АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Облік і оподаткування

УДК 004.056:657.1:004.738.5

DOI https://doi.org/10.5281/zenodo.19478268

Оцінка ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ

Іванова Наталія Анатоліївна,
кандидат економічних наук, доцент, доцент кафедри обліку і оподаткування, Уманський національний університет, м. Умань, Черкаська Україна, https://orcid.org/0000-0001-8714-9171

Яцко Максим Вікторович,
кандидат економічних наук, доцент, доцент кафедри обліку і аудиту, Державний вищий навчальний заклад «Ужгородський національний університет», м. Ужгород, Україна, https://orcid.org/0000-0003-1145-5302

Дерев'янко Світлана Іванівна,
кандидат економічних наук, доцент, доцент кафедри обліку та оподаткування, Національний університет біоресурсів і природокористування України, м. Київ, Україна, https://orcid.org/0000-0001-8576-0276

Прийнято: 18.03.2026 | Опубліковано: 30.03.2026

Анотація: Актуальність дослідження зумовлено стрімкою цифровізацією облікових процесів, поширенням хмарних облікових платформ та зростанням кіберзагроз, що підвищують вимоги до надійності внутрішнього

контролю і захисту фінансових даних. Встановлено, що традиційні підходи до контролю не забезпечують належного рівня безпеки в умовах розподіленої IT-інфраструктури.

Метою статті є підвищення ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ шляхом обґрунтування та розроблення підходів до її оцінювання і вдосконалення в умовах цифрової трансформації обліку та посилення кіберризиків.

Методи дослідження. У процесі дослідження використано методи системного аналізу, узагальнення і порівняння наукових підходів, аналітичні методи оцінювання ефективності контрольних систем, а також методи логічного моделювання для формування критеріїв і показників кібербезпеки.

Результати. Досліджено сучасні підходи до організації внутрішнього контролю кібербезпеки в умовах хмарних технологій та встановлено їх інтегрований характер. Виявлено специфіку функціонування хмарних облікових платформ і доведено їх вплив на трансформацію контрольних механізмів. Обґрунтовано систему критеріїв і показників оцінювання ефективності внутрішнього контролю. Виявлено ключові науково-практичні проблеми, зокрема невизначеність розподілу відповідальності, обмежену прозорість процесів, складність управління доступом та недостатню адаптивність контрольних систем.

Висновки. Доведено доцільність формування інтегрованої системи внутрішнього контролю кібербезпеки, що поєднує ризик-орієнтовані, технологічні та аналітичні інструменти. Встановлено, що її впровадження забезпечує підвищення надійності облікових даних, зниження кіберризиків і стабільність функціонування облікових платформ.

Перспективи подальших досліджень пов’язані з розробленням формалізованих моделей оцінювання ефективності внутрішнього контролю, інтеграцією технологій штучного інтелекту у системи кібербезпеки та стандартизацією підходів до аудиту хмарних облікових систем.

 ISSN 3041-2129

Ключові слова: цифровізація обліку, кіберризики, управління доступом, захист даних, хмарні технології, інформаційна безпека, автоматизований моніторинг, аудит IT-систем.

Assessment of the effectiveness of the internal control system for cybersecurity of cloud-based accounting platforms

Nataliia Ivanova,
Candidate of Economic Sciences (PhD), Associate Professor,
Associate Professor at the Department of Accounting and Taxation, Uman National University, Uman, Ukraine, https://orcid.org/0000-0001-8714-9171

Maksym Yatsko,
Candidate of Economic Sciences (PhD), Associate Professor,
Associate Professor at the Department of Accounting and Auditing, State Higher Educational Institution “Uzhhorod National University”, Uzhhorod, Ukraine,
https://orcid.org/0000-0003-1145-5302

Svitlana Derevianko,
Candidate of Economic Sciences (PhD), Associate Professor,
Associate Professor at the Department of Accounting and Taxation, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine,
https://orcid.org/0000-0001-8576-0276

Abstract: Relevance of the study is determined by the rapid digitalization of accounting processes, the widespread adoption of cloud-based accounting platforms, and the growing level of cybersecurity threats, which significantly increase the requirements for the reliability of internal control and protection of financial data. It

has been established that traditional control approaches are insufficient to ensure an adequate level of security in a distributed IT environment.

The purpose of the article is to enhance the effectiveness of the internal control system for cybersecurity of cloud-based accounting platforms through the substantiation and development of approaches to its assessment and improvement under conditions of digital transformation of accounting processes and increasing cyber risks.

Research methods. The study employs methods of system analysis, generalization and comparison of scientific approaches, analytical methods for evaluating the effectiveness of control systems, as well as logical modeling methods for developing criteria and indicators of cybersecurity.

Results. Modern approaches to organizing internal cybersecurity control in cloud environments have been studied, and their integrated nature has been established. The specific features of cloud-based accounting platforms have been identified, and their impact on the transformation of control mechanisms has been proven. A system of criteria and indicators for evaluating the effectiveness of internal control has been substantiated. Key scientific and practical problems have been identified, including unclear distribution of responsibilities, limited transparency of processes, complexity of access management, and insufficient adaptability of control systems.

Conclusions. The expediency of forming an integrated internal cybersecurity control system combining risk-oriented, technological, and analytical tools has been proven. It has been established that its implementation ensures higher reliability of accounting data, reduction of cyber risks, and stability of accounting platforms.

Prospects for further research are related to the development of formalized models for evaluating the effectiveness of internal control, integration of artificial intelligence technologies into cybersecurity systems, and standardization of approaches to auditing cloud-based accounting platforms.

 ISSN 3041-2129

Keywords: accounting digitalization, cyber risks, access management, data protection, cloud technologies, information security, automated monitoring, IT audit.

Постановка проблеми. Стрімке поширення хмарних облікових платформ у діяльності підприємств зумовлює суттєву трансформацію підходів до організації внутрішнього контролю, що пов'язано зі зміною архітектури зберігання та обробки фінансових даних, підвищенням рівня їх доступності та одночасним зростанням кіберризиків. У таких умовах традиційні механізми контролю, орієнтовані на локальні інформаційні системи, виявляються недостатніми для забезпечення належного рівня захисту облікової інформації, що підвищує ймовірність несанкціонованого доступу, витоку даних, їх спотворення або втрати. Особливої актуальності набуває проблема оцінювання ефективності систем внутрішнього контролю кібербезпеки, оскільки саме від якості цих систем залежить достовірність фінансової звітності, стабільність бізнес-процесів та рівень довіри з боку стейкхолдерів.

Водночас у науковому середовищі спостерігається фрагментарність підходів до визначення критеріїв та індикаторів ефективності внутрішнього контролю в умовах використання хмарних технологій, що ускладнює формування цілісної методологічної бази для їх оцінювання. Практичні труднощі пов'язані з розмежуванням відповідальності між користувачем і провайдером хмарних сервісів, динамічністю кіберзагроз, а також необхідністю інтеграції технічних, організаційних і управлінських компонентів контролю в єдину систему. У результаті підприємства часто функціонують за умов невизначеності щодо реального рівня захищеності своїх облікових систем, що створює додаткові ризики для фінансово-господарської діяльності. Таким чином, проблема оцінки ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ має міждисциплінарний характер і безпосередньо пов'язана з вирішенням

важливих наукових завдань щодо розроблення адекватних моделей контролю, адаптованих до цифрового середовища, а також практичних завдань підвищення рівня інформаційної безпеки, забезпечення надійності облікових даних і мінімізації кіберризиків у діяльності сучасних підприємств.

Аналіз останніх досліджень і публікацій. Огляд сучасних досліджень дає підстави виокремити чотири взаємопов'язані наукові напрями. Перший напрям пов'язаний із дослідженням технологічної архітектури та інфраструктурних рішень, що формують основу функціонування хмарних платформ і визначають можливості побудови ефективного внутрішнього контролю. У праці Й. Боровскова (Y. Borovskova) обґрунтовано ефективність використання DynamoDB та adaptive polling для оброблення довготривалих HTTP-запитів, що забезпечує стабільність оброблення даних і керованість сервісних процесів [1]. І. Р. Опірський та співавтори досліджують технічні аспекти шифрування даних на носіях, акцентуючи увагу на захисті інформації на рівні зберігання [2]. Ю. Бершчанський (Y. Bershchanskyi) та співавтори аналізують контейнеризовані системи штучного інтелекту, підкреслюючи значення ізоляції сервісів і масштабованості архітектури [3]. Л. Каптосв (L. Kaptosv) розглядає використання Redis для оптимізації кешування, що підвищує продуктивність і контрольованість оброблення даних у хмарному середовищі [4].

Другий напрям охоплює дослідження кібербезпеки хмарних сервісів як середовища функціонування облікових платформ і формування контрольного середовища. Т. Смірнова та співавтори досліджують технології забезпечення кібербезпеки хмарних сервісів різних моделей, акцентуючи на необхідності багаторівневого захисту [5]. Я. В. Шеверя та співавтори розглядають впровадження хмарних технологій у бухгалтерський облік, підкреслюючи зростання вимог до захисту даних і контролю доступу [6]. В. С. Івкова та Р. І. Банах пропонують методологію оцінювання захищеності хмарних технологій за допомогою інструментів відкритих джерел розвідки (Open Source

Intelligence, OSINT), що дозволяє виявляти зовнішні вразливості [7]. І. Аверічев та співавтори обґрунтовують інноваційні підходи до підвищення рівня кібербезпеки корпоративних мереж у хмарному середовищі [8].

Третій напрям стосується цифрової трансформації бухгалтерського обліку та організації облікових процесів у хмарному середовищі, що безпосередньо впливає на систему внутрішнього контролю кібербезпеки. Н. Лобода та співавтори досліджують інноваційні цифрові технології в обліку, звітності та аудиті, підкреслюючи зміну логіки контрольних процедур [9]. І. Санусі (I. Sanusi) та співавтори аналізують хмарні обчислення у безпеці облікових інформаційних систем, доводячи необхідність поєднання ефективності та захисту [10]. А. Гаурав (A. Gaurav) та М. Т. Амбар (M. T. Ambar) розглядають ефективність хмарних облікових систем у контексті фінансової звітності [11]. А. Атадога (A. Atadoga) та співавтори оцінюють вплив хмарних технологій на діяльність бухгалтерських фірм з позицій ефективності та безпеки [12].

Четвертий напрям охоплює дослідження ризиків хмарного обліку, ролі людського чинника, внутрішнього аудиту та кіберуправління у забезпеченні ефективності контролю. А. Е. Анаеге (A. E. Anaege) та співавтори досліджують кіберзагрози у хмарному обліку, акцентуючи на практичних вразливостях [13]. Х. Алкуда (H. Alqudah) та співавтори доводять, що ефективність внутрішнього аудиту залежить від рівня цифрової компетентності персоналу [14]. О. А. М. Алі (O. A. M. Ali) та співавтори аналізують вплив кіберуправління на зниження ризиків хмарного обліку [15].

Виділення невирішених раніше частин загальної проблеми. Попри розвиток досліджень у сфері кібербезпеки та внутрішнього контролю, їх інтеграція в умовах хмарних облікових платформ залишається недостатньо опрацьованою. Існуючі підходи здебільшого фокусуються на окремих аспектах без урахування специфіки хмарного середовища, зокрема розподіленої відповідальності, інтеграції через інтерфейс програмування

застосунків (Application Programming Interface, API) та динамічності кіберзагроз.

Недостатньо розробленими залишаються підходи до оцінювання ефективності внутрішнього контролю, його адаптивності та прозорості, що ускладнює забезпечення надійності облікової інформації. Це зумовлює необхідність поглиблення методичних засад оцінювання та їх адаптації до умов хмарного середовища.

Формулювання цілей статті (постановка завдання). Метою статті є підвищення ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ на основі розроблення та обґрунтування підходів до її оцінювання і удосконалення в умовах цифровізації облікових процесів і зростання кіберзагроз.

Завдання статті:

1. Проаналізувати сучасні підходи до організації внутрішнього контролю кібербезпеки та специфіку функціонування хмарних облікових платформ у контексті управління кіберризиками.

2. Обґрунтувати критерії та показники оцінювання ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ.

3. Виявити науково-практичні проблеми та розробити рекомендації щодо підвищення ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ з урахуванням сучасних викликів цифрового середовища.

Виклад основного матеріалу дослідження. Сучасні підходи до організації внутрішнього контролю кібербезпеки в умовах використання хмарних облікових платформ формуються під впливом цифровізації обліку, розподіленої інфраструктури інформаційних технологій (IT) та зростання кіберзагроз. Делегування частини функцій хмарним провайдерам зумовлює необхідність перегляду контрольних механізмів, зокрема щодо розмежування відповідальності, забезпечення цілісності даних і безперервності доступу. У

цих умовах внутрішній контроль набуває інтегрованого характеру, поєднуючи ризик-орієнтовані, процесні та технологічні інструменти (табл. 1).

Таблиця 1

Сучасні підходи до організації внутрішнього контролю кібербезпеки хмарних облікових платформ

Підхід	Основний зміст	Практичне значення
Ризик-орієнтований підхід	Ідентифікація, оцінка та пріоритизація кіберризиків у процесах обробки облікових даних	Дозволяє зосередити контрольні процедури на найбільш критичних загрозах
Процесно-інтегрований підхід	Вбудовування контрольних механізмів у всі етапи облікових і бізнес-процесів	Забезпечує безперервність контролю та мінімізує операційні ризики
Технологічно-орієнтований підхід	Використання засобів автоматизованого моніторингу, шифрування, автентифікації та журналювання подій	Підвищує швидкість виявлення інцидентів і рівень захисту даних
Підхід розподіленої відповідальності	Чітке визначення функцій і відповідальності між підприємством і хмарним провайдером	Зменшує ризики невизначеності та підвищує керованість системи
Аудиторсько-аналітичний підхід	Застосування внутрішнього аудиту, безперервного контролю та аналітики даних	Сприяє своєчасному виявленню відхилень і підвищенню прозорості

Джерело: сформовано автором на основі [5, с. 17; 8, с. 736; 14; 15, p. 79].

Синергічне поєднання наведених підходів формує багаторівневу систему внутрішнього контролю, яка забезпечує не лише технічний захист, але й управлінську керованість кібербезпекою. Практична реалізація такої системи передбачає інтеграцію ризик-орієнтованого аналізу з автоматизованими засобами контролю доступу, коли, наприклад, доступ до фінансових модулів хмарної облікової системи обмежується відповідно до ролей користувачів із застосуванням багатофакторної автентифікації та постійного моніторингу аномальної активності [5, с. 17]. Водночас процесно-інтегрований підхід забезпечує включення контрольних процедур

безпосередньо у бізнес-процеси, що проявляється у вбудованих перевірках коректності операцій, автоматичних тригерах при відхиленнях та фіксації всіх дій у журналах подій. Технологічна складова посилює ці механізми через використання інструментів шифрування та систем виявлення інцидентів, що дозволяє оперативно реагувати на спроби несанкціонованого доступу або зміну облікових даних. Підхід розподіленої відповідальності, своєю чергою, забезпечує чітке закріплення контрольних функцій між підприємством і провайдером, наприклад, коли провайдер відповідає за фізичну безпеку серверів і базову інфраструктуру, тоді як користувач – за налаштування доступу, політики безпеки та контроль операцій [8, с. 736]. Аудиторсько-аналітичний компонент підсилює систему через використання безперервного аудиту та аналітики журналів подій, що дає змогу не лише фіксувати інциденти, а й виявляти приховані закономірності кіберзагроз. У сучасних умовах така інтегрована модель дозволяє підвищити достовірність облікової інформації, знизити ризик її втрати або спотворення та забезпечити адаптивність системи внутрішнього контролю до динамічних змін цифрового середовища.

Специфіка функціонування хмарних облікових платформ визначається віддаленим зберіганням даних, мережевим доступом та інтеграцією з іншими цифровими сервісами, що істотно змінює підходи до внутрішнього контролю та управління кіберризиками. Перенесення облікових процесів у хмарне середовище підвищує гнучкість і оперативність обробки інформації, але водночас ускладнює контроль за доступом, цілісністю та безпекою даних, вимагаючи адаптації контрольних механізмів до умов розподіленої інфраструктури (табл. 2).

Таблиця 2

Специфіка функціонування хмарних облікових платформ та їх вплив на внутрішній контроль і управління кіберризиками

Особливість функціонування	Характеристика	Вплив на внутрішній контроль і кіберризики
Віддалене зберігання даних	Дані розміщуються на серверах хмарного провайдера	Потребує посилення контролю за доступом і шифруванням інформації
Доступ через мережу Інтернет	Можливість доступу з будь-якої локації та пристрою	Підвищує ризики несанкціонованого доступу та атак
Масштабованість ресурсів	Гнучке розширення обчислювальних потужностей	Ускладнює контроль за конфігурацією та змінами системи
Інтеграція з іншими системами	Обмін даними через API та зовнішні сервіси	Збільшує кількість потенційних вразливостей
Розподілена відповідальність	Частина функцій контролю виконується провайдером	Вимагає чіткого розмежування контрольних повноважень
Безперервність обслуговування	Система працює у режимі 24/7	Потребує постійного моніторингу та автоматизованого контролю

Джерело: сформовано автором на основі [6; 9, с. 105; 10, p. 1077; 12, p. 69].

Функціональна специфіка хмарних платформ трансформує логіку внутрішнього контролю з переважно регламентно-перевірочної у динамічну, аналітично орієнтовану систему управління кіберризиками. Це проявляється у переході до безперервного моніторингу доступу та операцій, коли будь-яка дія користувача у фінансових модулях фіксується та аналізується в режимі реального часу з використанням поведінкових моделей [9, с. 105]. Наприклад, нетипова активність, така як одночасний доступ до облікової системи з різних географічних локацій або різке збільшення обсягу операцій, автоматично ідентифікується як потенційно ризикова та ініціює додаткові контрольні процедури.

Практичне значення набуває інтеграція механізмів багаторівневої автентифікації та контекстного контролю доступу, коли рішення про надання доступу залежить не лише від облікових даних користувача, а й від параметрів

середовища, зокрема пристрою, IP-адреси або часу входу. У системах бухгалтерського обліку це дозволяє мінімізувати ризики несанкціонованого втручання у фінансові записи та забезпечити простежуваність усіх змін [12, p. 69].

Інтеграційний характер хмарних платформ обумовлює необхідність контролю міжсистемної взаємодії, що реалізується через перевірку коректності передачі даних між обліковими системами, банківськими сервісами та платіжними інструментами. У реальних умовах це проявляється у використанні автоматизованих процедур звірки транзакцій, коли невідповідності між даними систем фіксуються та підлягають додатковій перевірці [6]. Масштабованість ресурсів, у свою чергу, вимагає впровадження контролю змін конфігурації, що дозволяє відстежувати будь-які модифікації середовища та запобігати виникненню вразливостей.

Розподілена модель відповідальності зумовлює необхідність чіткої координації контрольних функцій між підприємством і провайдером, що на практиці реалізується через укладення угод про рівень сервісу та визначення зон відповідальності за безпеку. У сукупності це формує адаптивну систему внутрішнього контролю, здатну оперативно реагувати на кіберзагрози, забезпечувати цілісність облікових даних і підтримувати безперервність фінансово-господарських процесів у цифровому середовищі.

Обґрунтування критеріїв та показників оцінювання ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ потребує комплексного врахування технічних і організаційних аспектів їх функціонування. Ефективність у цьому контексті визначається не лише рівнем захищеності, а здатністю системи своєчасно ідентифікувати загрози, мінімізувати їх наслідки та забезпечувати стабільність облікових процесів без втрати достовірності даних (табл. 3).

Таблиця 3

Критерії та показники оцінювання ефективн

Особливість функціонування	Характеристика	Вплив на внутрішній контроль і кіберризики
Віддалене зберігання даних	Дані розміщуються на серверах хмарного провайдера	Потребує посилення контролю за доступом і шифруванням інформації
Доступ через мережу Інтернет	Можливість доступу з будь-якої локації та пристрою	Підвищує ризики несанкціонованого доступу та атак
Масштабованість ресурсів	Гнучке розширення обчислювальних потужностей	Ускладнює контроль за конфігурацією та змінами системи
Інтеграція з іншими системами	Обмін даними через API та зовнішні сервіси	Збільшує кількість потенційних вразливостей
Розподілена відповідальність	Частина функцій контролю виконується провайдером	Вимагає чіткого розмежування контрольних повноважень
Безперервність обслуговування	Система працює у режимі 24/7	Потребує постійного моніторингу та автоматизованого контролю

Джерело: сформовано автором на основі [7, с. 117; 13, p. 295; 14; 15, p. 83].

Запропонована система критеріїв і показників формує основу для кількісно-аналітичного оцінювання ефективності внутрішнього контролю, що забезпечує перехід від декларативної оцінки безпеки до обґрунтованого управління кіберризиками. У сучасних умовах це реалізується через інтегровані аналітичні панелі (dashboards), які акумулюють дані про інциденти, доступи та стан системи захисту. Зокрема, критерій надійності захисту практично відображається у динаміці спроб несанкціонованого доступу: їх різке зростання може сигналізувати про цілеспрямовану атаку або наявність вразливостей у конфігурації системи [7, с. 117].

Оперативність реагування набуває вимірюваного характеру через показники середнього часу виявлення та усунення інцидентів, що дозволяє оцінити не лише технічні можливості системи, а й ефективність організаційних процедур реагування. Наприклад, скорочення часу реагування після впровадження автоматизованих систем сповіщення свідчить про підвищення зрілості контрольного середовища. Критерій цілісності даних

реалізується через механізми автоматизованої звірки, коли навіть незначні розбіжності у фінансових записах можуть бути оперативно ідентифіковані та усунуті до формування звітності.

Контроль доступу в практичній площині передбачає регулярний перегляд прав користувачів і виявлення випадків їх надлишковості, що особливо актуально в умовах віддаленої роботи персоналу. Водночас прозорість і аудитованість забезпечуються повнотою журналювання, що дозволяє відтворити логіку будь-якої операції та встановити відповідальність у разі інциденту [13, p. 295]. Адаптивність системи проявляється у здатності швидко впроваджувати оновлення безпеки та змінювати політики доступу у відповідь на нові загрози, що є критично важливим у середовищі постійної еволюції кіберризиків. Отже, практичне застосування запропонованих критеріїв і показників дозволяє не лише оцінити поточний стан системи внутрішнього контролю, але й сформувати основу для її постійного вдосконалення, орієнтованого на забезпечення стійкості облікових платформ до кіберзагроз і підвищення надійності фінансової інформації.

Забезпечення ефективності внутрішнього контролю кібербезпеки в умовах використання хмарних технологій супроводжується низкою взаємопов’язаних науково-практичних проблем, зумовлених розподіленістю інфраструктури, сервісною моделлю обробки даних і високою динамікою кіберзагроз. Однією з ключових є невизначеність у розмежуванні відповідальності між підприємством і провайдером, що ускладнює формування цілісної системи контролю та знижує ефективність реагування на інциденти [14]. Обмежена прозорість внутрішніх процесів провайдера та доступу до технічної інформації звужує можливості повноцінного аудиту й оцінювання ризиків.

Суттєвою проблемою виступає асиметрія інформації щодо вразливостей і загроз, яка поєднується з розширенням поверхні атак через інтеграцію систем за допомогою інтерфейсів програмування застосунків API. Водночас

складність управління доступом у розподіленому середовищі зумовлює появу надлишкових прав і підвищує ризик внутрішніх загроз, що посилюється недостатнім рівнем кібербезпекової культури персоналу.

Обмежена адаптивність контрольних механізмів до швидких змін кіберсередовища, відсутність уніфікованих підходів до оцінювання ефективності та недостатня інтеграція автоматизованих засобів моніторингу знижують результативність внутрішнього контролю [15, p. 83]. Додатково ускладнюється забезпечення безперервності облікових процесів у разі інцидентів, а також обробка значних обсягів подій у режимі реального часу.

Підвищення ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ доцільно забезпечувати через формування інтегрованої моделі управління кіберризиками, що поєднує організаційні регламенти, технологічні інструменти та аналітичні механізми контролю. В умовах цифрового середовища першочергового значення набуває чітке нормативне закріплення розподілу відповідальності між підприємством і провайдером хмарних сервісів із деталізацією контрольних функцій, процедур реагування на інциденти та вимог до рівня захисту даних. Це дозволяє усунути зони невизначеності та підвищити керованість системи кібербезпеки.

Доцільним є впровадження ризик-орієнтованого підходу до організації внутрішнього контролю, що передбачає систематичну ідентифікацію та ранжування кіберризиків із подальшим фокусуванням контрольних процедур на критичних сегментах облікової системи. Практична реалізація цього підходу має супроводжуватися використанням автоматизованих засобів моніторингу, здатних у режимі реального часу виявляти аномальну активність і формувати сигнали про потенційні інциденти.

Важливим напрямом є вдосконалення механізмів управління доступом через впровадження принципу мінімальних привілеїв, багатофакторної автентифікації та контекстного контролю доступу, що враховує параметри

середовища використання системи. Одночасно необхідно забезпечити повноту журналювання операцій та їх аналітичну обробку, що створює основу для безперервного аудиту і підвищує прозорість облікових процесів.

Рекомендується посилити контроль інтеграційних взаємодій між хмарними обліковими платформами та іншими інформаційними системами, зокрема через перевірку коректності обміну даними, застосування механізмів шифрування та захисту інтерфейсів програмування застосунків (Application Programming Interface, API). Це дозволяє зменшити ризики компрометації даних у процесі міжсистемної взаємодії.

Суттєвим є розвиток адаптивності системи внутрішнього контролю, що передбачає регулярне оновлення політик безпеки, програмного забезпечення та інструментів захисту відповідно до актуальних кіберзагроз. У цьому контексті ефективним є впровадження елементів аналітики великих даних та алгоритмів виявлення аномалій, які підвищують здатність системи до превентивного реагування.

Не менш важливим є підвищення рівня кібербезпекової культури персоналу через систематичне навчання, тестування знань і формування відповідального ставлення до обробки облікової інформації. Сукупна реалізація зазначених рекомендацій забезпечує перехід від фрагментарного до системного внутрішнього контролю кібербезпеки, підвищує стійкість хмарних облікових платформ до кіберзагроз і сприяє забезпеченню достовірності та безперервності облікових процесів у сучасних умовах цифрової економіки.

Висновки. У результаті дослідження встановлено, що ефективність системи внутрішнього контролю кібербезпеки хмарних облікових платформ визначається рівнем інтеграції ризик-орієнтованих, процесних і технологічних підходів у єдину адаптивну систему управління кіберризиками. Обґрунтовано, що контроль у хмарному середовищі трансформується у безперервну аналітичну модель, орієнтовану на превентивне виявлення загроз, а

 ISSN 3041-2129

запропоновані критерії та показники забезпечують можливість його об’єктивного оцінювання.

Виявлено, що основними проблемами є невизначеність розподілу відповідальності між користувачем і провайдером, обмежена прозорість обробки даних, асиметрія інформації щодо кіберзагроз, розширення поверхні атак через інтеграцію систем, складність управління доступом і недостатня адаптивність контрольних механізмів. Додатково встановлено вплив людського фактора та відсутність уніфікованих підходів до оцінювання ефективності .

Обґрунтовано, що підвищення ефективності контролю досягається через формування інтегрованої моделі управління кіберризиками, впровадження автоматизованого моніторингу, удосконалення контролю доступу, посилення захисту інтеграцій та підвищення кібербезпекової культури персоналу.

Перспективи подальших досліджень пов’язані з розробленням формалізованих моделей оцінювання ефективності контролю, інтеграцією технологій штучного інтелекту у системи моніторингу кіберзагроз та стандартизацією підходів до аудиту кібербезпеки хмарних облікових платформ.

Список використаних джерел

1. Borovskova Y. Efficiency of using Dynamodb and adaptive polling for processing long-running http requests in server applications on NestJS. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2024. № 6. С. 86–93. DOI: https://doi.org/10.32782/1995-0519.2024.6.10.

2. Опірський І. Р., Хохлачова Ю. Є., Стефанків А. В., Шевчук Ю. А. Аналіз технічних особливостей реалізації шифрування даних на SD-картах в Android. *Сучасний захист інформації*. 2025. Вип. 1, № 61. С. 219–228. DOI: https://doi.org/10.31673/2409-7292.2025.016526.

3. Bershchanskyi Y., Klym H., Shevchuk Y. Containerized artificial intelligent system design in cloud and cyber-physical systems. *Advances in Cyber-Physical Systems*. 2024. Vol. 9, № 2. P. 151–157. URL: https://doi.org/10.23939/acps2024.02.151 (дата звернення: 26.01.2026).

4. Kaptosv L. Using Redis for Caching optimization in high-traffic web applications. *International Journal of Advanced Multidisciplinary Research and Studies*. 2025. Vol. 5, № 4. P. 1714–1722. DOI: https://doi.org/10.62225/2583049X.2025.5.4.4839.

5. Смірнова Т., Конопліцька-Слободенюк О., Буравченко К., Смірнов С., Кравчук О., Козірова Н., Смірнов О. Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS. *Кібербезпека: освіта, наука, техніка*. 2024. Вип. 4, № 24. С. 6–27. DOI: https://doi.org/10.28925/2663-4023.2024.24.627.

6. Шеверя Я. В., Яцко М. В., Мельянкова Л. В. Впровадження хмарних технологій у бухгалтерський облік України. *Актуальні питання економічних наук*. 2025. № 10. DOI: https://doi.org/10.5281/zenodo.15302198.

7. Івкова В. С., Банах Р. І. Методологія дослідження стану захищеності хмарних технологій за допомогою OSINT-інструментів. *Сучасний захист інформації*. 2025. № 2. С. 114–123. DOI: https://doi.org/10.31673/2409-7292.2025.026087.

8. Аверічев І., Роженко А., Кихтенко Є. Інноваційні підходи до підвищення рівня кібербезпеки корпоративних мереж при використанні хмарних технологій. *Кібербезпека: освіта, наука, техніка*. 2025. Вип. 1, 29. С. 732–747. DOI: https://doi.org/10.28925/2663-4023.2025.29.934.

9. Лобода Н., Петришин Л., Чабанюк О. Інноваційні цифрові технології в організації обліку, звітності та аудиту підприємств. *Фінансовий простір*. 2025. Вип. 4, № 58. С. 101–118. DOI: https://doi.org/10.30970/fp.4(58).2025.101117118.

10. Sanusi I., Sanusi A. R., Shamwill A. K., Yinusa S., Iliyasu R. Evaluation of cloud based computing in security accounting information system. *World Journal of Advanced Research and Reviews*. 2025. Vol. 25, № 3. P. 1073–1086. DOI: https://doi.org/10.30574/wjarr.2025.25.3.0734.

11. Gaurav A., Ambar M. T. Cloud-based accounting systems and financial reporting efficiency: a comparative review. *International Journal of Advanced Research and Multidisciplinary Trends*. 2025. Vol. 2, № 1. P. 882–893. URL: https://ijarmt.com/index.php/j/article/view/454/342 (дата звернення: 26.01.2026).

12. Atadoga A., Umoga U. J., Lottu O. A., Sodiya E. O. Evaluating the impact of cloud computing on accounting firms: a review of efficiency, scalability, and data security. *Global Journal of Engineering and Technology Advances*. 2024. Vol. 18, № 2. P. 065–074. DOI: https://doi.org/10.30574/gjeta.2024.18.2.0027.

13. Anaege A. E., Eneh O. M., Inweregbu O. A., Okwuego S. P. Cybersecurity threats in cloud accounting: a case study of microfinance banks in anambra state using NAMBUIT banking software. *International Journal of Research and Innovation in Applied Science*. 2025. Vol. X, № III. P. 290–300. DOI: https://doi.org/10.51584/IJRIAS.2025.10030021.

14. Alqudah H., Mansour A. A. Z., Rawashdeh B. S., Lutfi A., Al Barrak T., Almaiah M. A., Alrawad M. Enhancing the internal auditors' effectiveness in jordanian companies: the impact of cloud-based accounting usage and the moderating role of digital proficiency. *Computers in Human Behavior Reports*. 2024. Vol. 15. Article 100442. DOI: https://doi.org/10.1016/j.chbr.2024.100442.

15. Ali O. A. M., Matarneh A. J., Almalkawi A., Mohamed H. The impact of cyber governance in reducing the risk of cloud accounting in jordanian commercial banks from the perspective of jordanian auditing firms. *Modern Applied Science*. 2020. Vol. 14, № 3. P. 75–89. DOI: https://doi.org/10.5539/mas.v14n3p75.