WayScience

International Scientific and Practical Internet Conference

«Development of Education, Science and Business: Results 2025»

ISBN 978-617-8293-60-4

WayScience

International Scientific and Practical Internet Conference

«Development of Education, Science and Business: Results 2025»

ISBN 978-617-8293-60-4

РОЛЬ КІБЕРБЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ НАДІЙНОСТІ ОБЛІКОВОЇ СИСТЕМИ НА МАЛИХ ПІДПРИЄМСТВАХ В УМОВАХ ЦИФРОВІЗАЦІЇ

Бойко С.О.

Науковий керівник: Фартушняк О.В.
кандидат економічних наук, доцент
E-mail: soffetsoffit@gmail.com
Харківський національний економічний університет імені Семена Кузнеця
м. Харків

На сучасному етапі цифрової трансформації економіки малі підприємства стикаються з новими викликами в сфері бухгалтерського обліку, пов'язаними з кіберзагрозами. Облікова інформація (конфіденційні фінансові дані малого бізнесу) стає об'єктом кібератак, що може призвести до спотворення звітності, фінансових втрат та втрати довіри клієнтів і партнерів. Забезпечення кібербезпеки облікових систем є ключовим фактором для збереження цілісності, конфіденційності та доступності даних. Це безпосередньо впливає на стабільність і ефективність ведення бізнесу на малих підприємствах [1, с. 12]. Для малого бізнесу кіберзагрози становлять особливу небезпеку, оскільки відсутність спеціалізованих IT-відділів робить системи більш вразливими.

Актуальність теми зумовлена зростанням кількості кіберінцидентів у сфері економічних наук, зокрема в бухгалтерському обліку малого бізнесу. За даними досліджень, кіберзагрози, такі як фішинг, ransomware та несанкціонований доступ, становлять значний ризик для облікових баз даних. У малих підприємствах, де часто використовуються хмарні сервіси або прості онлайн-інструменти, ці загрози можуть призвести до повного паралічу діяльності. Саме з цією метою розглядається роль заходів кібербезпеки в інтеграції з процесами обліку для мінімізації ризиків, з урахуванням специфіки малого бізнесу.

Основні аспекти забезпечення кібербезпеки в бухгалтерському обліку на малих підприємствах:

1. Класифікація кіберризиків на внутрішні (помилки персоналу, недостатній контроль доступу, використання слабких паролів) та зовнішні (кібератаки, віруси, DDoS (distributed denial of service) атаки), що впливають на достовірність облікової інформації [2, с. 61]. Для малого бізнесу внутрішні ризики часто переважають через обмежену кількість співробітників, де один працівник може мати доступ до всієї бази даних.

2. Застосування технологій захисту, таких як шифрування даних, багатофакторна аутентифікація, регулярні резервні копії та використання хмарних рішень з вбудованим захистом. Важливо обирати доступні інструменти, як антивірусне ПЗ з автоматичними оновленнями та фаєрволи, які не вимагають значних інвестицій.

3. Інтеграція кібербезпеки в повсякденні облікові процедури, оцінка вразливостей систем обліку та моніторинг ризиків у реальному часі. Для малого бізнесу це може включати використання безкоштовних або недорогих інструментів сканування, як OpenVAS, для виявлення слабких місць.

4. Використання блокчейн-технології для забезпечення незмінності облікових записів та автоматизованого контролю [3, с. 125]. У контексті малого бізнесу блокчейн може застосовуватися для простих транзакцій, наприклад, у ланцюгах постачань.

5. Навчання персоналу для підвищення обізнаності бухгалтерів щодо кібергігієни для запобігання соціальної інженерії. На малих підприємствах це особливо актуально, оскільки власники часто самі ведуть облік, і прості тренінги (онлайн-курси від навчальних платформ та українських ресурсів) можуть значно знизити ризики.

Технологічні аспекти реалізації. Забезпечення кібербезпеки на малих підприємствах реалізується через комплексний підхід, включаючи впровадження стандартів ISO 27001 (адаптованих для малого бізнесу), регулярне оновлення програмного забезпечення облікових систем та інтеграцію інструментів моніторингу. Головна особливість – поєднання традиційного внутрішнього контролю з кіберзахистом, що дозволяє виявляти аномалії в облікових операціях у реальному часі та запобігати маніпуляціям даними. Для малого бізнесу в Україні доступні облікові програми, які інтегрують елементи захисту: наприклад, Dilovod – онлайн-сервіс для управлінського та бухгалтерського обліку з вбудованим шифруванням і багатофакторною аутентифікацією; BookKeeper – українська хмарна бухгалтерія з автоматичними резервними копіями та моніторингом доступу; Finmap – інструмент для фінансового обліку з фокусом на мобільність і захист даних у хмарі; Облік SaaS – платформа для малого бізнесу з інтеграцією електронного документообігу та базовим кіберзахистом; M.E.Doc – для електронної звітності з елементами шифрування документів. Ці програми дозволяють малим підприємствам уникнути дорогих кастомних рішень та забезпечують захист інформації через хмарні технології, де дані зберігаються на захищених серверах з регулярними перевірками рівня інформаційної безпеки. Наприклад, у Dilovod дані шифруються за стандартом AES-256, а доступ контролюється ролями користувачів, що мінімізує ризики внутрішніх витоків. Аналогічно, BookKeeper пропонує інтеграцію з двофакторною аутентифікацією (2FA) та є простим і ефективним для малого бізнесу. Для захисту інформації рекомендується: регулярне оновлення ПЗ для закриття вразливостей, використання VPN для віддаленого доступу, впровадження політики паролів (мінімум 12 символів з комбінацією букв, цифр і символів) та моніторинг логів активності. У разі використання хмарних сервісів, як у Finmap, важливо обирати провайдерів з сертифікацією GDPR або аналогічними стандартами, щоб забезпечити конфіденційність даних клієнтів.[4]

Основними перевагами інтеграції кібербезпеки є:

- підвищення достовірності фінансової звітності через запобігання спотворенням даних;
- зниження ризиків фінансових втрат від кіберінцидентів;
- посилення ефективності обліку через автоматизацію перевірок і зменшення часу на рутинні завдання;
- покращення конкурентоспроможності за рахунок довіри партнерів, оскільки захищені системи свідчать про надійність підприємства;
- економія ресурсів, оскільки превентивні заходи дешевші, ніж відновлення після атаки (за даними досліджень, середня вартість кіберінциденту для малого бізнесу в Україні становить понад 100 тис. грн).

Перспективи розвитку. У майбутньому планується розширення використання штучного інтелекту для прогнозування кіберзагроз на малих підприємствах, впровадження блокчейну в повсякденний облік для забезпечення прозорості транзакцій та розробка національних стандартів кібербезпеки в Україні, адаптованих для малого бізнесу. Також розглядається співпраця з міжнародними організаціями (наприклад, ISACA) для адаптації найкращих практик до українського бізнес-середовища. У контексті України перспективним є розвиток локальних хмарних платформ, як розширення Dilovod чи Finmap, з інтеграцією AI для автоматичного виявлення фішингу. Крім того, державні ініціативи, як програма "Дія.Бізнес", можуть включати модулі кібербезпеки для облікових систем.

Таким чином, інтеграція кібербезпеки в бухгалтерський облік на малих підприємствах сприятиме підвищенню надійності фінансової інформації, мінімізації ризиків у цифровій економіці та конкурентоспроможності бізнесу.

Список літератури:

1. Муравський В. Класифікація кіберризиків у бухгалтерському обліку // Вісник Економіки. – 2021. – № 3. – С. 45-56.

2. Деньга С.М., Верига Ю.О. Захист інформації в комп'ютерних інформаційних системах бухгалтерського обліку // Бухгалтерський облік і аудит. – 2004. – № 5. – С. 59-65.

3. Ярощук Т. Технологія блокчейн в бухгалтерському обліку та аудиті // Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. – 2021. – № 3-4. – С. 120-130.

4. Огляд українських облікових програм для малого бізнесу // Finacademy.net, 2024. [Електронний ресурс]. – Режим доступу: https://finacademy.net/ua/materials/article/perehodimo-na-ukrayinske.