УДК 657.1:004

Дутчак І. Б.,
к.е.н., доцент кафедри обліку і аудиту,
Львівський національний університет імені Івана Франка

ОСОБЛИВОСТІ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ В СИСТЕМІ БУХГАЛТЕРСЬКОГО ОБЛІКУ ПІДПРИЄМСТВА

Облікова інформація є одним з найцінніших активів будь-якої організації. Вона містить деталі про фінансові операції, клієнтів, співробітників та інші конфіденційні дані. Зростання кіберзагроз робить захист облікової інформації критично важливим завданням, про що стверджують вітчизняні науковці [1;2;3].

Облікова інформація – це сукупність даних, які відображають господарську діяльність підприємства та використовуються для прийняття управлінських рішень. Вона є основою для складання фінансової звітності та аналізу діяльності компанії.

Облікова інформація використовується як внутрішніми так і зовнішніми користувачами. До внутрішніх користувачів належать: керівники, менеджери, бухгалтери, які використовують її для прийняття управлінських рішень, контролю за діяльністю підприємства, складання бюджетів тощо. До зовнішніх користувачів належать: інвестори, кредитори, податкові органи, аналітики, які використовують облікову інформацію для оцінки фінансового стану підприємства, прийняття рішень про інвестування або кредитування тощо.

Носіями облікової інформації можуть бути первинні документи (накладні, рахунки, чеки тощо), регістри обліку (журнали, книги, відомості), звіти, наприклад, фінансова звітність (баланс, звіт про фінансові результати, звіт про рух грошових коштів), аналітичні звіти, статистична та управлінська звітність.

Важливо розуміти, що облікова інформація є основою для прийняття обґрунтованих управлінських рішень та забезпечення прозорості діяльності підприємства.

Забезпечення захисту облікової інформації є важливим, оскільки запобігає виникненню: 1) фінансових витрат пов'язаних із несанкціонованим доступом до облікових даних, що можуть призвести до шахрайських операцій, викрадення коштів та інших фінансових збитків; 2) репутаційних ризиків, що пов'язані із витоком конфіденційної інформації, що може завдати серйозної шкоди репутації компанії, призвести до втрати довіри клієнтів та партнерів; 3) юридичної відповідальності, яка виникає за порушення законодавства про захист персональних даних та інші правопорушення, пов'язані з витоком інформації.

Перелік інструментів захисту облікової інформації постійно зростає. До основних методів, що використовуються у технологіях захисту облікової інформації належать:

1. Шифрування. Суть методу полягає у перетворенні даних в незрозумілу форму, яку можна дешифрувати лише за допомогою спеціального ключа. Його застосовують для захисту даних під час передачі по мережі, зберігання на дисках, резервного копіювання.

2. Стіни вогнезахисту. Суть методу полягає у фільтруванні мережевого трафіку, блокування шкідливих програм та несанкціонованого доступу. Його застосовують для захисту периметру мережі, контролю доступу до внутрішніх ресурсів.

3. Система виявлення вторгнень. Суть методу у моніторингу мережі на предмет підозрілої активності, виявлення атак та спроб проникнення. Його застосовують для своєчасного виявлення та реагування на загрози.

4. Система управління доступом. Суть методу полягає у контролі доступу до інформаційних систем на основі принципів автентифікації та авторизації. Його застосовують для забезпечення доступу лише авторизованим користувачам до необхідних ресурсів.

5. Резервне копіювання. Суть методу полягає у створенні копій даних для відновлення у разі втрати або пошкодження. Його застосовують для захисту від випадкових або навмисних втрат даних.

6. Обладнання безпеки. Суть методу полягає у створенні фізичного захисту серверів, мережевого обладнання та інших компонентів IT-інфраструктури. Його застосовують для запобігання несанкціонованому фізичному доступу.

7. Програмне забезпечення безпеки. Суть методу полягає у використанні антивірусних програм, фаєрволів, систем виявлення вторгнень та іншого програмного забезпечення для захисту від шкідливого програмного забезпечення.

8. Свідомість користувачів. Суть методу у навчанні співробітників правилам інформаційної безпеки, розпізнавання фішингових атак та інших загроз.

Також ефективними є такі заходи як: регулярне оновлення програмного забезпечення, що дозволяє усунути вразливі місця, які можуть бути використані зловмисниками; проведення аудиту безпеки з метою оцінки ефективності системи захисту та виявлення потенційних слабких місць; розроблення плану відновлення після інцидентів, що дозволяє розробити план дій на випадок імовірної кібератаки.

Отже, захист облікової інформації треба розглядати як комплексний процес, який вимагає постійної уваги та інвестицій. Комбінація різних технологій, регулярне навчання персоналу та постійний моніторинг дозволять забезпечити надійний захист облікових даних.

Література

1. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Вип. №11/2017. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf/.

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. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. Львів. «Магнолія 2006», 2018. 320 с.