5. Сакун А., Іванова Н., Мільман Л. Застосування блокчейн-технологій у бухгалтерському обліку та аудиті: аналіз інноваційних можливостей у контексті цифрової трансформації. *Економіка. Фінанси. Право*. 2024. Вип. 2. С. 14-17. URL: https://doi.org/10.37634/efp.2024.2.3.

6. Потриваєва Н.В., Громова Я. М. Удосконалення аудиту поточних зобов'язань у взаємоз'язку з оптимізацією облікового процесу. *Вісник аграрної науки Причорномор'я*. 2018. Вип. 2. С.11-15. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/4665.

7. Яковенко А. О., Гнатьєва Т. М., Мельничук В. М. Світові тенденції інтеграції штучного інтелекту в бухгалтерському обліку. *Аграрні інновації*. 2024. № 23. С. 221–227. URL: https://doi.org/10.32848/agrar.innov.2024.23.32.

Стешенко О.О.,
здобувач першого (бакалаврського) рівня вищої освіти
обліково-фінансового факультету
Науковий керівник – **Лугова О.І.,**
канд. екон. наук, доцент
Миколаївський національний аграрний університет
м. Миколаїв

КІБЕРРИЗИКИ ТА КІБЕРЗАГРОЗИ У БУХГАЛТЕРСЬКОМУ ОБЛІКУ: ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОБЛІКОВИХ СИСТЕМ

У сучасних умовах цифровізації економіки та широкого впровадження інформаційних технологій у сферу бухгалтерського обліку питання кібербезпеки облікових систем набуває особливої актуальності. Автоматизація бухгалтерських процесів, використання ERP-систем, хмарних сервісів, електронного документообігу, дистанційного доступу до фінансових баз даних та інтеграція бухгалтерських платформ із банківськими і податковими сервісами суттєво підвищують ефективність облікової роботи, проте водночас формують нові ризики для захисту фінансової інформації. У зв'язку з цим кіберризики та кіберзагрози стають одним із ключових факторів, що впливають на достовірність бухгалтерського обліку, фінансову безпеку підприємств та стабільність їх господарської діяльності.

Кіберризики у бухгалтерському обліку слід розглядати як імовірність виникнення негативних наслідків унаслідок несанкціонованого доступу, втручання, модифікації, викрадення або знищення облікової інформації в інформаційно-комунікаційних системах підприємства [1]. Такі ризики можуть призводити до викривлення даних бухгалтерського обліку, втрати

фінансової інформації, порушення безперервності облікових процесів, розголошення конфіденційних відомостей, а також до значних фінансових і репутаційних втрат суб'єкта господарювання.

Однією з найбільш поширених кіберзагроз у сфері бухгалтерського обліку є несанкціонований доступ до облікових систем та баз даних. Отримавши доступ до бухгалтерського програмного забезпечення, зловмисники можуть змінювати реквізити контрагентів, підмінювати банківські рахунки, коригувати суми фінансових операцій, видаляти або фальсифікувати бухгалтерські записи, формувати фіктивні первинні документи чи викривляти фінансову звітність. Особливо високими є ризики для підприємств, які використовують віддалений доступ до облікових систем без належного рівня автентифікації та захисту каналів передачі даних.

Суттєву небезпеку становлять також шкідливі програмні засоби, зокрема віруси-шифрувальники, троянські програми та шпигунське програмне забезпечення, які можуть блокувати доступ до бухгалтерських баз даних, викрадати облікову інформацію або здійснювати приховане втручання в роботу бухгалтерського програмного забезпечення. Особливо небезпечними є атаки ransomware, під час яких зловмисники шифрують бухгалтерські бази даних підприємства та вимагають викуп за відновлення доступу до них. У таких випадках підприємство фактично втрачає можливість здійснювати облікові процедури, формувати звітність та виконувати податкові зобов'язання.

Окремим видом кіберзагроз є соціальна інженерія та фішингові атаки, спрямовані на працівників бухгалтерських служб. Шляхом надсилання підроблених електронних листів, повідомлень або фальшивих запитів від імені керівництва, банків чи державних органів зловмисники отримують логіни, паролі, електронні ключі чи інші засоби доступу до бухгалтерських систем. З огляду на те, що саме бухгалтерські працівники мають доступ до критично важливої фінансової інформації, вони часто стають пріоритетною ціллю кіберзлочинців [2].

Значну загрозу для бухгалтерського обліку становлять також внутрішні кіберризики, пов'язані з діями працівників підприємства. Недостатній розподіл прав доступу, відсутність контролю за змінами в облікових базах, використання спільних облікових записів, неналежне адміністрування інформаційних систем створюють передумови для внутрішніх зловживань, несанкціонованого коригування даних або приховування шахрайських дій. У цифровому середовищі внутрішні порушення часто набувають складнішого характеру, оскільки можуть залишатися непоміченими тривалий час.

Кіберзагрози у бухгалтерському обліку мають комплексний негативний вплив на діяльність підприємства. Передусім вони можуть

спричинити викривлення облікової інформації, що унеможливлює формування достовірної фінансової звітності та призводить до прийняття помилкових управлінських рішень. Крім того, порушення цілісності або доступності бухгалтерських даних може стати причиною невиконання податкових та звітних зобов'язань, застосування штрафних санкцій, блокування господарської діяльності, втрати довіри контрагентів та інвесторів. У разі витоку конфіденційної фінансової інформації підприємство може зазнати також значних репутаційних втрат.

Особливу роль у мінімізації кіберризиків у бухгалтерському обліку відіграє побудова ефективної системи інформаційної безпеки та внутрішнього контролю. Одним із базових заходів є впровадження багаторівневої системи автентифікації користувачів, розмежування прав доступу до облікових модулів та баз даних, ведення журналів дій користувачів і моніторинг змін в облікових системах. Важливим також є забезпечення регулярного резервного копіювання бухгалтерських баз даних та зберігання резервних копій у захищеному середовищі.

Не менш важливим напрямом протидії кіберзагрозам є підвищення цифрової грамотності бухгалтерського персоналу. Регулярне навчання працівників правилам кібергігієни, розпізнаванню фішингових атак, безпечному використанню електронного документообігу та захисту електронних ключів дозволяє суттєво знизити ймовірність людської помилки як одного з основних факторів кіберінцидентів.

У сучасних умовах перспективним напрямом розвитку бухгалтерського обліку є впровадження інтелектуальних систем моніторингу кіберризиків, які використовують алгоритми штучного інтелекту та машинного навчання для виявлення аномальної активності в облікових системах, нетипових транзакцій, підозрілих змін у базах даних та потенційних ознак кібершахрайства. Використання таких технологій дозволяє перейти від реактивної моделі реагування на кіберінциденти до проактивного управління кіберризиками [3].

Отже, цифровізація бухгалтерського обліку, попри значні переваги для автоматизації та підвищення ефективності облікових процесів, одночасно створює новий спектр кіберризиків і кіберзагроз, здатних суттєво впливати на достовірність облікової інформації, фінансову безпеку та безперервність діяльності підприємств. У цих умовах забезпечення кібербезпеки бухгалтерських систем стає невід'ємною складовою сучасної організації бухгалтерського обліку та важливим елементом системи економічної безпеки підприємства. Ефективне управління кіберризиками у сфері бухгалтерського обліку потребує комплексного поєднання технічних, організаційних, кадрових та аналітичних заходів, спрямованих на захист інформаційних ресурсів і забезпечення надійності цифрового облікового середовища.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.04.2026).

2. Accounting Fraud: Definition, Types, Red Flags and Prevention. SearchInform. URL: https://searchinform.com/articles/cybersecurity/cyber-threats/fraud/type/financial-fraud/accounting-fraud/ (дата звернення: 30.04.2026).

3. Romney M. B., Steinbart P. J. Accounting Information Systems. 15th ed. Harlow : Pearson Education. 2023. 816 p.

Тарнавська О.О.,
студентка 4-го курсу бакалаврату
Науковий керівник – **Черкасова С.О.,**
канд. екон. наук, доцент
Національний університет «Одеська політехніка»
м. Одеса

СУТНІСТЬ ТА ОСНОВНІ ПІДХОДИ ЩОДО ВИЗНАЧЕННЯ ПОНЯТТЯ «ВИРОБНИЧІ ЗАПАСИ»

Функціонування підприємств незалежно від форми власності об'єктивно передбачає залучення фінансових, технологічних, трудових і матеріальних ресурсів, без яких стабільна господарська діяльність є неможливою. Ресурси, що не є власністю підприємства, потребують завчасного формування резервів – з метою запобігання виробничим простоям та мінімізації операційних ризиків. Сукупність ресурсів, акумульованих для подальшого використання у господарському процесі та забезпечення його безперервності, в управлінській і обліковій практиці прийнято визначати як запаси.

Серед усіх видів запасів особливе місце посідають виробничі запаси, що характеризуються найбільшою питомою вагою та господарською значущістю. Саме вони формують структуру витрат підприємств різних галузей і видів діяльності. Раціональна організація їх обліку та об'єктивна оцінка безпосередньо позначаються як на ключових показниках фінансово-господарської діяльності суб'єктів господарювання, так і на повноті та достовірності інформації про їхній поточний фінансовий стан.

Слід зазначити, що у сучасній науковій літературі єдиного підходу до трактування категорії «запаси» досі не вироблено. Це пояснюється частим ототожненням зазначеного поняття з його окремими різновидами –