

АКТУАЛЬНІ ПРОБЛЕМИ ОПТИМІЗАЦІЇ ІНФОРМАЦІЙНИХ ПОТОКІВ

Інформаційна система управління підприємством залишається найбільш актуальним питанням, оскільки одночасно вирішує питання управління, розвитку, контролю, оптимізації, виходу на нові ринки. Серед провідних науковців не припиняються пошуки ефективних механізмів оптимізації інформаційної системи і визначення шляхів зменшення вартості та часу на формування й використання бази інформаційних ресурсів. Мета дослідження полягає в оптимізації системи управлінського обліку шляхом трансформації механізмів формування бази інформаційних ресурсів і розробці ефективних підходів до посилення економічної безпеки суб'єкта господарювання.

Інформаційна система є нерозривною з новітніми технологіями обробки інформації та має бути спроектована відповідно до програмних комплексів, призначених для оптимізації збору, обробки, зберігання інформації, параметрів комунікаційної інфраструктури, принципів і методів організації ІТ-інфраструктури.

База стратегічних даних повинна забезпечувати: прямий доступ користувачів до інформації та можливість її багаторазового використання; максимальний обсяг потрібної інформації для користувачів на всіх рівнях управління; оперативний пошук і видачу інформації згідно із запитом; захист інформації від спотворень; захист від несанкціонованого доступу до інформації [1, 75].

Появу категорії ризику в бухгалтерському обліку та необхідність подання інформації про ризики обумовлюють стандартами бухгалтерського обліку, що дає право вибору оцінок, формату подання інформації у звітності, вибору показників, які достовірніше відобразять результати діяльності та фінансовий стан підприємства [6, 156].

З метою зменшення рівня загроз в автоматизованій системі підприємства впроваджують засоби забезпечення безпеки інформаційної системи, які поділяють на групи: засоби попередження порушень безпеки; засоби виявлення порушень безпеки; засоби зменшення збитків і відновлення системи після навмисних та ненавмисних порушень системи.

Для персонального захисту даних управлінський персонал має виконати такі дії: визначити, які бази персональних даних використовуються в компанії, і встановити відповідальну за обробку інформації особу; організувати роботу з такими даними; виділити підрозділ або сформувати команду за базами персональних даних [5, 39].

Відповідно має бути налагоджено й програмне забезпечення, зокрема встановлені ключі доступу, паролі, антивірусні програми. На теперішній час ринок інформаційних технологій пропонує різні технологічні рішення, які здатні забезпечити захист інформаційного доступу. Додатково управлінський персонал має планувати витрати, пов'язані з ІТ-підтримкою придбаної програми або з підготовкою власних фахівців, здатних обслуговувати бази захисту.

Серед внутрішніх причин ризику було названо витік конфіденційної інформації, який може бути спричинений працівниками компанії або зовнішнім втручанням у роботу системи. Достатньо складно визначити, які причини усунути складніше – внутрішні або зовнішні. Для захисту витоку інформації, спричиненого внутрішнім порушенням безпеки, необхідно переглянути політику управління кадрами. На стратегічному рівні необхідно створити структуру функціональної взаємодії персоналу, на тактичному – запровадити режим інформаційної дисципліни й систематизувати документообіг [3, 40].

Стратегічним захистом ділової інформації повинні стати документування і програмне забезпечення бізнес-процесів. Щоб зберегти інформацію, на тактичному рівні необхідно створити систему захисту комерційної таємниці й конфіденційної інформації [2, 41].

Завдання, які вирішують при формуванні системи підготовки інформації для прийняття управлінських рішень, реалізуються на базі системи управлінського обліку, яка не тільки забезпечує користувачів інформацією, а й інтегрує технології обліку з технологіями управління компанією в цілому та за окремими підрозділами. Організація системи управлінського обліку залежить від специфіки діяльності кожного підприємства, тому керівники підприємств повинні розробляти власні гнучкі системи інформаційного забезпечення ефективного управління [4, 78].

Отже, сучасне уявлення системи обліку сформовано на засадах найкращої світової практики та прогресивних шляхів застосування інформаційно-комунікаційних технологій. Інформаційний модуль

системи є не центром, а функціональною платформою, яка генерує ресурси для побудови бази системи управлінського обліку. Додаткові функції персонального захисту даних шляхом авторизації із застосуванням провідних технологій і новітнього обладнання дозволяють налагодити системний, неперервний, об'єктивний зв'язок із зовнішніми та внутрішніми суб'єктами інформації. Запровадження інформаційного ключа знижує ризик порушення інформаційної і, як наслідок, економічної безпеки. Управлінський персонал отримує можливість керувати компанією на відстані, що суттєво позначається на оперативності генерації рішень і виконанні завдань. Актуалізація інформаційної системи забезпечує пошук і використання нових механізмів для просування компанії на світові ринки, реалізації інвестиційного потенціалу та формування ефективного інноваційного середовища.

Список використаних джерел

1. Живко З.Б., Данилович-Кропивницька М.Л. Інформаційна основа прийняття стратегічних управлінських рішень. Актуальні проблеми економіки. 2008. №10. С. 69–80.
2. Назаренко В. Укріплюємо безпеку бізнесу: комерційна таємниця і конфіденційна інформація. Баланс. 2011. №12. С. 41–44.
3. Назаренко В. Укріплюємо безпеку бізнесу: створення режиму інформаційної дисципліни. Баланс. 2011. №21. С. 40–44.
4. Нападівська Л. Управлінський облік: значення та застосування у практичній діяльності вітчизняних підприємств в умовах ринкових відносин. Бухгалтерський облік і аудит. 2009. №8–9. С. 78–93.
5. Романова Н. Персональні дані та їх захист. Баланс. 2011. №21. С. 38–39.
6. Шевелев А.Е., Шевелева Е.В. Риски в бухгалтерском учете. М.: Кнорус, 2009. 156 с.