Желюк Л.О., *к.е.н., доцент.*
Тернопільський національний економічний університет

ВИКОРИСТАННЯ ІНСТРУМЕНТАРІЮ КОНТРОЛІНГУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Інформатизація усіх сфер життєдіяльності, впровадження новітніх технологій обробки та поширення інформації актуалізувала питання захисту та безпеки інформаційних масивів, як на макро- так і мікрорівнях. Тривалий час розуміння інформаційної безпеки в нормативно-правових та літературних джерелах ототожнювалося тільки з безпекою інформації, що значно звужувало її сутність. Саме тому, з низки питань, присвячених розгляду проблем забезпечення інформаційної безпеки України, найбільш вивченими та дослідженими її аспектами є питання інформаційно-технічної безпеки. Висвітлення окремих аспектів інформаційної безпеки знайшло своє відображення у працях вітчизняних та зарубіжних фахівців серед них праці С. Алексєєва, І. Арістова, В. Артемова, І. Бачило, Д. Белла, К. Бєлякова, В. Білоуса, В. Богуша, В. Брижко, Д. Ермоленка, В. Калюжного, М. Левицького, В. Ліпкана, О. Литвиненка, О. Логінова, Г. Почепцова, В. Цимбалюка, О. Юдіна та інших.

На нашу думку, проблему інформаційної безпеки доцільно розглядати в двох площинах:

перша – це розробка механізмів протидії протизаконному збору і використанню інформації, унеможливлення несанкціонованого доступу до інформаційних ресурсів, виключення незаконного копіювання, запуску програм-вірусів, знищення та модифікації даних у інформаційних системах;

друга – це потреба врахування в системі управління підприємством внутрішніх та зовнішніх ризиків, невизначеності функціонування економіки країни, що в свою чергу вимагає створення систем наукового передбачення можливих загроз та підбору інструментів їх протидії. Серед таких систем особливе місце повинно відводитися контролінговому інструментарію захисту управлінської інформації підприємств, установ та організацій.

Контро́лінг (англ. controlling) – це комплексна система управління підприємством, що включає в себе управлінський облік, облік і аналіз витрат з метою контролю всіх статей витрат, всіх підрозділів і всіх складових виробленої продукції або наданих послуг, а також їх наступне планування [1]. Контролінг забезпечує інформаційно-аналітичну підтримку процесів прийняття рішень та містить у собі управління ризиками (стра-

ховою діяльністю підприємств), управління системою фінансових індикаторів, управління системою реалізації стратегічного, тактичного й оперативного планування, систему менеджменту якості.

Одним із перших обґрунтував особливості використання котролінгу для забезпечення інформаційної безпеки вітчизняних підприємства Оліфіров О.В. в монографії «Контролінг інформаційної системи підприємства» (2003р.)[2], який на основі дослідження бізнес-процесів розробив інформаційно-аналітичну модель, засновану на факторному аналізі ризиків підсистем інформаційного забезпечення управління підприємством та комплекс оптимізаційних та імітаційних моделей, заснованих на критеріальній оцінці ризиків і їх ймовірнісному аналізі.

Однак питання системи ефективного управління ризиками в умовах динамічного середовища через контролінгові важелі є недостаньо відпрацьованим і вимагає подальших наукових досліджень. Тому в рамках даної публікації вважаємо за доцільне обґрунтувати організаційно-методичне забезпечення використання контролінгу для управління інформаційними масивами в умовах макроекономічної нестабільності з метою їх ідентифікації та нейтралізації.

З метою своєчасної ідентифікації чинників, які сигналізують про той чи інший напрям розвитку окремих показників суб'єктів господарювання доцільно використовувати інструментарій стратегічного контролінгу, який за допомогою інструментарію стратегічного аналізу (бенчмаркінг, портфельний аналіз, SWOT-аналіз, ABC – аналіз (оцінка незначного числа кількісних величин, які є найціннішими та мають найбільшу питому вагу у загальній сукупності вартісних показників), XYZ- аналіз), стратегічного прогнозування (експертні методи, екстраполяція, кореляційно-регресивний аналіз), економіко-математичне моделювання (моделюванні впливу ризиків за допомогою основних критеріїв прийняття рішень в умовах невизначеності: критеріїв сподіваного значення, граничного значення, найбільш імовірної події, критеріїв Лапласа, Ваальлда, Севіджа, Гурвіца (критерій оптимізму-песимізму), Бейєса, (максимум середнього виграшу), мінімуму середнього ризику), яке дозволяє виявляти реальні та приховані загрози, настання яких може призвести до втрати потенційних шансів для розвитку підприємства.

Процес створення ефективної системи контролінгу інформаційної безпеки доцільно організувати в розрізі таких організаційних процедур:

1) створення інформаційно-аналітичної бази для проведення моніторингу. При цьому до основних сфер спостереження в рамках внутрішньої діагностики належать: організаційна, адміністративна, фінансова, виробнича, маркетингова, кадрова, комунікаційна підсистеми. Зовнішня діагностика повинна бути побудована на аналізі ринкової кон'юнктури а та-

кож політичного, економічного, соціального, екологічного, зовнішньоекономічного, науково-технічного середовища;

2) вибір індикаторів раннього попередження, які можуть указувати на розвиток того чи іншого негативного процессу, що матиме суттєвий вплив на безпеку підприємства. При цьому площина моніторингу повинна стосуватися як внутрішнього середовища підприємства, так і його конкурентів. До таких індикаторів повинні входити загальноекономічні (індикатори, які дозволяють своєчасно виявити зміни в тенденціях розвитку кон'юнктури економіки в цілому); ринкові індикатори, які дають змогу виявити тенденції на ринках, на яких здійснює свою діяльність підприємство; технологічні індикатори, які дають інформацію щодо розвитку нанотехнологій; соціальні індикатори, які відтворюють демографічну ситуація в країні; політичні індикатори, які характеризують зміни в інституційному середовищі;

3) розрахунок коридору граничних значень індикаторів, які гарантують безпеку підприємству на ринку, накшталт, податкової спроможності, фінансової стійкості, точки беззбитковості, рівня конкуренції, продуктивності праці, показника Free Cash-flow, який відтворює рух грошових коштів у рамках операційної та інвестиційної діяльності й оперативно сигналізує про проблеми в сфері збуту, виробництва, управління оборотними активами [3];

4) формування аналітичних завдань, що стосуються стратегічного передбачення та проектування розвитку підприємства. Наприклад, метою стратегічного проектування дистрибутивної мережі підприємства є розробка моделі, що визначає найекономічніше доцільний спосіб розподілу товару при стабільних або зростаючих потребах клієнта. Проектування дистрибутивної мережі повинно дати відповідь на головне питання, як максимізувати прибуток і поліпшити якість послуг, як кількісно визначити ступінь відповідності рівня логістичних витрат і рівня обслуговування клієнтів. При цьому етапи проектування включають: 1) логістичний аудит дистрибутивної мережі (збір і аналіз даних та інформації про історію і поточний стан операцій; аналіз рівня забезпечення вимог клієнтів (customer service levels); ухвалення допущень, пов'язаних з планом розвитку; формалізація поточної системи дистрибуції; формулювання рекомендацій по поточній модернізації системи дистрибуції); 2) моделювання дистрибутивної мережі (ухвалення планових показників, пов'язаних з побудовою проектної моделі; розробка моделі поточної системи дистрибуції, верифікація моделі, розрахунок показників з урахуванням плану розвитку; розробка альтернативних схем і побудова альтернативних моделей); 3) вибір оптимальної моделі та її впровадження (порівняння, аналіз, оцінка і вибір оптимальної моделі; розробка генерального плану впровадження; контроль впровадження; оцінка функціонування розробленої моделі); 4) впровадження системи динамічної модернізації розподільчої мережі (визначення і формалізація функції пос-

тійного моніторингу і аналізу логістичних параметрів дистрибутивної мережі; тюнінг і модернізація дистрибутивної мережі);

5) формування інформаційних потоків, так званого матричного балансу, який поєднує джерела отримання та напрямки використання управлінської інформації: забезпечення інформаційного зв'язку між джерелами інформації та системою раннього реагування, між системою та її користувачами;

6) розробка рекомендації щодо розвитку сильних сторін та нейтралізації слабких факторів, що можуть вплинути на діяльність суб'єктів господарювання.

Особливе місце в інформаційно-аналітичному забезпеченні діяльності підприємства за допомогою контролінгових систем повинно відводитися системам фінансового прогнозування з застосування інструментарію бюджетування, казуального прогнозування, екстраполювання, що стосуються ліквідності, структури капіталу, кредиторської і дебіторської заборгованості, інвестицій, оборотності оборотних активів тощо.

Для активного використання контролінгового інструментарію в сфері діагностики кризових явищ необхідно формувати відповідні фахові знання та професійні вміння. Контролінг лише тоді зможе активно виконувати функцію інформаційної безпеки, коли він вдало інтегруватиме основні елементи організації і управління діяльністю підприємства, а саме: всі категорії бізнес-процесів і їх витрати; адміністративну систему; систему планування і бюджетування; систему управлінського обліку; систему стратегічного управління, засновану на стратегічному позиціонуванні; документообіг; оперативне управління; моніторинг і аналіз результатів фінансово-господарської діяльності підприємства. Це безперечно, дозволить своєчасно діагностувати можливі загрози, і сприятиме кращому позиціонуванню діяльності підприємства на ринку.

Література:

1. Контроллинг в бизнесе: методологические и практические основы построения контроллинга в организациях / А.М. Карминский, Н.И.Оленев, А.Г.Примак, С.Г.Фалько. – М., 2003. – 256 с.
2. Оліфіров О.В. Контролінг інформаційної системи підприємства: Монографія. – Донецьк: ДонДУЕТ, 2003. – 325 с.
3. Волчков С.А., Балахонова И.В. Использование современных стандартов управления предприятием (MRPII, ERP, CSRP, ISO 9000) для непрерывного улучшения бизнес-процессов (BPI) // Организатор производства. – 2008. – № 1.