DOI: https://doi.org/10.32782/2524-0072/2024-67-26

УДК 657.9:004.6

ОРГАНІЗАЦІЯ ЗАХИСТУ БУХГАЛТЕРСЬКОЇ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБЛІКУ

ORGANIZATION OF ACCOUNTING INFORMATION PROTECTION IN AUTOMATED ACCOUNTING SYSTEMS

Гаркуша Сергій Анатолійович
кандидат економічних наук, доцент,
Сумський національний аграрний університет
ORCID: https://orcid.org/0000-0002-2043-1217

Harkusha Serhii
Sumy National Agrarian University

У статті розглядається організація захисту бухгалтерської інформації в автоматизованих системах обліку, що є критично важливим аспектом для забезпечення конфіденційності, цілісності та доступності даних. Визначено основні загрози, з якими стикаються підприємства, а також проаналізовано сучасні технології, які можуть бути впроваджені для підвищення рівня безпеки. Зокрема, акцентується увага на використанні штучного інтелекту, блокчейну та систем резервного копіювання. Особливу увагу приділено невирішеним питанням у сфері захисту, таким як недостатня інтеграція новітніх технологій, відсутність єдиних стандартів безпеки та актуалізація навчання персоналу. Стаття має на меті виявити ключові напрями для подальших досліджень у сфері інформаційної безпеки бухгалтерського обліку та визначити практичні рекомендації для підприємств.

Ключові слова: захист бухгалтерської інформації, автоматизовані системи обліку, інформаційна безпека, штучний інтелект, блокчейн.

This article explores the organization of accounting information protection in automated accounting systems, a critical aspect for ensuring the confidentiality, integrity, and availability of financial data. As businesses increasingly rely on technology for managing their financial information, the potential risks and threats associated with data breaches have become more pronounced. The research identifies the primary threats that enterprises face, including cyberattacks, unauthorized access, and data corruption. Additionally, it analyzes modern technologies that can be implemented to enhance the security of accounting systems. Among these technologies, artificial intelligence (AI) stands out as a powerful tool for detecting anomalies and predicting potential security breaches before they occur. AI algorithms can analyze vast amounts of data in real time, providing organizations with the insights needed to respond swiftly to any irregularities. Furthermore, the integration of blockchain technology offers a decentralized and immutable ledger that ensures data integrity and transparency, making it extremely difficult for malicious actors to manipulate financial records. The article also emphasizes the importance of backup systems, particularly cloud-based solutions, which enable organizations to recover data quickly in case of system failures or cyber incidents. However, despite the advancements in technology, several unresolved issues persist in the realm of information security. One significant challenge is the insufficient integration of innovative technologies into existing systems, leading to vulnerabilities that can be exploited by cybercriminals. Moreover, the lack of unified security standards hampers the ability of organizations to implement effective protection measures. Establishing comprehensive security frameworks that outline best practices and compliance requirements is essential for enhancing the overall security posture of accounting information systems. Another critical aspect highlighted in the article is the need for ongoing employee training. Human error remains one of the leading causes of data breaches; therefore, regular training programs are vital to ensure that employees are aware of potential threats and equipped with the knowledge to mitigate risks. By identifying these unresolved issues, this study opens new avenues for further research in the field of information security in accounting. The findings underline the necessity for organizations to adopt a systematic approach to protect accounting information, incorporating advanced technological solutions while addressing the human factor. This holistic perspective aims to foster a secure information environment that not only safeguards financial data but also builds trust among stakeholders. In conclusion, the article calls for collaboration among researchers, practitioners, and regulatory bodies to develop comprehensive frameworks that ensure the security of accounting information in the face of evolving threats and challenges.

Keywords: accounting information protection, automated accounting systems, information security, artificial intelligence, blockchain.

Постановка проблеми. В умовах цифровізації сучасного бізнесу автоматизовані системи обліку стали невід'ємною частиною управління фінансовими ресурсами підприємств. Такі системи дозволяють значно спростити процес обліку, автоматизувати розрахунки та забезпечити оперативність у прийнятті управлінських рішень. Однак, із зростанням рівня автоматизації виникають нові виклики, пов'язані із забезпеченням безпеки бухгалтерської інформації, яка є однією з найцінніших активів підприємства.

Бухгалтерська інформація включає дані про фінансовий стан, доходи, витрати, активи та зобов'язання підприємства, які є вкрай важливими для прийняття стратегічних рішень. Неналежний захист таких даних може призвести до серйозних фінансових втрат, втрати конкурентних переваг, порушення законодавства та завдати значної шкоди репутації підприємства.

Аналіз останніх досліджень і публікацій. За результатами дослідження літератури, зокрема [1–5], з'ясовано, що деякі теоретичні і практичні аспекти у цьому напрямі розглянуто у працях таких вчених та практиків, як Вітер С. А. [1], Гнатишин Л. [2], Грицай О. І. [3], Попівняк Ю. М. [4], Старенька О. М. [5] та ін.

Вітер С. А. та Світлішин І. І. [1, с. 502] зазначають, що кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями, це ускладнює виявлення та протидію зазначеним протиправним діям, тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загальнодержавного рівня, а кожного окремо взятого підприємства.

Грицай О. І. та Папіш В. І. [3] вказують на проблеми інтеграції, безпеки та ефективності стають ключовими аспектами, які вимагають уваги та розв'язання для успішного впровадження інформаційних технологій у сфері бухгалтерського обліку.

Попівняк Ю. М. [4, с. 155] стверджує, що у сучасному світі розвинутих технологій впровадженням останніх у процес ведення бухгалтерського обліку вже нікого не здивуєш. При цьому бухгалтерська інформація, яка формується у такому процесі, – особливий ресурс, що потребує ретельного захисту, адже від безпечного її використання залежить інформаційна безпека всього підприємства.

Гнатишин Л., Свиноус І., Протоцька Т. [2, с. 24] вказують, що за допомогою відповідної комп'ютерної програми захист можна значно посилити – зашифрувати облікову інформацію для запобігання несанкціонованому використанню, що робить її повністю безпечною.

Старенька О.М. [5, с. 73] розглянувши деякі переваги і недоліки без пекових заходів пропонує впроваджувати в бухгалтерський облік хмарних технологій, блокчейну і зазначає, що вони відповідають вимогам сьогодення, які продиктовані розвитком інформаційних технологій.

Аналіз сучасних тенденцій у сфері кібербезпеки показує, що для надійного захисту бухгалтерської інформації необхідно впроваджувати новітні технології, зокрема хмарні рішення та блокчейн, оскільки це дозволяє підвищити рівень безпеки даних, а також вирішити проблеми інтеграції, ефективності та кіберзлочинності, які стають все більш складними.

Виділення невирішених раніше частин загальної проблеми. У сфері організації захисту бухгалтерської інформації в автоматизованих системах обліку залишаються невирішеними питання інтеграції новітніх технологій, оцінки та управління ризиками, відсутності єдиних стандартів безпеки, актуалізації навчання персоналу, а також дослідження впливу кібератак на фінансові результати підприємств, тому дане питання потребує подальшого дослідження.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є аналіз існуючих методів та інструментів захисту бухгалтерської інформації в автоматизованих системах обліку, а також розробка практичних рекомендацій щодо підвищення рівня безпеки інформації. У роботі будуть розглянуті теоретичні основи інформаційної безпеки, особливості автоматизованих систем обліку, можливі загрози та методи їх нейтралізації.

Виклад основного матеріалу дослідження. Захист інформації – це процес забезпечення конфіденційності, цілісності та доступності даних, що є ключовими аспектами інформаційної безпеки. У контексті бухгалтерського обліку конфіденційність передбачає обмеження доступу до фінансових даних тільки для уповноважених осіб, цілісність забезпечує недоторканність та точність інформації, а доступність гарантує, що дані завжди доступні для використання у випадку потреби.

Досягнення високого рівня захисту бухгалтерської інформації можливе через застосування як організаційних, так і технічних методів. Організаційні методи включають розробку політик безпеки, підготовку персоналу

та контроль за дотриманням правил захисту. Технічні методи охоплюють використання спеціалізованих програмних засобів, шифрування даних, захист мережевого периметра тощо [1; 4].

Автоматизовані системи обліку – це програмні рішення, що дозволяють автоматизувати процеси збору, зберігання, обробки та аналізу бухгалтерської інформації. До таких систем належать ERP-системи (системи управління підприємством), CRM-системи (системи управління взаємовідносинами з клієнтами), а також спеціалізовані бухгалтерські програми, такі як BAS Бухгалтерія, Дебет плюс, MASTER: Бухгалтерія та ін.

Основними перевагами використання автоматизованих систем обліку є швидкість обробки даних, зниження ймовірності людських помилок, можливість інтеграції з іншими системами управління підприємством, а також оперативний доступ до інформації для прийняття управлінських рішень. Однак, одночасно з цими перевагами виникають і певні ризики.

Загрози для безпеки бухгалтерської інформації в автоматизованих системах можуть бути як зовнішніми, так і внутрішніми. Серед зовнішніх загроз найбільш поширеними є: кібератаки, віруси та шкідливе програмне забезпечення, незахищені мережеві з'єднання.

Внутрішні загрози виникають через: неналежне використання системи, випадкове видалення важливих файлів або нехтування правилами безпеки можуть спричинити витік інформації; співробітники можуть намагатися отримати доступ до інформації, яка не входить до їхніх посадових обов'язків; навмисні дії співробітників з метою завдати шкоди організації або передати інформацію конкурентам [3; 5].

Таким чином, забезпечення належного рівня безпеки в автоматизованих системах обліку потребує комплексного підходу, що охоплює як технічні, так і організаційні аспекти.

Для забезпечення захисту бухгалтерської інформації в автоматизованих системах застосовуються різні методи та технології, які можна розділити на організаційні та технічні (Таблиця 1).

Захист бухгалтерської інформації потребує комплексного підходу, який включає як організаційні, так і технічні заходи. Основна перевага організаційних методів – це формування єдиного підходу до безпеки, що знижує ризики через людські помилки, однак їх ефективність залежить від дотримання співробітниками правил і контролю за їх виконанням [1; 4].

Технічні методи забезпечують захист від зовнішніх і внутрішніх загроз шляхом використання сучасних технологій, таких як шифрування, системи виявлення вторгнень та антивірусне програмне забезпечення, однак такі методи вимагають регулярного оновлення, налаштування та моніторингу для підтримання актуальності захисту.

Програмні рішення, наприклад, засоби управління доступом або програми для резервного копіювання, дозволяють автоматизувати процеси захисту, що знижує потребу у втручанні користувачів та мінімізує ризик помилок, але ефективність таких рішень залежить від правильного налаштування та регулярного контролю.

Поєднання різних методів забезпечує надійний захист інформації, мінімізуючи ризики втрати або несанкціонованого доступу до бухгалтерських даних.

Ефективне управління ризиками у сфері захисту бухгалтерської інформації передбачає ідентифікацію потенційних загроз, оцінку ймовірності їх виникнення та аналіз можливих наслідків. На основі отриманої інформації визначаються відповідні заходи для зменшення ризиків або нейтралізації загроз (Таблиця 2).

У представленій таблиці ризики оцінено за кількома критеріями: тип загрози, ймовірність виникнення, можливі наслідки, рівень ризику та методи управління. Оцінка ризику базується на ймовірності виникнення загрози та її потенційних наслідках для організації.

Зовнішні загрози мають високий рівень ризику через поширеність кібератак. Найбільший ризик виникає при використанні вразливостей програмного забезпечення, тому важливо регулярно оновлювати програмні компоненти системи.

Внутрішні загрози також становлять суттєву небезпеку, особливо через недбалість працівників або несанкціонований доступ. Основними методами зниження ризиків є навчання співробітників та впровадження суворих правил доступу до інформації.

Технічні збої мають меншу ймовірність виникнення, але їх наслідки можуть бути значними, особливо при збої в обладнанні. Резервне копіювання та технічний моніторинг допомагають мінімізувати ці ризики.

Юридичні ризики оцінені як середні, оскільки порушення законодавства про захист даних можуть призвести до значних

Таблиця 1

Категорії та методи захисту інформації

Категорія	Метод захисту	Опис	Переваги	Недоліки
Організаційні методи	Розробка політик інформаційної безпеки	Встановлення правил і процедур щодо захисту даних, відповідальності працівників	Знижує людський фактор, формалізує процес захисту	Вимагає регулярного оновлення та контролю
	Навчання персоналу	Підвищення обізнаності працівників про загрози та правила роботи з інформацією	Зменшує ризики через людські помилки	Залежить від рівня залученості персоналу
	Аудит і контроль за дотриманням правил	Регулярні перевірки відповідності політикам безпеки	Дозволяє вчасно виявляти порушення та проблеми	Вимагає додаткових ресурсів та часу
Технічні методи	Шифрування даних	Перетворення інформації у незрозумілий формат, доступний лише з використанням ключа	Захищає конфіденційність навіть у разі перехоплення	Вимагає додаткових ресурсів для шифрування/ дешифрування
	Аутентифікація та контроль доступу	Забезпечує доступ до інформації лише авторизованим користувачам	Знижує ризик несанкціонованого доступу	Необхідність підтримки актуальності паролів та оновлення методів
	Резервне копіювання	Створення копій даних для відновлення у разі втрати або пошкодження	Дозволяє швидко відновити інформацію після інциденту	Вимагає регулярного оновлення та перевірки доступності резервів
	IDS/IPS (системи виявлення та запобігання вторгненням)	Виявлення спроб вторгнення в систему та блокування підозрілої активності	Дозволяє оперативно реагувати на загрози	Може викликати помилкові спрацьовування
	Антивірусне ПЗ та брандмауери	Захист від шкідливих програм та небажаних мережевих з’єднань	Забезпечує базовий рівень захисту від більшості загроз	Необхідність регулярного оновлення баз даних
Програмні рішення	Засоби управління доступом (Active Directory)	Керування правами доступу до різних ресурсів у мережі	Дозволяє централізовано управляти доступом до інформації	Складність налаштування та адміністрування
	Спеціалізовані програми для резервного копіювання	Програмне забезпечення для створення та збереження резервних копій	Забезпечує автоматизацію процесу резервування	Залежить від правильності налаштувань і регулярності оновлення

Джерело: узагальнено автором

Таблиця 2

Типи загроз та методи управління ризиками в автоматизованих системах обліку

Тип загрози	Приклад загрози	Ймовірність виникнення	Можливі наслідки	Рівень ризику	Методи управління
Зовнішні загрози	Кібератаки (наприклад, фішинг, DDoS атаки)	Висока	Витік даних, фінансові втрати, пошкодження репутації	Високий	Впровадження брандмауерів, антивірусних систем
	Використання вразливостей програмного забезпечення	Середня	Витік або спотворення даних	Середній	Регулярне оновлення програмного забезпечення
Внутрішні загрози	Недбалість працівників	Висока	Випадкова втрата даних, витік інформації	Високий	Навчання персоналу, контроль доступу
	Несанкціонований доступ	Середня	Витік конфіденційної інформації	Середній	Аутентифікація, розмежування прав доступу
Технічні збої	Збої в обладнанні	Низька	Втрата даних, зупинка роботи системи	Низький	Резервне копіювання, моніторинг технічного стану
	Помилки у програмному забезпеченні	Середня	Пошкодження або втрата інформації	Середній	Тестування та оновлення програмного забезпечення
Юридичні ризики	Порушення законодавства про захист інформації	Низька	Штрафи, позови, втрата довіри	Середній	Консультації з юристами, відповідність стандартам

Джерело: узагальнено автором

фінансових та репутаційних втрат. Важливо підтримувати відповідність вимогам стандартів інформаційної безпеки та консультуватися з фахівцями.

Для забезпечення ефективного захисту бухгалтерської інформації в автоматизованих системах обліку доцільно дотримуватись комплексу практичних заходів, які охоплюють технічні, організаційні та юридичні аспекти.

Технічні заходи зосереджені на впровадженні сучасних технологій захисту інформації, до основних рекомендацій належать:

– застосування кількох рівнів аутентифікації підвищує безпеку доступу до системи. Наприклад, крім пароля, можна використовувати SMS-коди або біометричні дані;

– шифрування даних забезпечує конфіденційність інформації, навіть якщо зловмисник отримає фізичний доступ до носія даних;

– використання систем виявлення вторгнень та засобів аналізу подій допомагає виявляти підозрілу активність та оперативно реагувати на інциденти;

– резервне копіювання регулярне створення резервних копій дозволяє швидко відновити втрачені дані у разі збоїв або кібератак, рекомендується зберігати копії в окремому безпечному місці.

Організаційні заходи передбачають створення відповідних політик та процедур безпеки, а також залучення персоналу до забезпечення захисту інформації:

– формування чітких правил і вимог щодо захисту інформації, які повинні виконувати всі працівники;

– працівники повинні знати про актуальні загрози інформаційній безпеці та методи їх запобігання;

– доступ до інформації має бути наданий лише тим працівникам, яким це необхідно для виконання їхніх посадових обов'язків, застосування ролей та рівнів доступу сприяє зниженню ризику несанкціонованого доступу;

– перевірки системи дозволяють виявляти слабкі місця та оцінювати ефективність застосованих заходів.

Юридичні аспекти включають дотримання законодавства та стандартів щодо захисту інформації:

– підприємства повинні дотримуватися вимог нормативних актів щодо захисту персональних даних та конфіденційної інформації;

– укладення договорів із працівниками та контрагентами, які обробляють інформацію, з метою забезпечення збереження її конфіденційності;

– страхування дозволяє мінімізувати фінансові втрати у разі реалізації кіберзагроз.

Сучасні технології та методи захисту інформації постійно розвиваються, щоб відповідати новим викликам і загрозам, які постають перед автоматизованими системами обліку. Відповідно до цих змін, можна виділити кілька перспективних напрямів розвитку захисту бухгалтерської інформації (Таблиця 3).

Штучний інтелект та машинне навчання можуть суттєво підвищити ефективність виявлення загроз через реальний аналіз даних, але впровадження цих технологій пов'язане з високими витратами та потребою в кваліфікованих спеціалістах. Блокчейн забезпечує високий рівень прозорості та захисту від несанкціонованих змін, роблячи його ідеальним для бухгалтерії, однак, його розуміння і впровадження серед користувачів потребує нових стандартів. Квантові обчислення пропонують нові рівні шифрування і швидкість обробки даних, але їхня висока вартість та стадія розробки можуть стати бар'єрами для широкого використання. Системи резервного копіювання в хмарі забезпечують швидке відновлення інформації, але залежать від стабільного інтернет-з'єднання, що може обмежити доступ до резервних копій. Стандарти та регуляторні вимоги відіграють важливу роль у підвищенні довіри клієнтів і запобіганні юридичним наслідкам, хоча їх впровадження може бути складним і вимагати постійного навчання персоналу.

Таким чином, розвиток систем захисту бухгалтерської інформації відкриває нові горизонти для підприємств, проте ставить перед ними серйозні виклики. Успішне впровадження новітніх технологій і стандартів вимагатиме зусиль і ресурсів, але значно підвищить ефективність і надійність захисту інформації.

Таблиця 3

Перспективи розвитку захисту бухгалтерської інформації

Перспектива розвитку	Опис	Переваги	Виклики
Штучний інтелект та машинне навчання	Використання алгоритмів для аналізу даних і виявлення аномалій у реальному часі.	Підвищення ефективності виявлення загроз; автоматизація процесів.	Висока вартість впровадження; потреба в спеціалізованих фахівцях.
Блокчейн	Використання децентралізованих реєстрів для зберігання бухгалтерських даних.	Неможливість зміни даних без відома; підвищена прозорість.	Обмежене розуміння технології серед користувачів; потреба у нових стандартах.
Квантові обчислення	Використання квантових технологій для шифрування та обробки даних.	Нова ера шифрування; висока швидкість обробки даних.	Технологія ще на стадії розробки; висока вартість впровадження.
Системи резервного копіювання	Інтеграція сучасних рішень для автоматичного резервного копіювання даних у хмарі.	Швидке відновлення даних; знижений ризик втрати даних.	Залежність від інтернет-з'єднання; можливі ризики безпеки в хмарі.
Стандарти та регуляторні вимоги	Адаптація до нових міжнародних стандартів захисту інформації та змін у законодавстві.	Підвищення довіри з боку клієнтів; захист від юридичних наслідків.	Складність впровадження нових стандартів; потреба в постійному навчанні персоналу.

Джерело: узагальнено автором

Висновки. Організація захисту бухгалтерської інформації в автоматизованих системах обліку є складним і багатогранним завданням, що вимагає комплексного підходу. У сучасному світі, де інформаційні технології активно розвиваються, з'являються нові виклики, що ставлять під загрозу конфіденційність, цілісність і доступність бухгалтерських даних.

Аналіз сучасних тенденцій показує, що ефективна система захисту інформації повинна ґрунтуватися на інтеграції інноваційних технологій, таких як штучний інтелект, блокчейн і квантові обчислення. Ці технології здатні забезпечити високий рівень безпеки даних і оперативне реагування на можливі загрози. Однак їх впровадження потребує значних інвестицій та кваліфікованого персоналу, що може стати серйозною перешкодою для багатьох підприємств.

Крім того, важливу роль у захисті інформації відіграють організаційні та юридичні заходи. Розробка чітких політик безпеки, навчання персоналу, а також дотримання міжнародних стандартів є необхідними умовами для забезпечення надійності системи. Регулярний аудит та оцінка ризиків допомагають виявити слабкі місця та вжити відповідних заходів для їх усунення.

Перспективи розвитку систем захисту бухгалтерської інформації вимагають від організацій готовності до змін і постійного вдосконалення. Впровадження нових технологій та стандартів не лише підвищить рівень захисту інформації, а й сприятиме зростанню довіри з боку клієнтів і партнерів.

Отже, захист бухгалтерської інформації в автоматизованих системах обліку є критично важливим завданням, яке потребує системного підходу та активної участі всіх учасників процесу. Лише таким чином можливо забезпечити ефективний захист від сучасних загроз та гарантувати надійність і цілісність фінансової інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Вітер С. А., Світлішин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. № 11. С. 497–502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf

2. Гнатишин Л., Свиноус І., Протоцька Т. Організація бухгалтерського обліку в умовах інформаційних та комунікаційних технологій. *Вісник національного університету природокористування.* 2022. № 29. С. 21–25. DOI: https://doi.org/10.31734/economics2022.29.021

3. Грицай О. І., Папіш В. І. Розвиток інформаційних технологій в Україні та їх інтегрування у сфері бухгалтерського обліку. *Економіка та суспільство*. 2024. Випуск 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-88

4. Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. *Бізнес Інформ*. 2019. № 8. С. 150–157. DOI: https://doi.org/10.32983/2222-4459-2019-8-150-157

5. Старенька О.М. Стан використання сучасних інформаційних технологій для бухгалтерського обліку на підприємствах. *Вісник соціально-економічних досліджень*. 2022. 75. № 1-2 (80-81). С. 61. URL: http://vsed.oneu.edu.ua/collections/2022/80-81/pdf/61-75.pdf

REFERENCES:

1. Viter, S. A., & Svitlyshyn, I. I. (2017). Zahyst oblikovoyi informatsiyi ta kyberbezpeka pidpryyemstva [Protection of accounting information and cybersecurity of the enterprise]. *Ekonomika i suspilstvo*, (11), 497–502. Available at: https://economyandsociety.in.ua/journals/11_ukr/80.pdf [in Ukrainian]

2. Hnatysyn, L., Svynous, I., & Protska, T. (2022). Orhanizatsiya buhhalters'koho obliku v umovakh informatsiynykh ta komunikatsiynykh tekhnolohiy [Organization of accounting in the context of information and communication technologies]. *Visnyk natsional'noho universytetu pryrodokorystuvannya*, (29), 21–25. DOI: https://doi.org/10.31734/economics2022.29.021 [in Ukrainian]

3. Grytsay, O. I., & Papish, V. I. (2024). Rozvytok informatsiynykh tekhnolohiy v Ukrayini ta yikh intehruvannya u sferi buhhalters'koho obliku [Development of information technologies in Ukraine and their integration in the field of accounting]. *Ekonomika ta suspilstvo*, (61). DOI: https://doi.org/10.32782/2524-0072/2024-61-88 [in Ukrainian]

4. Popivnyak, Yu. M. (2019). Kyberbezpeka ta zakhyst buhhalters'kykh danykh v umovakh zastosuvannya novitnikh informatsiynykh tekhnolohiy [Cybersecurity and protection of accounting data in the context of using modern information technologies]. *Biznes Inform*, (8), 150–157. DOI: https://doi.org/10.32983/2222-4459-2019-8-150-157 [in Ukrainian]

5. Starenka, O. M. (2022). Stan vykorystannya suchasnykh informatsiynykh tekhnolohiy dlya buhhalters'koho obliku na pidpryyemstvakh [The state of using modern information technologies for accounting in enterprises]. *Visnyk sotsial'no-ekonomichnykh doslidzhen'*, (75), 1-2(80-81), 61. Available at: http://vsed.oneu.edu.ua/collections/2022/80-81/pdf/61-75.pdf [in Ukrainian]