https://doi.org/10.26565/2311-2379-2026-110-02
УДК 004.77(004.08)

С. В. ЛУБЕНЕЦЬ *
кандидат технічних наук, доцент,
доцент ЗВО кафедри економічної кібернетики та прикладної економіки
ORCID ID: https://orcid.org/0000-0003-1061-8763, e-mail: s.lubenec@karazin.ua
А. М. ШЕЛЕСТОВА *
кандидат наук із соціальних комунікацій, доцент,
доцент ЗВО кафедри економічної кібернетики та прикладної економіки
ORCID ID: https://orcid.org/0000-0003-4866-1767, e-mail: anna.shelestova@karazin.ua
О. Є. ПОМОРЦЕВА *
кандидат технічних наук, доцент,
доцент ЗВО кафедри економічної кібернетики та прикладної економіки
ORCID ID: http://orcid.org/0000-0002-4746-0464, e-mail: olenapomortseva@karazin.ua
В. О. ГУБІН **
старший викладач кафедри штучного інтелекту
ORCID ID: https://orcid.org/0000-0003-1850-1930, e-mail: vadim.gubin@nure.ua

* Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
** Харківський національний університет радіоелектроніки, проспект Науки, 14, Харків, 61166, Україна

КІБЕРНЕТИЧНІ ТА ЕКОНОМІЧНІ АСПЕКТИ ЗНИЖЕННЯ РИЗИКІВ ХМАРНИХ СХОВИЩ У СТРУКТУРІ ІНФОРМАЦІЙНИХ СИСТЕМ

Визначено основні проблемні аспекти щодо ризиків застосування організаціями хмарних сховищ даних у структурі власних корпоративних інформаційних систем, з поєднанням питань технічної безпеки (кібернетичні аспекти), а також фінансової доцільності та витрат на кіберсховища (економічні аспекти). До найбільш важливих проблемних аспектів слід віднести: складнощі з проєктуванням безпечного хмарного сховища; економічні та фінансові аспекти управління витратами на хмарні сервіси; недостатній рівень володіння необхідними навичками та(або) ресурсами для належного проєктування, впровадження, управління та обслуговування хмарного середовища. Для пошуку можливих напрямів зниження ризиків хмарних сховищ досліджено основні та розширені принципи концепції «нульової довіри». Розглянуто питання забезпечення цілісності та конфіденційності даних хмарних сховищ інформаційних систем. Досліджено проблему довговічності як здатності системи хмарного зберігання надійно захищати дані від втрат чи пошкоджень протягом тривалого часу. Визначено сутність суверенітету даних, важливість місцезнаходження хмарних сховищ, а також ключову роль їх продуктивності у мінімізації часу простою корпоративної інформаційної системи та забезпеченні відмовостійкості даних і безперервності бізнесу. Досліджено проблемні економічні фактори у прогнозуванні витрат на хмарні ресурси та визначенні сукупної вартості володіння хмарним сховищем. Вказано на важливість дотримання сумісності застосованої в організації системи хмарного зберігання з раніше впровадженими рішеннями інформаційної безпеки. Сформульовано основні вимоги до сервісів, ресурсів та рішень хмарного зберігання для зниження ризиків та забезпечення радикальної відмовостійкості даних інформаційної системи. Визначено можливі напрямки та перспективи подальших наукових досліджень щодо розглянутої проблематики, пов'язані з використанням систем штучного інтелекту.

Ключові слова: **хмарне сховище даних, ризики хмарного зберігання, корпоративна інформаційна система, ресурси хмарного зберігання, штучний інтелект**.
JEL Classification: L86, C88, D81, O33.

Постановка проблеми. Цифровізація економіки й управління вимагає від компаній та організацій значних зусиль та ресурсів задля забезпечення ефективної цифрової інформаційної безпеки (Лубенець, Харченко, & Павленко, 2023). Надійне та безпечне

зберігання й резервування даних в управлінських інформаційних системах – один із ключових сучасних інструментів кіберзахисту.

Дані – це життєво важливий ресурс для будь-якої організації, і забезпечення їхньої стійкості до різних збоїв має вирішальне значення для безперебійної роботи корпоративної інформаційної системи та, відповідно, для стабільності бізнесу. Проте загрози інформаційній безпеці, людські помилки, пошкодження даних та стихійні лиха продовжують перешкоджати безперервній роботі компаній в різних країнах та регіонах світу (Лубенець, Харченко, & Шедякова, 2024).

Відповідно до звіту про тенденції програм-вимагачів за 2025 рік (Lenovo Data Storage Central, 2026), 96% кібератак тепер цілеспрямовано націлені на резервні копії компаній у спробі запобігти успішному відновленню даних із чистої резервної копії або викрасти конфіденційну інформацію. Тому для забезпечення стійкості даних в інформаційних системах необхідно впроваджувати комплексні та надійні програмні рішення. При цьому критично важливим стає безпечне резервне копіювання даних поза офісом.

Хмарні кіберсховища стали цінним інструментом для забезпечення збереження даних інформаційної системи у разі будь-якої атаки чи сценарію втрати даних. Завдяки типовому розгортанню поза межами офісу, вони захищають дані від стихійних лих, пожеж, повеней або інших подій, які унеможливлюють доступ до центру обробки даних. Вони також дають будь-якій організації значну перевагу в боротьбі з викупниками.

Проте багато організацій не беруть до уваги важливу роль безпечного зберігання резервних копій поза офісом для узгодження своєї стратегії інформаційної безпеки з розширеним правилом 3-2-1-1-0 (Kumar et al., 2025):

- наявність 3-х копій даних, включаючи виробничий набір даних, резервну копію та копію резервної копії;
- наявність 2-х різних типів носіїв (найчастіше це локальні диски та хмарне сховище);
- наявність 1-го віддаленого сховища (найчастіше використовується саме хмарне сховище);
- наявність 1-ї автономної чи незмінної копії даних для зниження інформаційних загроз із боку зловмисників;
- 0 помилок під час виконання стандартного тестування відновлення.

Тут перші три складові 3-2-1 відображають відому стандартну стратегію резервного копіювання, що існувала протягом понад двох останніх десятиліть. Однак, з поширенням використання хмарних технологій та зростанням кіберзагроз, наступні дві складові 1-0 покращили стару стратегію, перетворивши її на новішу та актуальнішу стратегію 3-2-1-1-0.

Незважаючи на розуміння цієї перевіреної та надійної практики, лише 61% організацій у структурі власної корпоративної інформаційної системи використовують хмарне сховище на додаток до резервних копій на дисках. При цьому вони, ймовірно, залишають прогалини у своїй стратегії відмовостійкості, наражаючи на ризик дані та операції.

Однак слід розуміти, що хоча хмарне сховище пропонує рішення для більшості, якщо не для всіх організацій, воно часто пов'язане зі значними проблемами та ризиками. Багато організацій – від найбільших підприємств до малих і середніх компаній – продовжують стикатися з різними проблемами, з яких найважливішими є наступні (Flexera, 2026):

- *економічні та фінансові аспекти управління витратами на хмарні сервіси*: 82% компаній згодні з тим, що повне розуміння та прогнозування всіх пов'язаних із хмарним сховищем витрат, таких як транзакції, доступ до даних та вихідний трафік, є складним завданням, що призводить до несподівано високих рахунків;
- *безпека*: 79% зазнають труднощів із проєктуванням безпечного хмарного сховища корпоративної інформаційної системи, включаючи логічне ізолювання, незмінність, шифрування та багато іншого;
- *ресурси/експертиза*: 78% не мають необхідних навичок та/або ресурсів для належного проєктування, впровадження, управління та обслуговування свого хмарного середовища.

При цьому однією з ключових проблем хмарних технологій є питання ризиків хмарних сховищ даних: виток або пошкодження даних, простої інформаційної системи, комплаєнс тощо (Кулаковська, 2024).

Тому актуальним є дослідження найважливіших кроків щодо зниження ризиків, пов'язаних з хмарними сховищами, для забезпечення відмовостійкості та надійності даних, для вивчення та всебічного розуміння сучасних передових методів, необхідних для забезпечення безперебійної роботи бізнесу, незалежно від проблем інформаційної безпеки.

Аналіз останніх досліджень. Проблеми та актуальні аспекти хмарних сховищ, а також ризиків щодо їх застосування, досліджувалися рядом науковців, аналітиків та профільних фахівців.

Зокрема, в науковій статті (Kumar & Agarwal, 2024) досліджено проблематику розподілених кібератак типу «відмова в обслуговуванні» (DDoS), які є одними з найбільших ризиків для хмарних сховищ даних. Перебої в обслуговуванні, конфлікти ресурсів, нанесення шкоди репутації та фінансові втрати компанії – це лише деякі з багатьох прямих та непрямих наслідків DDoS-атак. Для зниження ризиків та мінімізації наслідків цих атак авторами статті запропоновано методику швидкого обслуговування у хмарному середовищі на основі контейнеризації з розділенням вхідних запитів до даних сховища. Як результат, це забезпечує підтримку до 98% доступності хмарного сервісу під час масованих DDoS-атак.

У статті (Yang, Liu, Ding, & Liang, 2025) досліджуються ризики міграції даних організації у хмарне сховище для підтримки підписання контрактів з постачальниками хмарних сервісів та забезпечення ефективного аудиту цілісності даних. Авторами статті пропонується ефективне та практичне рішення даної проблеми. Зокрема, з використанням публічного блокчейну для розробки справедливого тристороннього протоколу підписання контрактів для міграції даних на аутсорсинг, який може ефективно запобігти зловмисному обману як власників даних, так і хмарних центрів обробки даних. При цьому додатково забезпечується цілісність даних організації під час процесу міграції.

У роботі (Djenna, Belaoued, Lifa, & Moualdi, 2024) проводиться аналіз і прогнозування актуальних інформаційних загроз з боку програм-вимагачів та ризиків їх застосування при організації кібератак на хмарні сховища. Авторами пропонується проактивний підхід до прогнозування атак програм-вимагачів з інтеграцією динамічного алгоритму глибокого навчання для аналізу функцій на основі пам'яті, що дозволяє виявляти наявність індикаторів програм-вимагачів у реальному часі.

У публікації (Wen & Deng, 2024) досліджуються проблематика вразливості аудиту цілісності даних у хмарному сховищі, переданих на аутсорсинг. Адже такі дані часто містять конфіденційну інформацію, що створює ризики розкриття під час обміну даними. Для вирішення цієї проблеми авторами запропоновано ефективну схему аудиту цілісності без сертифікатів для захисту конфіденційної інформації у хмарному сховищі (CIAS-SIP), яка підтримує захист конфіденційної інформації та не вказує блоки даних, які потребують очищення власником даних.

У ряді наукових робіт досліджуються фінансові ризики застосування організаціями хмарних сховищ даних. Так, у статті (Zhong, 2024) запропоновано комплексну систему раннього попередження для забезпечення безпеки даних та контролю фінансових ризиків сенсорної мережі хмарного зберігання даних. Система впроваджує модуль контролю фінансових ризиків, який допомагає користувачам попереджати та керувати фінансовими ризиками шляхом моніторингу й аналізу даних у сенсорній мережі в режимі реального часу. В роботі (Zhong, Zhao, & Dou, 2025) досліджується питання впровадження контролю витрат та побудови гарантійної моделі Financial BPO (Financial Business Process Outsourcing) у середовищі хмарних сервісів. Запропонований авторами метод дозволяє контролювати відповідні витрати на 60%, покращити рівень фінансового управління та ефективність підприємства, а також вчасно уникати ризиків його ринкових операцій.

Деякими науковцями та аналітиками для зниження ризиків використання хмарних сховищ даних розробляються ігрові моделі щодо аналізу безпеки хмарних сервісів та ресурсів. Зокрема, в роботі (Sun, 2021) дослідником запропонована модель гри прогнозування довіри, що складається з супервайзера, постачальника хмарних послуг та користувача. Дана модель дозволяє аналізувати та вирішувати ключові умови для різних учасників для досягнення взаємної довіри та безпрограшних ситуацій у використанні хмарних сховищ.

У той же час існує потреба в подальших дослідженнях, що стосуються розробки й запровадження дієвих інструментів та заходів зі зниження ризиків хмарних сховищ даних, у тому числі в структурі корпоративних інформаційних систем. Адже методи зловмисних дій

щодо кібератак на конфіденційні дані хмарних сховищ з метою їх викрадення чи пошкодження постійно вдосконалюються, що вимагає адекватних ефективних заходів боротьби з ними.

Зокрема, актуальними є питання розробки та аналізу дієвих рекомендацій щодо забезпечення надійного резервного копіювання конфіденційних даних, забезпечення їх цілісності, конфіденційності та довговічності зберігання у хмарних сховищах, а також високої продуктивності резервного копіювання та відновлення даних.

Метою роботи є дослідження актуальних проблем і напрямів зниження ризиків хмарних кіберсховищ даних при їх використанні в структурі корпоративних інформаційних систем.

Відповідно до мети дослідження в роботі були поставлені та вирішувалися наступні основні **завдання**:

- дослідити основні кібернетичні аспекти щодо зниження ризиків застосування хмарних сховищ даних;
- визначити проблемні економічні аспекти щодо фінансової доцільності та прогнозування витрат на хмарні сховища;
- розробити керівні принципи та рекомендації зі зниження ризиків використання хмарних сховищ у структурі корпоративних інформаційних систем;
- дослідити сучасні сервіси та ресурси хмарного зберігання даних;
- визначити перспективи подальших наукових досліджень та розробок щодо проблематики роботи.

Методологія дослідження. У процесі досліджень застосовувалася комплексна методологія, яка поєднує технічний аналіз (кібернетика) та фінансове прогнозування. Структура методологічного апарату дослідження містить такі загальнонаукові методи як огляд та аналіз інформаційних джерел; системний аналіз, що дозволяє розглядати хмарне сховище як складну підсистему у структурі інформаційної системи; аналіз та синтез для вивчення окремих видів ризиків (витік даних, простої хмарного сервісу тощо) та об'єднання їх у загальну модель інформаційних загроз; класифікація для систематизації ризиків хмарних сховищ за джерелами виникнення, а також економічних ризиків за прогнозованістю витрат та масштабами можливих збитків, доцільністю інвестицій у зберігання та захист даних.

Основні результати дослідження. Результати проведених досліджень проблематики хмарних сховищ даних надали можливість визначити наступні основні напрями й кроки зниження ризиків та підвищення ефективності їх застосування в структурі корпоративних інформаційних систем.

Нульова довіра. Першим важливим кроком до зниження ризиків хмарних сховищ є дотримання концепції «нульової довіри» (Zero Trust) (Ren, et al., 2025). Концепція Zero Trust – це система безпеки, яка працює за принципом «нікому не довіряй, перевіряй все». Необхідно явно перевіряти дані, завжди передбачати можливий злом та забезпечувати доступ до даних інформаційної системи з мінімальними привілеями.

Основні та розширені принципи концепції Zero Trust щодо стійкості даних, а також відповідні їм дії для забезпечення інформаційної безпеки, наведено на рис. 1.

Загрози можуть виходити як ззовні, так і зсередини мережі, тому жодному об'єкту – будь то користувач, пристрій або програма – не можна довіряти за умовчанням. Для хмарного сховища концепція «нульової довіри» також вимагає логічного поділу мережі, що передбачає ізоляцію даних і систем таким чином, щоб вони не були доступні безпосередньо ненадійним мережам.

Поділ програмного забезпечення та сховища є ключовим принципом, який відповідає концепції «нульової довіри», гарантуючи, що навіть якщо одна частина мережі буде скомпрометована, критично важливі дані залишаться захищеними. Розміщуючи програмне забезпечення і сховище у різних сегментах мережі та застосовуючи суворий контроль доступу, організації можуть створити віртуальний бар'єр, який захищає критично важливі дані корпоративної інформаційної системи від потенційних загроз.

Крім того, цей поділ забезпечує дотримання принципу «мінімальних привілеїв». Кожен компонент працює незалежно, маючи лише необхідні дозволи на виконання своєї функції. Це означає, що навіть якщо зловмисник отримає доступ до програмного рівня, він не зможе отримати доступ до рівня зберігання даних без проходження додаткових перевірок безпеки і контролю.

Концепція Zero Trust гарантує, що дані залишаться стійкими та доступними навіть за умов складних кібератак, тим самим знижуючи ризики хмарного зберігання для бізнесу.

Рис. 1. Основні та розширені принципи концепції Zero Trust
Fig. 1. Basic and advanced principles of the Zero Trust concept

Джерело: авторська розробка / Source: author's development

Цілісність даних та конфіденційність. Наступний крок щодо зниження ризиків хмарних сховищ у структурі інформаційних систем – це забезпечення цілісності та конфіденційності даних (Wen & Deng, 2024). Для цього критично важливим є незмінність та шифрування всіх даних.

Незмінність запобігає зміні чи видаленню даних сховища, переводячи їх у стан «один раз записано, багато разів прочитано» (write once read many (WORM)) (Anjum, Latif, & Chen, 2025). Зробивши дані незмінними, організації можуть захиститися від випадкових чи зловмисних змін як зсередини, так і ззовні організації, тим самим забезпечуючи надійний та захищений від несанкціонованого доступу запис інформації. Це особливо важливо для дотримання нормативних вимог, а також захисту критично важливих даних інформаційної системи від кіберзагроз.

Ще одним важливим компонентом інформаційної безпеки є шифрування, що є процесом перетворення даних у закодований формат, доступ до якого мають тільки авторизовані користувачі з ключами шифрування. Володіння ключами шифрування гарантує, що доступ до даних сховища мають лише ті, кому вони призначені. Це забезпечує захист від зловмисників, навіть якщо їм вдалося успішно викрасти дані, оскільки вони залишаться нечитаними та захищеними.

Довговічність. У хмарному сховищі довговічність передбачає здатність системи зберігання надійно захищати дані від втрати або пошкодження з часом. У галузі інформаційної безпеки та кіберзахисту надійність зазвичай виражається кількістю дев'яток (Veeam Software, 2026).

Наприклад, 11 дев'яток означає 99,999999999% надійності. Це типовий рівень надійності для триразового копіювання даних організації в одному центрі обробки даних (зоні доступності), що належить або керується хмарним провайдером (рис. 2).

Зміна кількості реплікацій та включених центрів обробки даних змінює кількість дев'яток. Так, для 12-ти дев'яток зазвичай є три копії даних у трьох центрах обробки даних в одному або двох регіонах (див. рис. 2). Чим більше дев'яток, тим більше знижуються ризики використовуваної стратегії хмарного зберігання.

Вкрай важливо адаптувати надійність до рівня неприйняття ризику, який організація готова прийняти. Зокрема, різниця між 11-ма і 12-ма дев'ятками значніша, ніж здається: при 11-ти дев'ятках ризик втрати даних збільшується в 10 разів порівняно з 12-ма.

Зберігання даних та суверенітет. У питанні зниження ризиків хмарних сховищ даних важливим також є їхнє місцезнаходження. Місцезнаходження даних відноситься до географічного розташування, де зберігаються та обробляються дані інформаційної системи. Це важливо для організацій, яким необхідно дотримуватися місцевих правил та політики щодо зберігання даних. Наприклад, певні дані можуть потребувати збереження у певній країні чи регіоні для виконання юридичних вимог. У контексті хмарного зберігання місцезнаходження даних гарантує, що дані зберігаються в певному місці, що може допомогти організаціям дотримуватись вимог відповідності та захищати конфіденційну інформацію.

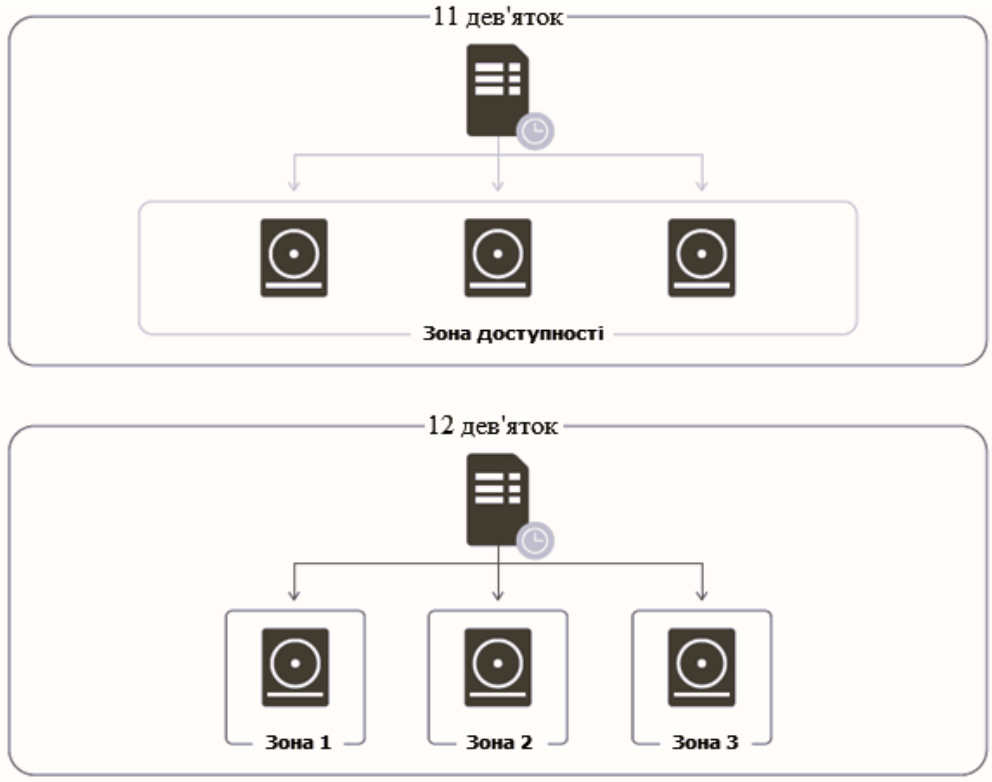

Рис. 2. Триразове копіювання даних організації в одній та трьох зонах доступності
Fig. 2. Triple replication of organization data in one and three availability zones

Джерело: авторська розробка / Source: author's development

Суверенітет даних, з іншого боку, – це юридичне поняття, яке відноситься до юрисдикційного контролю за даними. Це означає, що дані підпорядковуються законам та правилам країни, де вони зберігаються, зокрема для України згідно (Закон України «Про хмарні послуги», 2022).

Місцезнаходження даних та суверенітет мають вирішальне значення для організацій, що працюють у кількох країнах, оскільки їм необхідно забезпечити відповідність їх методів обробки даних законам кожної країни. Суверенітет даних допомагає захистити конфіденційність та безпеку даних, гарантуючи, що вони регулюються відповідною правовою базою.

У цьому контексті для зниження ризиків, пов'язаних із хмарними сховищами, дуже важливо забезпечити глобальне покриття цього сервісу. Окрім відповідності вимогам та конфіденційності, глобальна присутність знижує затримку та максимізує продуктивність інформаційних систем організацій.

Сумісність із існуючими рішеннями IT-безпеки. Для забезпечення відмовостійкості та надійності даних поточні рішення кібербезпеки в компанії повинні безперебійно працювати спільно з її хмарним сховищем даних. Наявність такої сумісності в хмарному сховищі дозволяє різним системам взаємодіяти та обмінюватися даними ефективно щоразу, коли потрібно переміщати, отримувати доступ або керувати корпоративними даними на різних платформах. Цей безперебійний зв'язок спрощує введення в експлуатацію та підвищує відмовостійкість даних інформаційної системи організації. На противагу цьому, ручне налаштування та зв'язування рішень можуть бути складним завданням, що загрожує значною кількістю помилок.

Додатково при забезпеченні сумісності також важливою є безперебійна підтримка клієнтів (Ali, Khan, Nazir, Alarfaj, & Alreshoodi, 2025). Якщо постачальники послуг захисту даних та хмарного сховища не взаємодіють ефективно, один постачальник може вказати на іншого під час вирішення будь-яких проблем із підтримкою. Однак за допомогою єдиного або сумісного рішення щодо захисту інформації такий неефективний та фрагментований процес підтримки можна уникнути.

Продуктивність. При оцінці ризиків хмарного сховища для резервного копіювання поза офісом та досягнення цільових показників рівня обслуговування (Service Level Objectives(SLO)), продуктивність має ключове значення (Qazi, Kwak, Khan, Ali, & Khan, 2024). Продуктивність резервного копіювання та відновлення повинна відповідати цільовим показникам часу відновлення (Recovery Time Objectives (RTO)) і цільовим показникам точки відновлення (Recovery Point Objectives (RPO)). З одного боку, продуктивність резервного копіювання має бути достатньо ефективною, щоб уникнути збоїв у роботі корпоративної інформаційної системи та завершувати копіювання у бажаний проміжок часу. У той же час, продуктивність відновлення повинна забезпечувати швидке відновлення даних для мінімізації часу простою інформаційної системи. Рішення для хмарного зберігання даних має забезпечувати необхідну пропускну здатність та миттєвий доступ, щоб відповідати таким чутливим до часу вимогам.

У питанні продуктивності також важливою є базова мережева інфраструктура інформаційної системи. Незалежно від з'єднань і налаштувань, мережа повинна підтримувати високошвидкісну передачу даних з низькою затримкою як для резервного копіювання, так і для відновлення. Недостатня мережна інфраструктура може призвести до затримок у вікнах резервного копіювання та відновлення, що збільшує ризик невідповідності цільовим показникам SLO.

Таким чином, продуктивність хмарного сховища та мережна інфраструктура корпоративної інформаційної системи, що підтримує його, повинні бути узгоджені, щоб забезпечити відмовостійкість даних і безперервність бізнесу.

Сукупна вартість володіння хмарним сховищем. У зниженні ризиків зберігання даних та забезпеченні їх стійкості не менш важливими є економічні аспекти функціонування та використання хмарних сховищ. Зокрема щодо так званої сукупної вартості володіння хмарним сховищем (total cost of ownership (TCO)) (Everman, Gao, & Zong, 2022).

Багато організацій стикаються з несподіваними витратами на хмарне сховище у структурі своїх інформаційних систем. Адже крім самого сховища існує багато факторів, кожен з яких однаково важливий, і які необхідно враховувати при прогнозуванні витрат на хмарні ресурси.

У своїй основі прогнозувати витрати на хмарне сховище відносно легко, оскільки з організації стягується плата за кожен гігабайт (ГБ) даних, що зберігаються. Далі ціна може сильно варіюватися в залежності від характеру запису та читання даних, частоти доступу до них та мережевих витрат, включаючи міжрегіональні передачі та вихідний трафік. Однак проблема полягає в тому, що існують і додаткові витрати, які чітко задокументовані, але які не так легко прогнозувати. Серед них можна виділити наступне:

1) Вартість дзвінків через програмний інтерфейс API (Application Programming Interface) для запису та читання зазвичай розраховується за 1000 або 10000 транзакцій, що означає, що вона безпосередньо залежить від розміру блоку даних у резервному копіюванні.

Хоча менші розміри блоків забезпечують більше стискання даних та деталізацію відновлення, кількість викликів API при цьому значно збільшується. Оновлення незмінності також призводить до додаткових витрат на транзакції API і залежить від розміру блоку даних.

2) За вилучення даних часто стягується плата за ГБ, і це стосується класів зберігання, оптимізованих для зберігання даних протягом 30 днів і більше. Плата стягується при кожному тестуванні чи відновленні.

Вихідний трафік аналогічний вилученню даних і стягується при кожному відновленні або тестуванні, коли дані залишають мережу хмарного провайдера і потрапляють до локального або альтернативного хмарного середовища організації.

Відновлення даних у тому ж регіоні чи в тій же хмарі зазвичай не тягне за собою таких витрат.

3) Кваліфіковані фахівці з впровадження, управління та обслуговування корпоративної хмарної інфраструктури зберігання даних часто отримують зарплату у шестизначних сумах та вище.

Також варто зазначити, що багато хмарних провайдерів мають різні ціни в різних регіонах, що ще більше ускладнює ситуацію. І це також слід враховувати у TCO.

Таким чином, існує багато кроків, які необхідно зробити для зниження ризиків під час використання хмарного сховища даних у структурі корпоративної інформаційної системи. При цьому та чи інша організація можете самостійно наслідувати описані вище кроки силами власних фахівців з інформаційної безпеки та кіберзахисту. Однак все ж таки правильнішим буде покластися в цьому питанні на компанії, які спеціалізуються на сервісах хмарного зберігання даних.

Розглянемо приклади використання хмарних сервісів зберігання, а також деякі їх особливості, що забезпечують зниження ризиків хмарних сховищ та ефективне відновлення даних після кібератак.

Так, багато хмарних провайдерів, таких як Microsoft Azure, AWS та Google Cloud, виходять за рамки базового розміщення сховища, додатково пропонуючи сотні сервісів з обчислювальними ресурсами та пам'яттю. Ці ресурси стали невід'ємною частиною роботи віртуальних машин у хмарі. Поряд із сервісом хмарного зберігання, близькість обчислювальних ресурсів та сховища є ключовою перевагою при використанні хмарного провайдера з широким спектром пропозицій IaaS (Bushay, 2025), таких як віртуальні машини Azure, Amazon EC2 та Google Cloud Compute Engine.

Повне використання цих переваг дозволяє швидко та безпосередньо відновлювати резервні копії, що зберігаються у хмарі, на хмарні віртуальні машини у рамках стратегії аварійного відновлення (DR). Оскільки ресурси сховища та обчислювальні ресурси знаходяться у безпосередній близькості, час відновлення значно скорочується, що дозволяє організаціям швидко відновлювати критично важливі системи та дані навіть у разі часткової чи повної недоступності локальної інфраструктури. Ця тісна інтеграція гарантує, що організація зможе підтримувати безперервність свого бізнесу, мінімізувати час простою та швидко відновлюватися після збоїв без затримок, притаманних іншим варіантам хмарного резервного копіювання.

Як приклад безпечного хмарного сховища можна також вказати на Veeam Data Cloud Vault (Veeam Software, 2026). Воно є повністю керованим, безпечним ресурсом хмарного сховища на платформі Microsoft Azure. Даний ресурс розроблений відповідно до суворих принципів стійкості даних у рамках концепції «нульової довіри» (Zero Trust Data Resilience (ZTDR)) і гарантує, що корпоративні дані організації завжди будуть захищені від будь-яких несподіванок. Використання цього ресурсу також знижує ризики непередбачуваності моделей ціноутворення у хмарі, що спрощує складання бюджету та прогнозування витрат на хмарне зберігання.

Висновки. Таким чином, результати проведених досліджень та рекомендації щодо їх практичної реалізації можуть сприяти підвищенню ефективності інформаційної безпеки організацій. Використання хмарних сховищ із забезпеченням радикальної відмовостійкості даних дасть можливість організації знизити відповідні ризики, відновлюватися після збоїв, зберігаючи впевненість та контроль над усіма даними корпоративної інформаційної системи. Існуючі послуги, ресурси та рішення хмарного зберігання повинні безперервно вдосконалюватися у створенні інноваційних способів вирішення цих завдань, забезпечуючи відмовостійкість даних, надаючи резервне копіювання, відновлення даних, переносимість даних, безпеку даних, а також аналітику даних. Завдяки використанню сучасних сервісів хмарного зберігання з реалізацією запропонованих у роботі методів зниження ризиків

керівники IT-підрозділів та служб безпеки організацій будуть впевнені в безпеці власних корпоративних інформаційних систем, оскільки їхні програми й дані будуть надійно захищені та завжди доступні у їх хмарних, віртуальних та фізичних середовищах.

Важливим напрямком подальших досліджень щодо розглянутої у статті проблематики є питання застосування систем штучного інтелекту у забезпеченні ефективної інформаційної безпеки та зниженні ризиків застосування хмарних сховищ інформаційних систем (I.T.Pro, 2025). Штучний інтелект може сприяти як вчасному виявленню агресивних кібератак з метою пошкодження чи витоку даних хмарного сховища, так і швидкому реагуванню на відповідні інформаційні загрози (Relea, Samuelb, Patilc, & Krishnan, 2025).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лубенець С. В., Харченко І. М., Павленко Є. П. Актуальні проблеми міжнародної інформаційної безпеки. Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм. 2023. Вип. 17. С. 42–48. https://doi.org/10.26565/2310-9513-2023-17-04

2. Лубенець С. В., Харченко І. М., Шедякова Т. Є. Тенденції, виклики та рішення цифрової інформаційної безпеки в Центральній та Східній Європі. Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм. 2024. Вип. 19. С. 16–24. https://doi.org/10.26565/2310-9513-2024-19-02

3. 2025 Ransomware Trends and Proactive Strategies. Lenovo Data Storage Central. 2026. URL: https://lenovodatastoragecentral.com/reports/2025-ransomware-trends-and-proactive-strategies/

4. Kumar T., Sharma P., Cheng X., Lalar S., Kumar S., & Bansal S. Enhanced triple layered approach for mitigating security risks in cloud. Computers, Materials and Continua. 2025. Vol. 83, № 1. P. 719–738. https://doi.org/10.32604/cmc.2025.060836

5. State of the Cloud Report. Flexera. 2026. URL: https://info.flexera.com/CM-REPORT-State-of-the-Cloud

6. Кулаковська І. Ризики використання хмарних технологій. Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. Т. 341, № 5. С. 45–52. https://doi.org/10.31891/2307-5732-2024-341-5-6

7. Kumar A., Agarwal M. Quick service during DDoS attacks in the container-based cloud environment. Journal of Network and Computer Applications. 2024. Vol. 229. 103946. https://doi.org/10.1016/j.jnca.2024.103946

8. Yang C., Liu Y., Ding Y., & Liang H. Secure data migration from fair contract signing and efficient data integrity auditing in cloud storage. Journal of Network and Computer Applications. 2025. Vol. 239. 104173. https://doi.org/10.1016/j.jnca.2025.104173

9. Djenna A., Belaoued M., Lifa N., & Moualdi D. E. PARCA: Proactive anti-ransomware cybersecurity approach. Procedia Computer Science. 2024. Vol. 238. P. 821–826. https://doi.org/10.1016/j.procs.2024.06.098

10. Wen J., & Deng L. Certificateless integrity auditing scheme for sensitive information protection in cloud storage. Journal of Systems Architecture. 2024. Vol. 156. 103267. https://doi.org/10.1016/j.sysarc.2024.103267

11. Yihui Z. Design of cloud data storage security and financial risk control management early warning system based on sensor networks. Measurement: Sensors. 2024. Vol. 32. 101064. https://doi.org/10.1016/j.measen.2024.101064

12. Zhong W., Zhao L., & Dou Q. The implementation strategy of cost control and the construction of a guarantee model of financial BPO in the cloud computing environment. International Journal of Information System Modeling and Design. 2025. Vol. 16, № 1. 367278. https://doi.org/10.4018/IJISMD.367278

13. Sun P. A trust game model of service cooperation in cloud computing. Journal of Network and Computer Applications. 2021. Vol. 173. 102864. https://doi.org/10.1016/j.jnca.2020.102864

14. Ren Y., Wang Z., Sharma P. K., Alqahtani F., Tolba A., & Wang J. Zero trust networks: evolution and application from concept to practice. Computers, Materials and Continua. 2025. Vol. 82, № 2. P. 1593–1613. https://doi.org/10.32604/cmc.2025.059170

15. Anjum N., Latif Z., Chen H., & Khan S. U. Security and privacy of industrial big data: motivation, opportunities, and challenges. Journal of Network and Computer Applications. 2025. Vol. 237. 104130. https://doi.org/10.1016/j.jnca.2025.104130

16. Veeam Data Cloud Vault. Veeam Software. 2026. URL: https://www.veeam.com/products/veeam-data-cloud/cloud-storage-vault.html

17. Про хмарні послуги: Закон України від 17 лют. 2022 р. № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20

18. Ali T., Khan H. U., Nazir B., Alarfaj F. K., & Alreshoodi M. Optimizing service level agreement in cloud computing with smart virtual machine scheduling using clustered differential evolution and deep learning. Journal of Network and Computer Applications. 2025. Vol. 244. 104361. https://doi.org/10.1016/j.jnca.2025.104361

19. Qazi F., Kwak D., Khan F. G., Ali F., & Khan S. U. Service level agreement in cloud computing: taxonomy, prospects, and challenges. Internet of Things. 2024. Vol. 25. 101126. https://doi.org/10.1016/j.iot.2024.101126

20. Everman B., Gao M., & Zong Z. Evaluating and reducing cloud waste and cost — a data-driven case study from Azure workloads. Sustainable Computing: Informatics and Systems. 2022. Vol. 35. 100708. https://doi.org/10.1016/j.suscom.2022.100708

21. Bushay K. D. Infrastructure as a service / platform as a service. Encyclopedia of Libraries, Librarianship, and Information Science. 2025. Vol. 1. P. 627–639. https://doi.org/10.1016/B978-0-323-95689-5.00109-7

22. Veeam завершив придбання Securiti AI для створення платформи впровадження безпечного ШІ в масштабах підприємства. I.T.Pro. 2025. URL: https://itpro.ua/post/veeam_zavershiv_pridbannya_securiti_ai_dlya_stvorennya_platformi_vprovadzhennya_bezpechnogo_ii_v_masshtabakh_pidpriiemstva/

23. Relea M., Samuel J., Patil D., & Krishnan U. Exploring ransomware detection based on artificial intelligence and machine learning. Procedia Computer Science. 2025. Vol. 252. P. 548–556. https://doi.org/10.1016/j.procs.2025.01.014

Конфлікт інтересів: автори повідомляють про відсутність конфлікту інтересів.

Стаття надійшла до редакції 23.02.2026
Стаття рекомендована до друку 10.04.2026
Стаття опублікована 25.05.2026

REFERENCES

1. Lubenets, S., Harchenko, I., & Pavlenko, Y. (2023). Current problems of international information security. The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism, 17, 42–48. https://doi.org/10.26565/2310-9513-2023-17-04 (in Ukrainian)

2. Lubenets, S., Harchenko, I., & Shediakova, T. (2024). Trends, challenges and solutions of digital information security in Central and Eastern Europe. The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism, 19, 16–24. https://doi.org/10.26565/2310-9513-2024-19-02 (in Ukrainian)

3. Lenovo Data Storage Central. (2026). 2025 ransomware trends and proactive strategies. Retrieved from https://lenovodatastoragecentral.com/reports/2025-ransomware-trends-and-proactive-strategies/

4. Kumar, T., Sharma, P., Cheng, X., Lalar, S., Kumar, S., & Bansal, S. (2025). Enhanced triple layered approach for mitigating security risks in cloud. Computers, Materials and Continua, 83(1), 719–738. https://doi.org/10.32604/cmc.2025.060836

5. Flexera. (2026). State of the cloud report. Retrieved from https://info.flexera.com/CM-REPORT-State-of-the-Cloud

6. Kulakovska, I. (2024). Risks of using cloud technologies. Вісник Хмельницького національного університету. Серія: Технічні науки, 341(5), 45–52. https://doi.org/10.31891/2307-5732-2024-341-5-6 (in Ukrainian)

7. Kumar, A., & Agarwal, M. (2024). Quick service during DDoS attacks in the container-based cloud environment. Journal of Network and Computer Applications, 229, 103946. https://doi.org/10.1016/j.jnca.2024.103946

8. Yang, C., Liu, Y., Ding, Y., & Liang, H. (2025). Secure data migration from fair contract signing and efficient data integrity auditing in cloud storage. Journal of Network and Computer Applications, 239, 104173. https://doi.org/10.1016/j.jnca.2025.104173
9. Djenna, A., Belaoued, M., Lifa, N., & Moualdi, D. E. (2024). PARCA: Proactive anti-ransomware cybersecurity approach. Procedia Computer Science, 238, 821–826. https://doi.org/10.1016/j.procs.2024.06.098
10. Wen, J., & Deng, L. (2024). Certificateless integrity auditing scheme for sensitive information protection in cloud storage. Journal of Systems Architecture, 156, 103267. https://doi.org/10.1016/j.sysarc.2024.103267
11. Yihui, Z. (2024). Design of cloud data storage security and financial risk control management early warning system based on sensor networks. Measurement: Sensors, 32, 101064. https://doi.org/10.1016/j.measen.2024.101064
12. Zhong, W., Zhao, L., & Dou, Q. (2025). The implementation strategy of cost control and the construction of a guarantee model of financial BPO in the cloud computing environment. International Journal of Information System Modeling and Design, 16(1), 367278. https://doi.org/10.4018/IJISMD.367278
13. Sun, P. (2021). A trust game model of service cooperation in cloud computing. Journal of Network and Computer Applications, 173, 102864. https://doi.org/10.1016/j.jnca.2020.102864
14. Ren, Y., Wang, Z., Sharma, P. K., Alqahtani, F., Tolba, A., & Wang, J. (2025). Zero trust networks: Evolution and application from concept to practice. Computers, Materials and Continua, 82(2), 1593–1613. https://doi.org/10.32604/cmc.2025.059170
15. Anjum, N., Latif, Z., Chen, H., & Khan, S. U. (2025). Security and privacy of industrial big data: Motivation, opportunities, and challenges. Journal of Network and Computer Applications, 237, 104130. https://doi.org/10.1016/j.jnca.2025.104130
16. Veeam Software. (2026). Veeam data cloud vault. Retrieved from https://www.veeam.com/products/veeam-data-cloud/cloud-storage-vault.html
17. Law of Ukraine «On Cloud Services» № 2075-IX (2022, February 17). Retrieved from https://zakon.rada.gov.ua/laws/show/2075-20 (in Ukrainian)
18. Ali, T., Khan, H. U., Nazir, B., Alarfaj, F. K., & Alreshoodi, M. (2025). Optimizing service level agreement in cloud computing with smart virtual machine scheduling using clustered differential evolution and deep learning. Journal of Network and Computer Applications, 244, 104361. https://doi.org/10.1016/j.jnca.2025.104361
19. Qazi, F., Kwak, D., Khan, F. G., Ali, F., & Khan, S. U. (2024). Service level agreement in cloud computing: Taxonomy, prospects, and challenges. Internet of Things, 25, 101126. https://doi.org/10.1016/j.iot.2024.101126
20. Everman, B., Gao, M., & Zong, Z. (2022). Evaluating and reducing cloud waste and cost—A data-driven case study from Azure workloads. Sustainable Computing: Informatics and Systems, 35, 100708. https://doi.org/10.1016/j.suscom.2022.100708
21. Bushay, K. D. (2025). Infrastructure as a Service/Platform as a Service. Encyclopedia of Libraries, Librarianship, and Information Science, 1, 627–639. https://doi.org/10.1016/B978-0-323-95689-5.00109-7
22. I.T.Pro. (2025). Veeam Completes Acquisition of Securiti AI to Create Enterprise-Wide Platform for Secure AI Deployment. Retrieved from https://itpro.ua/post/veeam_zavershiv_pridbannya_securiti_ai_dlya_stvorennya_platformi_vprovadzhennya_bezpechnogo_ii_v_masshtabakh_pidpriiemstva/ (in Ukrainian)
23. Relea, M., Samuel, J., Patil, D., & Krishnan, U. (2025). Exploring ransomware detection based on artificial intelligence and machine learning. Procedia Computer Science, 252, 548–556. https://doi.org/10.1016/j.procs.2025.01.014

Conflict of Interest: the authors declare no conflict of interest.

The article was received by the editors 23.02.2026
The article is recommended for printing 10.04.2026
The article was published on 25.05.2026

S. LUBENETS*, PhD (Technical Sciences), Associate Professor, Associate Professor of the Department of Economic Cybernetics and Applied Economics, https://orcid.org/0000-0003-1061-8763, s.lubenec@karazin.ua
A. SHELESTOVA*, PhD in Social Communication Studies, Associate Professor, Associate Professor of the Department of Economic Cybernetics and Applied Economics,
https://orcid.org/0000-0003-4866-1767, anna.shelestova@karazin.ua
O. POMORTSEVA*, PhD (Technical Sciences), Associate Professor, Associate Professor of the Department of Economic Cybernetics and Applied Economics,
http://orcid.org/0000-0002-4746-0464, olenapomortseva@karazin.ua,
V. HUBIN**, Senior lecturer of Artificial Intelligence Department,
https://orcid.org/0000-0003-1850-1930, vadim.gubin@nure.ua

* V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
** Kharkiv National University of Radio Electronics, 14 Nauky Ave., Kharkiv, 61166, Ukraine

CYBERNETIC AND ECONOMIC ASPECTS OF REDUCING THE RISKS OF CLOUD STORAGES IN THE STRUCTURE OF INFORMATION SYSTEMS

The article identifies key problematic aspects of the risks associated with the use of cloud data storage by organizations within the structure of their own corporate information systems, combining issues of technical security (cyber aspects), as well as financial feasibility and costs of cyber storage (economic aspects). The most important problematic aspects include: difficulties in designing a secure cloud storage; economic and financial aspects of managing costs of cloud services; insufficient level of proficiency in the necessary skills and / or resources for the proper design, implementation, management and maintenance of a cloud environment. To identify possible areas for mitigating the risks of cloud storage, the basic and extended principles of the "zero trust" concept are studied. Issues of ensuring the integrity and confidentiality of data in cloud storage of information systems are considered. The problem of durability as the ability of a cloud storage system to reliably protect data from loss or damage over a long period of time is studied. The essence of data sovereignty, the importance of the location of cloud storage, and the key role of their performance in minimizing the downtime of a corporate information system and ensuring data fault tolerance and business continuity are determined. The article examines the economic factors that contribute to forecasting cloud resource costs and determining the total cost of ownership for cloud storage. It also highlights the importance of ensuring compatibility between an organization's cloud storage system and previously implemented information security solutions. Key requirements for cloud storage services, resources, and solutions are formulated to mitigate risks and ensure the radical resilience of information system data. Potential areas and prospects for further research on this topic, related to the use of artificial intelligence systems, are identified.

Keywords: **cloud data storage, cloud storage risks, enterprise information system, cloud storage resources, artificial intelligence**.

JEL Classification: L86, C88, D81, O33.

Як цитувати: Лубенець С.В., Шелестова А.М., Поморцева О.Є., & Губін В.О. Кібернетичні та економічні аспекти зниження ризиків хмарних сховищ у структурі інформаційних систем. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Економічна»*. 2026. Вип. 110. С. 24–35. https://doi.org/10.26565/2311-2379-2026-110-02

In cites: Lubenets S., Shelestova A., Pomortseva O., & Hubin V. (2026). Cybernetic and economic aspects of reducing the risks of cloud storages in the structure of information systems. *Bulletin of V. N. Karazin Kharkiv National University. Economic Series*, (110), 24–35. https://doi.org/10.26565/2311-2379-2026-110-02 (in Ukrainian)