Миханчук Наталія
студентка,
науковий керівник: Ярощук Олексій
кандидат економічних наук, доцент
Західноукраїнський національний університет

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВНУТРІШНІЙ АУДИТ ЦИФРОВИХ ОБЛІКОВИХ СИСТЕМ

Цифровізація облікових процесів підприємств і організацій спричинила глибокі зміни у структурі, функціонуванні та взаємозв'язках систем бухгалтерського обліку. В умовах активного використання корпоративних інформаційних систем (ERP), хмарних технологій, мобільних додатків і аналітичних платформ постає необхідність забезпечення високого рівня інформаційної безпеки цифрового облікового середовища. Забезпечення цілісності, конфіденційності та доступності облікової інформації стає критичним завданням для збереження довіри користувачів фінансової звітності, захисту активів підприємства та запобігання кіберризикам.

Цифрове облікове середовище охоплює комплекс автоматизованих засобів, які здійснюють збір, обробку, передачу, зберігання та архівування фінансових та управлінських даних. У цьому контексті аудит інформаційної безпеки є інструментом незалежної оцінки стану захищеності інформаційних систем, адекватності застосованих заходів контролю, надійності механізмів автентифікації та авторизації, відповідності нормативно-правовим вимогам і внутрішнім політикам підприємства. Систематичний аудит цифрового середовища дозволяє ідентифікувати вразливості, запровадити процедури реагування на інциденти, розробити політики резервного копіювання та захисту від несанкціонованого доступу.

Важливу роль у забезпеченні інформаційної безпеки відіграють внутрішній контроль, стандарти кіберзахисту (ISO/IEC 27001, NIST, COBIT), технології шифрування, багатофакторна аутентифікація, мережеві екрани, протоколи виявлення вторгнень та інструменти журналювання дій користувачів. У цифровому обліковому середовищі ці елементи повинні інтегруватися у модулі фінансового обліку, документообігу, казначейських операцій і внутрішнього аудиту. При цьому аудит IT-середовища не обмежується технічною оцінкою – він включає в себе аналіз ризиків інформаційних потоків, доступів до

конфіденційних даних, безпеки інтерфейсів API, політик паролів, надійності хмарних сервісів та відповідності персоналу політикам інформаційної безпеки.

Упровадження автоматизованих систем контролю доступу, інтелектуального аналізу подій (SIEM), інструментів оцінки відповідності (compliance check) забезпечує можливість моніторингу подій у режимі реального часу, що, у свою чергу, сприяє підвищенню якості внутрішнього контролю та аудиту. У перспективі, синергія між цифровими технологіями та аудиторськими підходами дає можливість створення самонавчальних систем аудиту на базі штучного інтелекту, що дозволяє оперативно реагувати на порушення в режимі онлайн, виявляти аномалії в облікових записах та підвищити точність аудиторських висновків.

Таким чином, інформаційна безпека є невід'ємною складовою цифрового облікового середовища, а аудит – ключовим механізмом забезпечення її ефективності. Забезпечення цілісності цифрової облікової інфраструктури потребує комплексного підходу, що охоплює як технологічні, так і організаційні аспекти. Подальші дослідження доцільно спрямувати на розробку методології оцінювання зрілості інформаційної безпеки в облікових системах, побудову моделей управління кіберризиками в обліковому середовищі та створення цифрових профілів аудиторської надійності.

Список використаних джерел

1. Ярощук О. В. Ризик-менеджмент в управлінні капіталом підприємства. Економічний аналіз. 2012. Т. 11, № 1. С. 460–466.

2. Ярощук О. Системна оцінка стійкості функціонування підприємств. Наука молода. 2008. № 10. С. 197-205.

3. Ярощук О., Белова І. Технологія блокчейн в бухгалтерському обліку та аудиті. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. 2020. Випуск 3-4. С. 28-44. DOI: https://doi.org/10.35774/ibo2020.03.028

4. Belova I., Homotiuk A., Yaroshchuk O. Digital transformation of managerial and business processes in Ukraine during martial law. Ekonomichnyy analiz. 2024. Vol. 34, No. 1. P. 42–52.

5. Belova I., Yaroshchuk O., Homotiuk A. Development of digitalization processes in the European Union: prospective experience for Ukraine. Ekonomichnyy analiz. 2023. Vol. 33, No. 1. P. 180-191.

6. ISACA. COBIT 2019 Framework: Introduction and Methodology. ISACA, 2019.

7. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. International Organization for Standardization.

8. Laudon K. C., Laudon J. P. Management Information Systems: Managing the Digital Firm. 16th Ed. Pearson, 2020.

9. Kranacher M.-J., Riley R., Wells J. Forensic Accounting and Fraud Examination. Wiley, 2020.