СУЧАСНІ ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БУХГАЛТЕРСЬКОМУ ОБЛІКУ

Дмитро Олександрович ФЕДЕНКО,

аспірант кафедри бухгалтерського обліку та консалтингу факультету обліку та податкового менеджменту Київського національного економічного університету ім. Вадима Гетьмана
https://orcid.org/0009-0008-6802-7038

Інформаційна безпека в сучасному бізнес-середовищі стала однією з найважливіших складових успішності будь-якої організації. Бухгалтерський облік, як одна з ключових функцій в управлінні фінансами підприємства, не є винятком. Забезпечення інформаційної безпеки в бухгалтерському обліку має величезне значення для збереження конфіденційності, цілісності та доступності фінансової інформації. В даному звіті ми розглянемо сучасні теоретико-методологічні підходи до забезпечення інформаційної безпеки в бухгалтерському обліку та їх вплив на практику бухгалтерського обліку сьогодні.

Інформаційна безпека в бухгалтерському обліку передбачає застосування різних теоретичних підходів і методологій для забезпечення безпеки фінансової інформації. Один із найважливіших аспектів цього процесу - це конфіденційність інформації, що зберігається та обробляється в бухгалтерському обліку. Методології шифрування та захисту даних, такі як методологія "за замовчуванням" (by default), грають ключову роль у забезпеченні конфіденційності фінансових даних.

Теоретичні засади інформаційної безпеки в бухгалтерському обліку є важливою основою для розуміння та реалізації заходів з захисту фінансової інформації в організаціях. Ці засади визначають принципи, концепції та методи, на яких ґрунтується побудова системи інформаційної безпеки в бухгалтерському обліку. Ось кілька ключових теоретичних засад:

1. Конфіденційність: ця засада визначає необхідність забезпечення конфіденційності фінансової інформації. Значення полягає в тому, щоб лише авторизовані користувачі мали доступ до конфіденційної інформації. Це досягається за допомогою різних методів, таких як шифрування даних, контроль доступу та обмеження привілеїв користувачів.

2. Цілісність: ця засада підкреслює важливість збереження цілісності фінансової інформації. Іншими словами, дані не повинні бути змінені безпідставно. Використання цифрових підписів та систем контролю змін допомагають досягти цієї цілі.

3. Доступність: ця засада вказує на необхідність забезпечення доступності фінансової інформації тим, хто має на неї право. Організація повинна бути готовою до запобігання, виявлення та відновлення від інцидентів, що можуть призвести до втрати доступу до даних.

4. Аутентифікація та авторизація: ці засади передбачають перевірку ідентифікації користувача (аутентифікацію) та призначення прав доступу (авторизацію) на основі ролей та відповідальностей. Це допомагає уникнути несанкціонованого доступу до інформації.

5. Моніторинг та аудит: система інформаційної безпеки повинна включати засади моніторингу та аудиту, щоб виявляти та реагувати на можливі загрози та інциденти безпеки. Аудит дозволяє відстежувати дії користувачів та реагувати на підозрілі активності.

6. Захист від загроз і ризиків: засада захисту від загроз та ризиків полягає в ідентифікації потенційних загроз і ризиків і впровадженні відповідних заходів для їх запобігання та зменшення.

7. Стратегія інформаційної безпеки: стратегія інформаційної безпеки визначає загальний план дій та підходи організації до забезпечення інформаційної безпеки в бухгалтерському обліку. Ця стратегія має бути відповідною до потреб та характеру організації.

8. Освіта та навчання: засада освіти та навчання передбачає інформування та навчання персоналу щодо правил і процедур інформаційної безпеки. Важливо, щоб всі співробітники були обізнані з основами інформаційної безпеки та відомі ризики та загрози.

Ці теоретичні засади є фундаментом для розробки імплементації системи інформаційної безпеки в бухгалтерському обліку та допомагають забезпечити захист фінансової інформації в сучасному бізнес-середовищі [1].

Сучасні організації все частіше використовують інтегровані системи бухгалтерського обліку та управління, що робить їх більш вразливими перед можливими загрозами. Забезпечення інформаційної безпеки вимагає впровадження методологій, які враховують цю інтеграцію і забезпечують захист фінансових даних на всіх рівнях системи. Прикладами можуть бути методологія забезпечення доступності даних, методологія реагування на інциденти безпеки та методологія моніторингу та аудиту системи бухгалтерського обліку.

Забезпечення інформаційної безпеки в бухгалтерському обліку супроводжується рядом завдань та викликів. Одним із найважливіших завдань є забезпечення освіти та навчання персоналу щодо правил та процедур інформаційної безпеки. Іншими завданнями є визначення ризиків, розробка політик безпеки, впровадження технічних заходів захисту та постійний моніторинг забезпечення безпеки.

Сучасні теоретико-методологічні підходи до забезпечення інформаційної безпеки впливають на практику бухгалтерського обліку важливим чином. Вони вимагають від організацій зосередитися на захисті фінансових даних та розробці стратегій в разі інцидентів безпеки. Крім того, ці підходи сприяють покращенню якості бухгалтерської інформації, оскільки зменшують ризик помилок та несанкціонованого доступу до неї.

Сучасні теоретико-методологічні підходи до інформаційної безпеки мають значний вплив на бухгалтерський облік. Ці підходи враховують різні аспекти захисту фінансової інформації та стандарти для забезпечення конфіденційності, цілісності та доступності даних. Ось деталізований огляд

впливу сучасних теоретико-методологічних підходів на бухгалтерський облік [2]:

1. Шифрування даних: сучасні методи шифрування грають ключову роль у забезпеченні конфіденційності фінансової інформації. Вони дозволяють перетворити дані в такий спосіб, що вони стають незрозумілими для осіб без відповідних ключів. Впровадження шифрування в бухгалтерському обліку допомагає захищати фінансові дані від несанкціонованого доступу, навіть якщо зловмисники отримають фізичний доступ до зберіганої інформації.

2. Методологія за замовчуванням (by default): цей підхід передбачає забезпечення максимальної безпеки "за замовчуванням". Його суть полягає в тому, щоб системи бухгалтерського обліку мали вбудовані заходи безпеки, які автоматично активуються при їх розгортанні. Це включає в себе стандартні налаштування безпеки, обмеження доступу і регулярне оновлення.

3. Інтеграція з системами інформаційної безпеки: сучасні підходи в бухгалтерському обліку вимагають інтеграції з системами інформаційної безпеки. Це означає, що системи обліку повинні співпрацювати з моніторинговими системами, системами виявлення загроз, системами реагування на інциденти і т. д. Це дозволяє більш ефективно виявляти та реагувати на можливі загрози для фінансової інформації.

4. Регулярні аудити і моніторинг безпеки: сучасні підходи вимагають проведення регулярних аудитів безпеки та постійного моніторингу систем бухгалтерського обліку. Аудити допомагають перевірити, чи дотримуються всі стандарти безпеки, а моніторинг дозволяє виявити і реагувати на несправності та інциденти в реальному часі.

5. Стандарти і вимоги: сучасні теоретико-методологічні підходи враховують стандарти та вимоги, такі як ISO 27001, які встановлюють основні принципи інформаційної безпеки, що повинні бути впроваджені в бухгалтерський облік. Дотримання цих стандартів сприяє підвищенню рівня безпеки [3].

6. Інтернал-контроль та ризик-орієнтований підхід: сучасні методи бухгалтерського обліку враховують інтернал-контроль та ризик-орієнтований підхід. Це означає, що бухгалтери та аудитори визначають потенційні ризики та розробляють контрольні процедури для їх зменшення та виявлення.

Сучасні теоретико-методологічні підходи ставлять інформаційну безпеку в центр уваги в бухгалтерському обліку, роблять її більш інтегрованою та комплексною і забезпечують більш високий рівень захисту фінансової інформації [4].

Сучасні теоретико-методологічні підходи до забезпечення інформаційної безпеки в бухгалтерському обліку важливі для забезпечення конфіденційності, цілісності та доступності фінансової інформації. Вони вимагають від організацій приділяти велику увагу цій проблемі та вживати заходів для захисту бухгалтерських даних. Дотримання сучасних методологій і підходів є ключовим для забезпечення успішності в управлінні фінансами та виконанням обов'язків перед стейкхолдерами організації.

Список використаних джерел:

1. Проект Закону про правотворчу діяльність, реєстр. № 5707 від 25.06.2021 (прийнято за основу 16.11.2021). URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72355.

2. РФ змінила підхід у веденні інформаційної війни проти України – експерт AMES (05.08.2020). URL : https://www.prostir.ua/?blogs=rf-zminyla-pidhid-u-vedenni-informatsijnoji-vijnyproty-ukrajiny-ekspert-ames.

3. Самотуга А. В. Проактивна зовнішня інформаційна політика України й питання її законодавчої регламентації. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матер. V Міжнар. наук.-практ. конф. (м. Дніпро, 12 бер. 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. С. 79-82.

4. Самотуга А. В. Україна в міжнародному інформаційному праві. Актуальні проблеми державотворення, правотворення та правозастосування : матеріали наук. семінару (м. Дніпро, 10 груд. 2020 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. С. 89-91.