ОБЛІКОВЕ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ БІЗНЕСУ: ЗАГРОЗИ В УМОВАХ ВИКОРИСТАННЯ ДІДЖИТАЛ-ТЕХНОЛОГІЙ

Будник І.М., здобувач ступеня доктора філософії
igorbydnik1@gmail.com
Науковий керівник: Денчук П.Н., к.е.н., доцент
Західноукраїнський національний університет

Економічну безпеку бізнесу доцільно розглядати як здатність оцінити зовнішні та внутрішні загрози та ризики та приймати превентивні заходи їх усунення через ефективну діяльність та аналіз релевантних інформаційних потоків з метою прийняття своєчасних управлінських рішень.

Достовірна облікова інформація відіграє важливу роль в забезпеченні економічної безпеки бізнесу.

Окремі економісти та фахівці у сфері обліку розглядають облікове забезпечення як на процес реєстрації, класифікації та звітування про фінансові операції та події. З їхньої точки зору, облікове забезпечення допомагає створювати фінансову звітність, яка надає інформацію про фінансовий стан підприємства і його результати, що є важливим для прийняття ефективних управлінських рішень [1, с.253].

Однак зводити поняття облікового забезпечення лише до питань формування інформації в обліку та звітності в сучасних умовах не є логічним.

Роль обліку в системі економічної безпеки, крім питань формування інформації, є ширшою і стосується:

- аспектів аналізу та планування. В цьому контексті облікове забезпечення доцільно розглядати як інструмент для фінансового аналізу та планування. Облікове забезпечення дозволяє підприємствам використовувати фінансові дані для прийняття важливих управлінських рішень і розробки стратегій розвитку;
- забезпечення юридичної та податкової відповідальності, оскільки достовірна облікова та звітна інформація є необхідною для дотримання законодавства та уникнення правопорушень;
- управління ризиками – ґрунтуючись на системі достовірного обліку і звітності та використовуючи методи фінансового аналізу підприємство може визначити потенційні фінансові ризики і прийняти заходи для їх зменшення або уникнення;

- фінансової безпеки та довіри. В цьому аспекті облікове забезпечення розглядають як засіб збільшення довіри інвесторів, кредиторів і споживачів до бізнесу. Якісний облік і звітність допомагають збільшити довіру до стійкості та надійності компанії.

Як і будь-яка діяльність організація обліку і формування звітності також може втілювати в собі певні ризики і загрози, які мають вплив на економічну безпеку бізнесу.

До джерел загроз економічній безпеці, які формуються в системі обліку доцільно віднести:

1) відсутність нормативних документів, які регулюють облік в компанії (Положення про облікову політику, посадових інструкцій тощо);

2) неефективне функціонування безпосередньо облікової системи (збору первинних даних, формування облікових регістрів, захисту облікової інформації, організації формування звітності);

3) недотримання вимог стандартів, нормативно-правових актів;

4) відсутність кваліфікованого персоналу підприємства [2, с.490].

Прослідковується взаємозв’язок між обліковим забезпеченням економічної безпеки бізнесу і забезпеченням безпеки облікової інформації.

Проблема забезпечення безпеки облікової інформації є надзвичайно актуальною з розвитком діджитал-технологій. В умовах використання сучасних технологій в обліку його інформаціє стає об’єктом інтересу для хакерів та кіберзлочинців. Їх дії можуть призвести до фінансових втрат, порушення конфіденційності та нанесенню непоправної шкоди репутації фірми. Тому безпека облікової інформації є необхідною для запобігання подібним інцидентам. До загроз безпеки облікової інформації в умовах використання діджитал-технологій можна віднести:

- фішинг: зловмисники можуть відправляти фішингові листи або повідомлення, що намагаються обманути користувачів і викрасти їхні облікові дані;
- вторгнення в облікові записи: хакери можуть намагатися зламати паролі та втручатися в облікові записи користувачів, отримуючи таким чином доступ до конфіденційної інформації;
- витік даних: загроза витоку облікової інформації виникає, коли хакери отримують доступ до баз даних компаній та розповсюджують конфіденційну інформацію;

- зловживання даними: конфіденційні дані попадають у руки зловмисників, їх можуть використовувати для шахрайства, вимагань викупу або інших злочинів.

Зловмисники постійно шукають способи доступу до конфіденційних даних, і тому необхідно вживати заходів для їхнього захисту. З цією метою важливо використовувати складні паролі, які складаються з букв, цифр та спеціальних символів, і регулярно їх оновлювати; методи двохфакторної аутентифікації для додаткового захисту облікових записів; шифрування даних під час передачі та зберігання, щоб запобігти несанкціонованому доступу; регулярне оновлення операційних системи та програмного забезпечення для закриття вразливостей; системи моніторингу для виявлення незвичайної активності та вторгнень в систему.

Оскільки в умовах застосування діджитал-технологій облік став більш вимогливим і складним завданням, облікові працівники повинні розуміти, як працювати з обліковими програмами, електронними таблицями, хмарними технологіями, системами електронного документообігу та іншими цифровими інструментами [3, с.150].

Для досягнення успіху в сфері обліку, обліковий персонал повинен мати добре розвинуті цифрові навички. Це включає в себе не тільки здатність користуватися програмами, але й здатність аналізувати великі обсяги даних, робити прогнози та ефективно використовувати цифрові інструменти для оптимізації процесів обліку.

Література.

1. Будько О.В. Обліково-аналітична інформація в системі інформаційного забезпечення сталого розвитку. *Держава та регіони. Серія: Економіка та підприємництво.* 2019. № 3. С. 252-257. URL: http://nbuv.gov.ua/UJRN/drep_2019_3_48 (дата звернення 1.11. 2023).
2. Бондарчук Н.В., Васільєва Л.М. Роль обліку у забезпеченні економічної безпеки підприємства. *Молодий вчений.* 2017. № 9 (49) С.489-493. URL: http://molodyvcheny.in.ua/files/journal/2017/9/109.pdf (дата звернення 2.11. 2023).
3. Шишкова Н. Л. Перспективи it-модернізації бухгалтерського обліку: актуалізація теорії і практики. *Економічний вісник.* 2019. №3. С. 146- 159. URL: https://ev.nmu.org.ua/docs/2019/3/EV20193_146-159.pdf (дата звернення 30.10. 2023).