглядів або онлайн-консультацій.

Згідно з дослідженням компанії Frost & Sullivan, впровадження телездоров'я прискорилося приблизно на два роки через глобальну пандемію [5].

Гнучкість хмарного зберігання також заощадить гроші медичних компаній. Наприклад, оскільки кількість відвідувань пацієнтів у сезон грипу зростає, вони можуть збільшити ємність своїх хмар протягом цього часу. Влітку, коли менше людей хворіє, вони можуть зменшити його.

Це також дозволяє компаніям скорочувати витрати на найновіші оновлення апаратного або програмного забезпечення, оскільки CSP керує всім цим.

4. Переважання граничних обчислень.

Граничне обчислення останніми роками набрало популярності. Це схоже на хмарні обчислення, оскільки воно зберігає дані та інформацію в Інтернеті, але зберігає їх локально (тобто «на межі»). Це наближує сховище даних до використовуваних пристроїв, усуваючи необхідність покладатися на зберігання даних у віддаленому, центральному місці.

Граничні обчислення дуже корисні у віддалених місцях, де мало можливості підключення до централізованого сайту, де зазвичай зберігаються дані. Він також може полегшити будь-які проблеми із затримкою, які впливають на швидкість або продуктивність програм у реальному часі.

Наприклад, перебуваючи в автомобілі з автономним керуванням, замість того, щоб запускати алгоритм через традиційну службу хмарних обчислень, граничні обчислення можуть запускати його локально. Це покращує ефективність і швидкість доставки.

Граничні обчислення використовуються для Інтернет речей (IoT), таких як розпізнавання облич, віддалені дзвінки в двері, розумні вимикачі світла, Bluetooth та системи контролю температури [6].

5. Зростання безсерверних обчислень.

Безсерверні хмарні обчислення – це відносно нова розробка, яка особливо корисна для розробників програмного забезпечення. Замість обслуговування, оновлення та масштабування серверів CSP відповідають за розподіл ресурсів.

Оскільки провайдер хмарних послуг стягує оплату з компанії лише тоді, коли вона виділяє ресурси для доставки фрагмента коду, це може значно скоротити витрати для компаній.

Це звільняє більше часу для співробітників, щоб зосередитися на функціях, орієнтованих на клієнтів, таких як UX та UI, оскільки немає необхідності турбуватися про інфраструктуру. В результаті можемо очікувати, що додаткові інструменти для співпраці з розробниками допоможуть інтернет-групам надалі спростити їхній робочий процес. Ці типи інструментів можна краще використовувати, якщо менше часу проводиться на стороні сервера.

З огляду на те, що безсерверні обчислення більш енергоефективні, економічно ефективні та гнучкі, легко зрозуміти, чому їх популярність буде продовжувати зростати цього року.

6. Поширення віртуальних хмарних робочих столів.

Віртуальні хмарні робочі столи (або робочий стіл як послуга DaaS) доставляють нам робочі станції через хмару. Це означає, що все – від налаштувань комп'ютера до операційних систем – доставляється через Інтернет.

Оскільки дистанційна робота стає нормою, DaaS набуде все більшого значення, оскільки дозволить нам працювати з будь-якого місця та на будь-якому пристрої. За даними Gartner, DaaS буде зростати на 58,8% щорічно до 2023 року.

DaaS також допомагає зменшити витрати, оскільки підприємства можуть усунути необхідність оновлення обладнання та дублювання технологій. Крім того, оскільки це погодинна модель передплати, компанії можуть заздалегідь передбачити витрати та скоригувати свої потреби за запитом.

Наприклад, якщо компанія наймає нових співробітників, їм доведеться розширити свої можливості. З віртуальними робочими столами це можна зробити легко.

Це також безпечно. Автоматично створюється резервне копіювання та зберігається у захищеному центрі обробки даних. Оскільки все централізовано, це набагато безпечніше, ніж зберігати всі дані на окремому пристрої. І їх можна швидко відновити у разі пошкодження.

Хакери демонстративно використовують кризу COVID-19. Фішинг та інші кібератаки зростають, а злочинці використовують тривогу, яку відчувають робітники у сучасних незвичних обставинах. Опитування CNBC також виявило, що більше третини опитаних керівників повідомили про зростання кіберзагроз, пов'язаних з роботою на відстані.

Типові ризики у разі роботи на відстані [13].

Мережеві ризики. Для віддаленого доступу до ресурсів компанії співробітники зазвичай використовують різні комбінації захищених і незахищених, дротових або бездротових мереж, а власне приватних чи загальнодоступних мереж. Це дає безліч варіантів входу для хакерів та кіберзлочинців – компанії просто не можуть захистити кожну мережу, якою користуються співробітники.

Фізичний захист пристроїв. Захист фізичних пристроїв під час віддаленої роботи стає серйозним ризиком і викликом, оскільки втрачений пристрій – особистий чи корпоративний – становить загрозу втрати конфіденційних даних та особистої інформації. Під особливим ризиком перебувають пристрої працівників, які подорожують або працюють поза домом.

Використання персональних пристроїв у комерційних цілях. У цій ситуації є великий ризик того, що особисте використання програмних продуктів та інших ресурсів може дати злочинцям доступ до ресурсів компанії. Як правило, компанії не мають контролю над програмами та програмами, встановленими на персональних пристроях, разом із корпоративними.

Шахрайство орієнтоване на віддалених працівників. Хакери вміють використовувати психологічні особливості людини і можуть тонко маніпулювати працівниками поза колективним офісним середовищем. Під час віддаленої роботи є ризик того, що працівник не зможе скористатися такими простими методами соціальної інженерії, як перевірка підозрілого повідомлення з колегою поблизу.

Хмарна безпека включає технології, елементи управління, процеси та політику, які колективно захищають хмарні системи, дані та інфраструктуру. Це піддомен комп'ютерної безпеки та у більш широкому сенсі інформаційної безпеки [8].

Хмарна безпека є найважливішою вимогою для всіх організацій. Особливо з огляду на останнє дослідження (ISC) 2, згідно з яким 93% організацій помірно або надзвичайно стурбовані безпекою хмар, а кожна четверта організація підтвердила інцидент із безпекою хмар за останні 12 місяців.

Розглянемо шість стратегічних кроків, які може зробити організація для покращення безпеки віддалених працівників.

1. Покращене управління паролями та безпека.

Неефективні або неповні системи управління паролями продовжували заважати бізнесу протягом усього 2020 року. Перехід на роботу на відстань лише посилив цю проблему. У 2021 році потрібно докласти серйозних зусиль для покращення управління паролями. Це має включати шлях єдиного входу (SSO) для кожної програми та послуги, які використовує компанія. Єдиний вхід повинен поєднуватися з багатофакторною автентифікацією, і більша частина ризику кібербезпеки віддалених працівників буде негайно усунена.

2. Підвищення прозорості інфраструктури.

Видимість трафіку даних стає все більш важливою, оскільки віддалені співробітники використовують для свого підключення до Інтернет бізнес-пристрої, які раніше були захищені корпоративною інфраструктурою. Такі інструменти, як виявлення мережі та реагування на неї, є чудовим способом відновити цю видимість. Можливість детального моніторингу та відображення мережевого трафіку між пристроями працівників для роботи з дому (WFH) та корпоративними програмами, даними та послугами в приватних центрах обробки даних або загальнодоступних хмарах може допомогти виявити аномалії трафіку або помилки конфігурації, які призводять до проблем із продуктивністю або кібербезпекою, – пов'язані проблеми.

3. Розгортання обладнання для забезпечення безпеки віддалених працівників корпоративного рівня.

Більшість середніх і великих підприємств уже розгорнули багато засобів безпеки мережі для управління та контролю пристроїв кінцевих точок, які використовуються співробітниками. Брандмауери нового покоління, системи запобігання вторгненням, інструменти мережевого шкідливого програмного забезпечення та автентифікація для доступу до Wi-Fi – це лише кілька прикладів. Але коли все більше і більше співробітників почали працювати вдома, адміністратори IT-безпеки зрозуміли, що їхні спроби керувати та контролювати політику безпеки ускладнюються, коли пристрої більше не захищаються корпоративною мережею. Шлюзи для віддалених працівників, які розширюють функції корпоративної

безпеки в будинках співробітників, можуть допомогти створити єдину політику безпеки та поділити будинок на роботу та некомерційні мережі. Ці пристрої також створюють захищений тунель VPN для віддалених ресурсів. Це позбавляє працівників від необхідності встановлювати та постійно вмикати програмне забезпечення для віддаленого VPN.

4. Віртуальні робочі столи.

Багато компаній переходять від розгортання корпоративних ноутбуків до роботи на відстані і покладаються на віртуальні робочі столи. Хоча інфраструктури віртуальних робочих столів мають багато переваг в управлінні IT, продуктивності та економії, основною причиною переходу підприємств на віртуалізовані робочі столи є запобіганням втраті даних. Віртуальні робочі столи дозволяють кінцевим користувачам запускати бізнес-ОС, що виглядає та працює так, ніби вона локальна для користувача. Фактично потоки на робочий стіл надходять із захищеного приватного центру обробки даних або у разі настільних ПК як постачальників послуг із загальнодоступної хмари. Це запобігає потраплянню чутливих бізнес-даних до віддалених робочих столів, де вони можуть випадково або навмисно просочитися.

5. Нульова довіра.

Швидше за все у 2021 році найпопулярнішим роком для IT-безпеки буде нульова довіра. Однак, на відміну від багатьох інших раніше популярних тенденцій, нульова довіра насправді є законною та ідеальною структурою безпеки для співробітників та цифрових активів як усередині, так і поза корпоративною інфраструктурою. Вам потрібно врахувати ці принципи нульової довіри, щоб визначити, де знаходиться фірма з її інфраструктурою безпеки, і куди їй потрібно рухатися, щоб досягти вражаючих переваг безпеки.

6. Навчання та матеріали з техніки безпеки WFH.

Зараз найкращий час для створення або вдосконалення наявних навчальних матеріалів з безпеки та супутніх матеріалів. Метою тут має бути ознайомлення співробітників з деякими типовими помилками та хибними уявленнями про кібербезпеку, які часто виникають під час віддаленої роботи. Це включає такі теми, як управління паролями, захист корпоративного обладнання, використання авторизованих програм для співпраці, зберігання конфіденційних даних, запобігання тіньовим IT-ризикам та безпечна перевірка ідентичності людей, з якими працюють співробітники.

Бізнес перейшов у хмару завдяки пандемії COVID-19, але зростання довіри до публічних, приватних та гібридних хмар даних відкрило шлях до нових викликів. Хмарні загрози безпеці через неправильно налаштовані заходи безпеки та відсутність моніторингу поступаються місцем більш суворим протоколам безпеки та можливостям тестування безпеки. Зростання впровадження хмарних технологій означає зростання довіри до безпеки інфраструктури [12].

Пріоритетом буде віддалена робота, а разом з цим і вартість потенційного порушення даних. У 2020 році ми дізналися, що навіть епоха соціального фізичного дистанціювання не може уповільнити загрози соціальної інженерії. Кіберзлочинці продовжуватимуть здійснювати атаки соціальної інженерії та намагатимуться використовувати загальноприйняті домашні пристрої, які можна використовувати для компрометації особи та надання доступу до інформаційних ресурсів. Ці атаки в основному стосуватимуться різних форм фішингу, включаючи електронну пошту, голосове спілкування, текстові повідомлення, миттєві повідомлення та навіть сторонні програми. Враховуючи все сказане, ми передбачаємо, що

віддалені працівники будуть домінувати як вектор атаки номер один для експлуатації у 2021 році.

На жаль, виявлення порушень даних займе більше часу через збільшення віддаленої роботи. Зі зростанням кількості атак фішингу та вимагачів більшість компаній вже скомпрометовані – і вони про це не знають. Реальність така, що співробітники користуються споживчим Інтернетом без будь-якого контролю, що, по суті, є шведським столом для кібератак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Worldwide Public Cloud Services Spending Will More Than Double by 2023. USA, Framingham, July 3, 2019. URL: https://www.idc.com/getdoc.jsp?containerId=prUS45340719 (дата звернення: 17.09.2021).

2. Кононюк А.Е. Фундаментальная теория облачных технологий: Общенаучные подходы формирования систем облачных технологий. Киев : Освіта України, 2018 Т. 1. 621 с.

3. Вольська К.О., Дикий А.П. Бухгалтерський облік у «хмарі»: порядок переходу та адаптації інформаційної системи підприємства. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. ЖДТУ, № 2(37), с. 24–29, 2017. DOI: 10.26642/pbo-2017-2(37)-24-29.

4. Хмарні обчислення, Integrity Systems. URL: http://integritysys.com.ua/solutions/pricatecloud-solution. (дата звернення: 17.09.2021).

5. Кононюк А.Е. Фундаментальная теория облачных технологий: Введение в фундаментальную теорию облачных технологий. Киев : Освіта України, 2018 Т. 2. 528 с.

6. Облачные вычисления (Cloud computing). URL: http://www.tadviser.ru/index.php/Статья:Облачные_вычисления_%28Cloud_computing%29. (дата звернення: 17.09.2021).

7. Cloudcomputing. URL:https://en.wikipedia.org/wiki/Cloud_computing#Service_models (дата звернення: 17.09.2021).

8. The NIST Definition of Cloud Computing. URL: https://csrc.nist.gov/publications/detail/sp/800-145/final (дата звернення: 17.09.2021).

9. Fernando Doglio. "Content as a Service: Your Guide to the What, Why, and How" ButterCMS, May 7, 2019. URL: https://buttercms.com/blog/content-as-a-service-your-guide-to-the-what-whyand-how (дата звернення: 17.09.2021).

10. Olson John A. Data as a Service: Are We in the Clouds?. *Journal of Map & Geography Libraries.* 6 (1): 76–78. DOI: 10.1080/15420350903432739.

11. Desktop virtualization. URL: https://en.wikipedia.org/wiki/Desktop_virtualization #Desktop_as_a_service (дата звернення: 17.09.2021).

12. Mike Roberts. "Serverless Architectures", May 22, 2018. URL: https://martinfowler.com/articles/serverless.html#unpacking-faas (дата звернення: 17.09.2021).

13. Antony Ananich. "What is IaaS?", Mar. 2, 2016. URL: https://web.archive.org/web/20160302153830/http://ananich.pro/2016/02/what-is-iaas/ (дата звернення: 17.09.2021).

14. Donovan Jones. "Blackstone Acquires Cloudreach For Access To iPaaS Market", February 21, 2017. URL: https://seekingalpha.com/article/4048008-blackstone-acquires-cloudreach-foraccess-to-ipaas-market (дата звернення: 17.09.2021).

REFERENCES:

1. Worldwide Public Cloud Services Spending Will More Than Double by 2023. USA, Framingham, July 3, 2019. Retrieved from: https://www.idc.com/getdoc.jsp?containerId=prUS45340719.

2. Koniuk, A.E. (2018). Fundamental'naya teoriya oblachnykh tekhnologiy: Obshchenauchnyye podkhody formirovaniya sistem oblachnykh tekhnologiy [Fundamental theory of cloud technologies: General scientific approaches to the formation of systems of cloud technologies]. Kyiv: Osvita Ukrayiny, (Vol. 1) [in Ukrainian].

3. Vol's'ka, K.O. & Dikiy, A.P. (2017). Bukhhalters'kyy oblik u "khmari": poryadok perekhodu ta adaptatsiyi informatsiynoyi systemy pidpryyemstva [Cloud accounting: the order of transition and adaptation of the information system of the enterprise]. *Problemy teoriyi ta metodolohiyi bukhhalters'koho obliku, kontrolyu i analizu – Problems of theory and methodology of accounting, control and analysis*, 2(37), 24–29 [in Ukrainian]. DOI: 10.26642/pbo-2017-2(37)-24-29.

4. Khmarni obchyslennya, Integrity Systems. Retrieved from: http://integritysys.com.ua/solutions/pricatecloud-solution.

5. Koniuk, A.E. (2018). Fundamental'naya teoriya oblachnykh tekhnologiy: Obshchenauchnyye podkhody formirovaniya sistem oblachnykh tekhnologiy [Fundamental theory of cloud technologies: General scientific approaches to the formation of systems of cloud technologies]. Kyiv: Osvita Ukrayiny, (Vol. 2) [in Ukrainian].

6. Oblachnyye vychisleniya [Cloud computing]. Retrieved from: http://www.tadviser.ru/index.php/Статья:Облачные_вычисления_%28Cloud_computing%29.

7. Cloud computing. Retrieved from: https://en.wikipedia.org/wiki/Cloud_computing#Service_models.

8. The NIST Definition of Cloud Computing. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-145/final.

9. Fernando Doglio. "Content as a Service: Your Guide to the What, Why, and How" ButterCMS, May 7, 2019. Retrieved from: https://buttercms.com/blog/content-as-a-service-your-guide-to-the-what-whyand-how.

10. Olson, John A. Data as a Service: Are We in the Clouds? *Journal of Map & Geography Libraries.* 6 (1): 76–78. DOI: 10.1080/15420350903432739.

11. Desktop virtualization. Retrieved from: https://en.wikipedia.org/wiki/Desktop_virtualization #Desktop_as_a_service.

12. Mike Roberts. "Serverless Architectures", May 22, 2018. Retrieved from: https://martinfowler.com/articles/serverless.html#unpacking-faas.

13. Antony Ananich. "What is IaaS?", Mar. 2, 2016. Retrieved from: https://web.archive.org /web/20160302153830/http://ananich.pro/2016/02/what-is-iaas/.

14. Donovan Jones. "Blackstone Acquires Cloudreach For Access To iPaaS Market", February 21, 2017. Retrieved from: https://seekingalpha.com/article/4048008-blackstone-acquires-cloudreach-foraccess-to-ipaas-market.

ЗМІСТ