УДК 657.6:004.056

Салямон-Міхєєва Катерина Дмитрівна
кандидат економічних наук, доцент,
доцент кафедри обліку та аудиту
Державний податковий університет
Saliamon-Mikhieieva Kateryna
PhD in Economics, Associate Professor,
Associate Professor of the Department of Accounting and Auditing,
State Financial Control and Analysis
State Tax University
ORCID: 0000-0001-8001-0468

DOI: 10.25313/2617-572X-2026-1-11836

АУДИТ У КОНТЕКСТІ КІБЕРРИЗИКІВ

AUDIT IN THE CONTEXT OF CYBER RISKS

Анотація. *У статті розглянуто актуальну проблему впливу кіберризиків на організацію та методику аудиту фінансової звітності в умовах цифровізації економіки. З огляду на те, що цифрові технології все глибше інтегруються в облікові процеси, питання врахування кіберризиків набуває особливої важливості для забезпечення достовірності фінансової звітності.*

Метою дослідження є обґрунтування теоретичних та методичних підходів до проведення аудиту в умовах зростаючих кіберризиків і розробка практичних рекомендацій щодо інтеграції оцінки кіберзагроз у систему аудиторського ризику. Це передбачає не лише адаптацію існуючих аудиторських методик, але й розроблення нових підходів до аналізу цифрових загроз.

У дослідженні використано сучасні наукові підходи та міжнародні рекомендації професійних організацій, таких як IAASB, а також стандарти ISO/IEC 27001, що стосуються інформаційної безпеки. Методологія дослідження включала аналіз літературних джерел, узагальнення міжнародного досвіду, а також моделювання та апробацію нових аудиторських процедур, спрямованих на виявлення кіберризиків.

За результатами дослідження виявлено основні проблеми інтеграції кіберризиків у систему аудиторського ризику, запропоновано авторську модель включення кіберризиків до процедур оцінки ризику суттєвого викривлення. Визначено перелік додаткових аудиторських процедур, спрямованих на перевірку інформаційної безпеки та ІТ-контролів клієнта, що дозволяє аудитору більш обґрунтовано оцінити ризики суттєвого викривлення в умовах цифровізації.

Перспективи подальших досліджень включають розробку кількісних методів оцінки кіберризиків, а також емпіричний аналіз впливу кіберінцидентів на результати аудиторських перевірок. Окремим напрямом може стати адаптація міжнародних підходів до оцінки кіберризиків з урахуванням національних особливостей аудиторської практики.

Ключові слова: *аудит, кіберризики, аудиторський ризик, інформаційна безпека, ІТ-контролі, цифровізація.*

Summary. *The article addresses the relevant issue of the impact of cyber risks on the organization and methodology of financial statement auditing in the context of economic digitalization. As digital technologies are increasingly integrated into accounting and reporting processes, the consideration of cyber risks becomes critically important for ensuring the reliability and integrity of financial information. Cyber threats, including unauthorized access to data, system failures, and cyberattacks, significantly increase audit risk and require auditors to revise traditional audit approaches.*

The purpose of the study is to substantiate theoretical and methodological approaches to auditing under growing cyber risks and to develop practical recommendations for integrating cyber risk assessment into the overall audit risk model. This involves not only adapting existing audit procedures but also developing new methods for identifying, analyzing, and responding to digital threats affecting financial reporting.

The research is based on modern scientific approaches and international recommendations of professional organizations, including the International Auditing and Assurance Standards Board (IAASB), as well as information security standards such as ISO/IEC 27001. The research methodology includes analysis of scientific literature, generalization of international best practices, modeling, and testing of audit procedures aimed at identifying and assessing cyber risks.

The results of the study identify key problems related to the integration of cyber risks into the audit risk system and propose an author's model for incorporating cyber risks into the assessment of the risk of material misstatement. A set of additional audit procedures focused on evaluating information security and IT controls of the audited entity is defined, enabling auditors to form a more justified assessment of audit risks in the digital environment. Future research perspectives include the development of quantitative methods for cyber risk assessment and empirical analysis of the impact of cyber incidents on audit outcomes.

Key words: *audit, cyber risks, audit risk, information security, IT controls, digitalization.*

Постановка проблеми. Активна цифровізація бізнес-процесів, впровадження хмарних технологій, автоматизованих облікових систем та віддалених форм доступу до фінансової інформації істотно підвищили залежність підприємств від інформаційних технологій. Паралельно з цим зросла кількість та складність кіберінцидентів, які здатні спричиняти втрату, викривлення або несанкціоновану зміну фінансових даних. У таких умовах кіберризики стають суттєвим фактором, що впливає на достовірність фінансової звітності та, відповідно, на якість аудиторських висновків.

Традиційна методологія аудиту ґрунтується на оцінці аудиторського ризику, який включає властивий ризик, ризик контролю та ризик невиявлення. Однак у класичному підході ризики, пов'язані з кіберзагрозами, часто розглядаються фрагментально або опосередковано — як складова IT-середовища клієнта, без належної формалізації їх впливу на фінансову звітність. Це призводить до ситуації, коли значні кіберзагрози залишаються поза межами системної оцінки аудитором. Зазначена проблема має важливе практичне значення, оскільки від адекватності врахування кіберризиків залежить обґрунтованість аудиторського висновку та рівень довіри користувачів фінансової звітності. Водночас вона є актуальною і з наукової точки зору, оскільки потребує розвитку теоретичних положень аудиту шляхом адаптації його концепцій до умов цифрової економіки.

Аналіз останніх досліджень і публікацій. Проблеми впливу цифровізації, IT-ризиків та кіберзагроз на аудиторську діяльність досліджуються у працях зарубіжних науковців і професійних організацій. Зокрема, у роботах M.A. Vasarhelyi, D. Alles, A. Kogan розглядається трансформація аудиту в умовах цифрової економіки, застосування безперервного аудиту та аналітики даних, при цьому наголошується на зростанні ризиків, пов'язаних з надійністю та безпекою інформаційних систем [1].

Безпосередній зв'язок між цифровими ризиками та якістю аудиту досліджують H. Brown-Liburd та J. Hammersley, які у своїх працях обґрунтовують необхідність врахування технологічних і кіберризиків під час оцінки аудиторського ризику та планування аудиторських процедур. Питання впливу кіберінцидентів на фінансову звітність і аудиторські рішення також порушуються у дослідженнях K. Raman, J. Singh та A. Kumar, де кіберризики розглядаються як фактор ризику суттєвого викривлення [3; 4].

Окремий напрям становлять дослідження, присвячені IT-аудиту та внутрішнім контролям інформаційних систем. У працях R. Moeller висвітлюються питання управління IT-ризиками та контролю інформаційних систем, однак без системної інтеграції кіберризиків у класичну модель аудиторського ризику фінансової звітності [6].

Важливу роль у розвитку практичних підходів до врахування кіберризиків відіграють рекомендації професійних організацій, зокрема IAASB, IFAC та AICPA, які акцентують увагу на необхідності оцінки кіберзагроз при розумінні середовища суб'єкта господарювання та його системи внутрішнього контролю. Водночас зазначені документи мають переважно рекомендаційний характер і не пропонують уніфікованої методики включення кіберризиків до системи аудиторського ризику.

В українських наукових публікаціях увага зосереджується переважно на цифровізації обліку та розвитку IT-аудиту, тоді як комплексні дослідження аудиту в умовах кіберризиків залишаються обмеженими.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування теоретичних та методичних підходів до проведення аудиту в умовах кіберризиків та розробка практичних рекомендацій щодо інтеграції оцінки кіберзагроз у систему аудиторського ризику.

Для досягнення поставленої мети в статті передбачено вирішення таких завдань:
- уточнити сутність кіберризиків у контексті аудиторської діяльності;
- визначити основні види кіберризиків, що впливають на достовірність фінансової звітності;
- проаналізувати вплив кіберризиків на етапи аудиторського процесу;
- інтегрувати модель включення кіберризиків до оцінки аудиторського ризику;
- запропонувати напрями вдосконалення аудиторських процедур в умовах цифрових загроз.

Виклад основного матеріалу дослідження. У сучасних умовах цифровізації економіки кіберри-

зики стають одним із ключових факторів, що впливають на достовірність фінансової звітності та якість аудиторських висновків. У контексті аудиторської діяльності кіберризики доцільно розглядати як ймовірність виникнення подій, пов'язаних із порушенням конфіденційності, цілісності або доступності інформаційних ресурсів, які можуть призвести до суттєвих викривлень фінансової інформації або обмежити можливість аудитора отримати достатні та належні аудиторські докази.

На відміну від традиційних ризиків, кіберризики мають системний і латентний характер, оскільки їх наслідки можуть не проявлятися негайно у фінансовій звітності, а виявлятися лише на етапі аудиторської перевірки або після настання кіберінциденту. Це зумовлює необхідність їх інтеграції в процес оцінки аудиторського ризику на ранніх етапах аудиту, відповідно до підходів, рекомендованих IAASB [7].

З урахуванням специфіки аудиторської діяльності кіберризики доцільно розглядати як багатокомпонентну сукупність загроз, що формуються під впливом як технічних, так і організаційних чинників та мають різноспрямований вплив на процес формування фінансової звітності. Однією з найбільш поширених груп є ризики несанкціонованого доступу до фінансової інформації, які виникають у разі недоліків у системі контролю доступу до облікових та управлінських інформаційних систем. Такі ризики можуть призводити до навмисної або ненавмисної зміни бухгалтерських записів, спотворення первинних документів, а також до фальсифікації фінансової звітності, що безпосередньо впливає на достовірність аудиторських доказів.

Не менш суттєвими є ризики порушення цілісності даних, які пов'язані з можливістю некоректної обробки, втрати або несанкціонованої модифікації облікової інформації. Причинами таких ризиків можуть бути як кібератаки та збої програмного забезпечення, так і відсутність належного контролю за внесенням змін до інформаційних систем. У результаті фінансова інформація може не відображати реальний фінансовий стан підприємства, що ускладнює оцінку ризиків суттєвого викривлення на рівні тверджень фінансової звітності.

Окрему групу становлять ризики втрати доступності інформаційних ресурсів, які проявляються через збої в роботі IT-систем, кібератаки типу DDoS (Distributed Denial of Service) або неналежну організацію процесів резервного копіювання та відновлення даних. Такі ризики мають не лише фінансові, а й процедурні наслідки, оскільки можуть унеможливити своєчасне виконання аудиторських процедур, обмежити доступ аудитора до необхідної інформації та негативно вплинути на дотримання строків проведення аудиту.

Важливе місце у структурі кіберризиків посідають ризики, пов'язані з людським фактором. Вони охоплюють помилки персоналу, недостатній рівень кіберобізнаності працівників, а також зловживання службовими повноваженнями та внутрішні загрози. Особливістю цієї групи ризиків є їх складність для ідентифікації за допомогою традиційних аудиторських методів, оскільки вони часто маскуються під звичайні операційні помилки або неформальні управлінські практики.

Зростаючого значення в умовах цифровізації набувають ризики, пов'язані з використанням сторонніх IT-послуг, зокрема хмарних сервісів та аутсорсингових IT-провайдерів. У таких умовах відповідальність за збереження та захист фінансової інформації частково передається третім сторонам, що ускладнює процес отримання аудиторських доказів щодо надійності та безпеки інформаційних систем клієнта та підвищує залежність аудитора від зовнішніх джерел інформації.

Загальною передумовою реалізації зазначених ризиків є ризики недостатньої ефективності IT-контролів, які проявляються у формальному або неефективному функціонуванні процедур інформаційної безпеки. Такі недоліки суперечать вимогам міжнародних стандартів, зокрема ISO (ISO/IEC 27001), і призводять до підвищення ризику суттєвих викривлень фінансової інформації. У сукупності це свідчить про необхідність комплексного підходу до ідентифікації та оцінки кіберризиків у процесі аудиту фінансової звітності [10].

Кіберризики істотно впливають на всі етапи аудиторського процесу, змінюючи як зміст, так і методологію проведення аудиту фінансової звітності. Їх вплив зумовлений тим, що формування, обробка та зберігання фінансової інформації дедалі більше відбуваються в автоматизованому інформаційному середовищі, уразливому до несанкціонованого доступу, порушення цілісності даних і втрати доступності інформаційних ресурсів. У таких умовах аудиторський процес виходить за межі традиційної перевірки фінансових показників і потребує комплексної оцінки цифрового середовища підприємства.

На етапі планування аудиту вплив кіберризиків проявляється у необхідності поглибленого аналізу IT-інфраструктури клієнта та ідентифікації потенційних джерел цифрових загроз. Аудитор повинен оцінити, якою мірою ризики несанкціонованого доступу, порушення цілісності даних або залежність від сторонніх IT-провайдерів можуть призвести до суттєвих викривлень фінансової звітності. Виявлення підвищеного рівня кіберризиків зумовлює перегляд загальної аудиторської стратегії, зокрема визначення характеру, часу та обсягу аудиторських процедур, а також рівня професійного скептицизму, що відповідає підходам, рекомендованим IAASB [7].

Під час оцінки системи внутрішнього контролю кіберризики фокусують увагу аудитора на ефективності IT-контролів, які забезпечують конфіденційність, цілісність і доступність фінансової інформації.

Недостатній контроль доступу до облікових систем, формальний характер процедур управління змінами або відсутність належного резервного копіювання підвищують ризик контролю та знижують можливість аудитора покладатися на внутрішній контроль клієнта. У таких умовах традиційні підходи до тестування контролів потребують доповнення аналізом цифрових слідів, логів операцій та механізмів інформаційної безпеки.

На етапі виконання аудиторських процедур кіберризики зумовлюють необхідність адаптації методів отримання аудиторських доказів. Ризики порушення цілісності даних або втрати доступності інформаційних ресурсів можуть обмежити можливість використання первинних електронних документів і журналів операцій, що змушує аудитора застосовувати альтернативні процедури або розширювати обсяг перевірки. Крім того, наявність ризиків, пов'язаних із людським фактором або сторонніми IT-послугами, підвищує значущість аналітичних процедур, використання інструментів аналізу даних і залучення IT-експертів для оцінки надійності інформаційних систем.

Особливий вплив кіберризики мають на процес отримання достатніх і належних аудиторських доказів. Порушення доступності або цілісності фінансової інформації ускладнює підтвердження тверджень фінансової звітності та підвищує ризик невиявлення. У таких випадках аудитор змушений переглядати оцінку аудиторського ризику та коригувати аудиторські процедури з метою зниження ймовірності формування необґрунтованого аудиторського висновку.

Кіберризики також впливають на формування професійного судження аудитора, підвищуючи роль професійного скептицизму та критичної оцінки інформації, наданої управлінським персоналом. Наявність внутрішніх загроз або недоліків IT-контролів може свідчити не лише про технічні проблеми, а й про загальну слабкість системи корпоративного управління, що потребує належного відображення у результатах аудиту.

На завершальному етапі аудиту кіберризики можуть впливати на характер аудиторського висновку та комунікацію з управлінським персоналом. Виявлення суттєвих недоліків у системі інформаційної безпеки або контролях, пов'язаних із фінансовою звітністю, зумовлює необхідність інформування осіб, наділених управлінськими повноваженнями, та надання рекомендацій щодо усунення виявлених ризиків.

Узагальнюючи, вплив кіберризиків на аудиторський процес проявляється у трансформації підходів до планування, виконання та оцінки результатів аудиту. Це обумовлює потребу в інтеграції питань кібербезпеки у методологію аудиту та формує нові вимоги до професійних компетенцій аудитора в умовах цифрової економіки.

Зростання ролі цифрових технологій зумовлює необхідність перегляду традиційних підходів до оцінки аудиторського ризику. Класична модель аудиторського ризику, що базується на взаємозв'язку властивого ризику, ризику контролю та ризику невиявлення, не повною мірою відображає специфіку цифрового середовища, у якому значна частина фінансової інформації формується автоматизовано та є вразливою до кіберзагроз. У зв'язку з цим у статті пропонується розглядати кіберризики як окремий аналітичний компонент, що впливає насамперед на величину властивого ризику та ризику контролю.

Інтеграція кіберризиків у систему аудиторського ризику передбачає доповнення традиційної схеми оцінки аудиторського ризику етапом ідентифікації та оцінки кіберризиків, який здійснюється на початкових стадіях аудиту. На цьому етапі аудитор аналізує цифрове середовище підприємства, визначає ключові джерела кіберзагроз, оцінює ступінь залежності фінансової звітності від інформаційних систем та ідентифікує потенційні канали впливу кіберінцидентів на достовірність облікових даних.

У межах запропонованої моделі кіберризики безпосередньо підвищують властивий ризик, оскільки автоматизовані облікові системи, використання хмарних сервісів та інтеграція різних інформаційних платформ збільшують складність облікових процесів і ймовірність суттєвих викривлень фінансової інформації ще до врахування дії внутрішнього контролю. Високий рівень кіберризиків свідчить про підвищену вразливість фінансової звітності до помилок або шахрайства, навіть за відсутності навмисних порушень з боку персоналу.

Одночасно кіберризики істотно впливають на ризик контролю, оскільки ефективність системи внутрішнього контролю в цифровому середовищі значною мірою залежить від надійності IT-контролів та процедур інформаційної безпеки. Недоліки у контролі доступу, управлінні змінами, резервному копіюванні або моніторингу подій безпеки знижують здатність внутрішнього контролю своєчасно запобігати або виявляти суттєві викривлення фінансової інформації. Таким чином, високий рівень кіберризиків обґрунтовує підвищену оцінку ризику контролю, навіть за формальної наявності внутрішніх регламентів і політик безпеки.

З урахуванням підвищеного властивого ризику та ризику контролю відбувається коригування ризику невиявлення, який визначає допустимий рівень імовірності того, що аудиторські процедури не виявлять існуючі суттєві викривлення. У запропонованій моделі зростання кіберризиків зумовлює необхідність зниження ризику невиявлення шляхом розширення обсягу аудиторських процедур, застосування більш детальних тестів та використання спеціалізованих методів перевірки інформаційних систем.

Описово запропоновану модель інтеграції кіберризиків у систему аудиторського ризику можна представити таким чином: кіберризики розгляда-

ються як чинник, що безпосередньо впливає на величину властивого ризику та ризику контролю, що, у свою чергу, зумовлює необхідність коригування допустимого рівня ризику невиявлення і відповідного модифікування характеру, часу та обсягу аудиторських процедур. Такий підхід забезпечує чіткий причинно-наслідковий зв'язок між цифровими загрозами та професійними рішеннями аудитора на етапах планування і виконання аудиту фінансової звітності.

Застосування такої моделі дозволяє аудитору більш адекватно визначити характер, час і обсяг аудиторських процедур, зосередивши увагу на найбільш уразливих ділянках формування фінансової звітності. Крім того, інтеграція кіберризиків у систему аудиторського ризику сприяє підвищенню обґрунтованості професійного судження аудитора та якості аудиторського висновку в умовах зростаючих цифрових загроз.

У контексті дослідження пропонується вдосконалити аудиторські процедури шляхом їх цілеспрямованої адаптації до умов зростаючих кіберризиків. Зокрема, традиційні процедури доцільно доповнювати оцінкою політик інформаційної безпеки підприємства з урахуванням їх фактичного застосування в облікових процесах, а також перевіркою ефективності контролів доступу до облікових систем. Такий підхід дозволяє більш обґрунтовано оцінити рівень властивого ризику та ризику контролю в цифровому середовищі.

З метою зниження ризику невиявлення суттєвих викривлень пропонується використовувати аналіз журналів подій і змін у базах даних як окрему аудиторську процедуру. Систематичне дослідження логів доступу та історії змін у ключових облікових даних дає змогу виявляти нетипові операції та приховані викривлення, які не завжди фіксуються в традиційній бухгалтерській документації.

Крім того, у випадках застосування складних або інтегрованих інформаційних систем доцільним є залучення IT-фахівців та розширене використання аналітичних процедур для виявлення аномалій у масивах фінансових даних. Запропонований комплекс процедур сприяє підвищенню якості аудиту та забезпечує зниження ризику невиявлення суттєвих викривлень у фінансовій звітності в умовах цифрових загроз [13].

У результаті проведеного дослідження встановлено, що кіберризики є невід'ємною складовою сучасного аудиторського середовища та суттєво впливають на достовірність фінансової звітності й якість аудиторських висновків. Обґрунтовано, що в умовах цифровізації традиційні підходи до аудиту є недостатніми та потребують адаптації шляхом системної інтеграції оцінки кіберризиків у модель аудиторського ризику, з урахуванням їх впливу на властивий ризик, ризик контролю та ризик невиявлення.

Практичне значення отриманих результатів полягає у можливості використання запропонованої авторської моделі інтеграції кіберризиків і рекомендацій щодо вдосконалення аудиторських процедур під час планування та проведення аудиту фінансової звітності. Їх застосування сприяє підвищенню обґрунтованості професійного судження аудитора, зниженню ризику невиявлення суттєвих викривлень та адаптації аудиторського процесу до умов цифрових загроз.

Перспективи подальших досліджень пов'язані з розробленням кількісних методів оцінки кіберризиків у системі аудиторського ризику, а також з проведенням емпіричного аналізу впливу кіберінцидентів на результати аудиторських перевірок і якість аудиторських висновків. Окремим напрямом подальших наукових пошуків може стати адаптація міжнародних підходів до оцінки кіберризиків з урахуванням національних особливостей аудиторської практики.

Література

1. Vasarhelyi M. A., Alles M. G., Kogan A. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*. 2004. Vol. 1. P. 1–21.

2. Vasarhelyi M. A., Kogan A., Tuttle B. M. Big data in accounting: An overview. *Accounting Horizons*. 2015. Vol. 29, № 2. P. 381–396.

3. Brown-Liburd H., Issa H., Lombardi D. Behavioral implications of Big Data's impact on audit judgment and decision making. *Accounting Horizons*. 2015. Vol. 29, № 2. P. 451–468.

4. Hammersley J. S., Myers L. A., Sheng X. Market perceptions of audit quality following cyber incidents. *Journal of Accounting and Public Policy*. 2018. Vol. 37, № 6. P. 491–509.

5. Raman K., Singh J., Kumar A. Cyber risk and financial reporting reliability. *International Journal of Accounting Information Systems*. 2019. Vol. 34. P. 1–15.

6. Moeller R. R. IT Audit, Control, and Assurance. 4th ed. Hoboken: John Wiley & Sons, 2019. 624 p.

7. International Auditing and Assurance Standards Board. The consideration of cybersecurity risks in an audit of financial statements. New York: IAASB, 2021. 15 p.

8. International Federation of Accountants. Technology and the future-ready profession. New York: IFAC, 2020. 28 p.

9. American Institute of Certified Public Accountants. SOC for Cybersecurity: A practitioner's guide. New York: AICPA, 2018. 42 p.

10. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022.

11. ISACA. Auditing cybersecurity: Risk-based approach. Rolling Meadows: ISACA, 2021. 36 p.

12. Куцик П. О., Жук В. М. Цифровізація обліку та аудиту: виклики та перспективи розвитку. *Облік і фінанси*. 2021. № 4. С. 15–22.

13. Салямон-Міхєєва К. Д., Краєвський В. М. Контроль якості аудиторських послуг у контексті цифрової трансформації бізнесу. *Український економічний часопис*. 2025. Вип. 11. С. 89–93.

References

1. Vasarhelyi, M. A., Alles, M. G. and Kogan, A. (2004), "Principles of analytic monitoring for continuous assurance", Journal of Emerging Technologies in Accounting, vol. 1, pp. 1–21.

2. Vasarhelyi, M. A., Kogan, A. and Tuttle, B. M. (2015), "Big data in accounting: An overview", Accounting Horizons, vol. 29, no. 2, pp. 381–396.

3. Brown-Liburd, H., Issa, H. and Lombardi, D. (2015), "Behavioral implications of Big Data's impact on audit judgment and decision making", Accounting Horizons, vol. 29, no. 2, pp. 451–468.

4. Hammersley, J. S., Myers, L. A. and Sheng, X. (2018), "Market perceptions of audit quality following cyber incidents", Journal of Accounting and Public Policy, vol. 37, no. 6, pp. 491–509.

5. Raman, K., Singh, J. and Kumar, A. (2019), "Cyber risk and financial reporting reliability", International Journal of Accounting Information Systems, vol. 34, pp. 1–15.

6. Moeller, R. R. (2019), IT Audit, Control, and Assurance, 4th ed, John Wiley & Sons, Hoboken, USA.

7. International Auditing and Assurance Standards Board (2021), The consideration of cybersecurity risks in an audit of financial statements, IAASB, New York, USA.

8. International Federation of Accountants (2020), Technology and the future-ready profession, IFAC, New York, USA.

9. American Institute of Certified Public Accountants (2018), SOC for Cybersecurity: A practitioner's guide, AICPA, New York, USA.

10. International Organization for Standardization (2022), ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO, Geneva, Switzerland.

11. ISACA (2021), Auditing cybersecurity: Risk-based approach, ISACA, Rolling Meadows, USA.

12. Kutsyk, P. O. and Zhuk, V. M. (2021), "Digitalization of accounting and auditing: challenges and development prospects", Oblik i finansy, no. 4, pp. 15–22.

13. Saliamon-Mikhieieva, K. D. and Kraievskyi, V. M. (2025), "Audit quality control in the context of digital transformation of business", Ukrainskyi ekonomichnyi chasopys, vol. 11, pp. 89–93.

Дата першого надходження статті до видання: 02.01.2026
Дата прийняття статті до друку після рецензування: 22.01.2026
Дата публікації: 31.01.2026