ЦЕНТР ФІНАНСОВО-ЕКОНОМІЧНИХ НАУКОВИХ ДОСЛІДЖЕНЬ

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE

ФІНАНСОВІ АСПЕКТИ РОЗВИТКУ ДЕРЖАВИ, РЕГІОНІВ ТА СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: ТЕОРІЯ, МЕТОДОЛОГІЯ, ПРАКТИКА

FINANCIAL ASPECTS OF DEVELOPMENT OF THE STATE, REGIONS AND ECONOMIC ENTITIES: THEORY, METHODOLOGY, PRACTICE

Збірник тез доповідей
Book of abstracts

30 березня 2024 р.
March 30, 2024

м. Рівне, Україна
Rivne, Ukraine

ЦЕНТР ФІНАНСОВО-ЕКОНОМІЧНИХ НАУКОВИХ ДОСЛІДЖЕНЬ

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE

ФІНАНСОВІ АСПЕКТИ РОЗВИТКУ ДЕРЖАВИ, РЕГІОНІВ ТА СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: ТЕОРІЯ, МЕТОДОЛОГІЯ, ПРАКТИКА

FINANCIAL ASPECTS OF DEVELOPMENT OF THE STATE, REGIONS AND ECONOMIC ENTITIES: THEORY, METHODOLOGY, PRACTICE

Збірник тез доповідей
Book of abstracts

30 березня 2024 р.
March 30, 2024

м. Рівне, Україна
Rivne, Ukraine

СЕКЦІЯ 6. РОЗВИТОК ПРОДУКТИВНИХ СИЛ І РЕГІОНАЛЬНА ЕКОНОМІКА
SECTION 6. DEVELOPMENT OF PRODUCTIVE FORCES AND REGIONAL ECONOMICS 24

Ванькович Д. В.
ОЦІНКА РЕЗУЛЬТАТИВНОСТІ ФІНАНСОВОЇ ПОЛІТИКИ "ЗЕЛЕНОГО" ІНВЕСТУВАННЯ В УКРАЇНІ 24

СЕКЦІЯ 7. ІННОВАЦІЇ ТА ІНВЕСТИЦІЙНА ДІЯЛЬНІСТЬ
SECTION 7. INNOVATIONS AND INVESTMENT ACTIVITIES 27

Тимошенко О. В.
МЕТОДИЧНИЙ ІНСТРУМЕНТАРІЙ ОЦІНЮВАННЯ ІНВЕСТИЦІЙНОЇ ПРИВАБЛИВОСТІ ГАЛУЗІ 27

СЕКЦІЯ 8. ДЕМОГРАФІЯ, ЕКОНОМІКА ПРАЦІ, СОЦІАЛЬНА ЕКОНОМІКА І ПОЛІТИКА
SECTION 8. DEMOGRAPHY, ECONOMICS OF LABOR, SOCIAL ECONOMICS AND POLICY 29

Підлипна Р. П.
ВПЛИВ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ЧИННИКІВ НА ФІНАНСОВЕ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОГО ЗАХИСТУ В УКРАЇНІ 29

Хандій О. О.
ЯКІСТЬ ТРУДОВОГО ЖИТТЯ В УМОВАХ ВОЄННОГО СТАНУ: ЗМІНИ, ТЕНДЕНЦІЇ, ВИКЛИКИ 31

СЕКЦІЯ 9. ФІНАНСИ, БАНКІВСЬКА СПРАВА, СТРАХУВАННЯ
SECTION 9. FINANCE, BANKING, INSURANCE 34

Галустян Р. О.
ВИКОРИСТАННЯ ЗОВНІШНІХ ФІНАНСОВИХ РЕСУРСІВ В ЕКОНОМІЦІ ДЕРЖАВИ 34

Коломієць Ю. Ю.
СИСТЕМА ОРГАНІЗАЦІЇ УПРАВЛІННЯ КРЕДИТНИМИ РИЗИКАМИ БАНКУ 36

Самошкіна О. А.
ДЕРЖАВНЕ СТИМУЛЮВАННЯ РОЗВИТКУ СТРАХОВОГО ЗАБЕЗПЕЧЕННЯ АГРОПРОМИСЛОВОГО ВИРОБНИЦТВА УКРАЇНИ В УМОВАХ ВОЄННИХ РИЗИКІВ 38

СЕКЦІЯ 10. ЕКОНОМІЧНА КІБЕРНЕТИКА
SECTION 10. ECONOMIC CYBERNETICS 42

Радзіховська Л. М., Скаженюк М. О.
ОСОБЛИВОСТІ РИЗИКІВ, ПОВ'ЯЗАНИХ З ХМАРНИМИ ТЕХНОЛОГІЯМИ 42

СЕКЦІЯ 10
SECTION 10

ЕКОНОМІЧНА КІБЕРНЕТИКА
ECONOMIC CYBERNETICS

УДК УДК 004.7:366.4(043.2)

Радзіховська Л. М.
к. пед. н., доцент
доцент кафедри економічної кібернетики та
інформаційних систем
Вінницький торговельно-економічний інститут ДТЕУ
Скаженюк М. О.
здобувач освітнього ступеня “магістр”
Вінницький торговельно-економічний інститут ДТЕУ

ОСОБЛИВОСТІ РИЗИКІВ, ПОВ'ЯЗАНИХ З ХМАРНИМИ ТЕХНОЛОГІЯМИ

Хмарні технології є моделлю надання IT-послуг, де ресурси (сервери, сховища даних, мережі, програмне забезпечення) надаються через Інтернет, а не локально на комп'ютері користувача.

При використанні хмарної моделі користувач не володіє фізичними серверами або програмним забезпеченням. Постачальник хмарних послуг володіє та обслуговує сервери та програмне забезпечення, а також відповідає за їх безпеку та доступність. Користувач можете отримати доступ до своїх даних та програмного забезпечення через Інтернет, що дає вам можливість працювати з будь-якого фіксованого місця та з будь-якого пристрою.

Хмарні технології – це гнучкий та економічний спосіб отримати доступ до IT-ресурсів. Їх можна використовувати для зберігання даних, розгортання програмного забезпечення, аналізу даних, розробки штучного інтелекту та багато іншого [4].

Хмарні технології революціонізують спосіб, у який ведеться бізнес, обробляються дані та використовується програмне забезпечення. Їхні переваги численні: економія коштів допомагає заощадити гроші на обладнанні, програмному забезпеченні та IT-персоналі, підвищення гнучкості дає можливість швидко та легко масштабувати свої IT-ресурси в міру зростання бізнесу, підвищення безпеки може допомогти захистити дані.

Безпека хмарних даних є комплексом заходів, спрямованих на захист даних, що зберігаються або обробляються в хмарному середовищі. Вона включає в себе: конфіденційність − забезпечення того, що доступ до даних мають лише авторизовані особи, цілісність – гарантування, що дані не були змінені або пошкоджені, доступність – гарантування того, що дані доступні для авторизованих користувачів, коли їм це потрібно [2].

Однак, існують і ризики, пов'язані з безпекою хмарних даних: несанкціонований доступ − зловмисники можуть отримати доступ до даних через вразливості в хмарній інфраструктурі або програмному забезпеченні, втрата даних − дані можуть бути втрачені через людську помилку, технічні збої або стихійні лиха, неналежне використання даних − дані можуть бути використані без вашого відома або згоди.

Для забезпечення безпеки хмарних даних доцільно проводити ряд заходів. зокрема: шифрування даних робить їх нечитабельними для несанкціонованих осіб, контроль доступу − важливо встановити чіткі правила доступу до даних, щоб лише авторизовані користувачі могли їх переглядати, змінювати або видаляти, резервне копіювання − регулярне резервне копіювання даних допоможе відновити їх у разі втрати, моніторинг − важливо постійно моніторити хмарне середовище на наявність ознак несанкціонованої активності, відповідність − важливо переконатися, що ваш постачальник хмарних послуг відповідає всім стандартам безпеки.

Хмарні технології пропонують багато переваг, але також створюють ряд юридичних ризиків, які потребують уважного розгляду. Ось деякі з найважливіших: зберігання та обробка даних в хмарі може призвести до порушення законів про захист даних, таких як GDPR, CCPA та HIPAA, угоди про рівень обслуговування (SLA) з постачальниками хмарних послуг повинні бути чітко сформульовані та охоплювати всі важливі аспекти, такі як доступність, безпека та відповідальність, важливо ретельно вивчити SLA перед його підписанням, додаткові договори, такі як угоди про конфіденційність та нерозголошення інформації, також можуть бути необхідними, важливо чітко визначити, хто несе відповідальність за різні аспекти безпеки та захисту даних в хмарному середовищі, це може бути складно, адже відповідальність може бути розподілена між користувачем, постачальником хмарних послуг та іншими третіми сторонами, важливо мати чіткий план реагування на інциденти, який визначає дії, які слід вжити у випадку порушення безпеки [1].

Важливо також чітко визначити, кому належать права на інтелектуальну власність, пов'язану з хмарними технологіями. Це може включати дані, програмне забезпечення та контент. Потрібно мати чіткі політики та процедури для захисту інтелектуальної власності. Важливо вибрати юрисдикцію, яка має сприятливе законодавство та судову систему, мати можливість вільно переносити дані з однієї хмарної платформи на іншу. Це може бути складно, адже постачальники хмарних послуг можуть використовувати різні формати даних та протоколи. Повинен бути чіткий план міграції даних, який визначає процес переміщення даних [3].

Таким чином, хмарні технології пропонують економність, гнучкість, продуктивність та кращу безпеку. Проте, вони також несуть ряд ризиків: юридичні (договори, відповідальність), безпекові (доступ, втрата даних) та операційні (перебої, залежність). Щоб мінімізувати ризики, потрібно чітко формулювати договори, дбати про безпеку даних, обирати надійного постачальника та мати план міграції даних.

Список літератури

1. Що таке хмарні технології та як вони можуть допомогти вашому підприємству. URL: https://business.diia.gov.ua/cases/tehnologii/so-take-hmarni-tehnologii-i-ak-voni-mozut-dopomogti-vasomu-pidpriemstvu (Дата звеременення 14.03.2024).

2. Що таке хмарні технології: переваги та недоліки хмарних сервісів. URL: https://edin.ua/shho-take-xmarni-texnologiï-i-navishho-voni-potribni/ (Дата звеременення 14.03.2024).

3. Найкращі практики захисту хмарних сховищ. URL: https://rb.gy/h8xumz (Дата звеременення 15.03.2024).

4. Що таке безпека в хмарі. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security (Дата звеременення 15.03.2024).