УДК 657.1:65.014.1

Н.С. Ковалевська, канд. екон. наук, проф. (*ДБТУ, Харків*)
О.В. Баслик, здоб. PhD (*ДБТУ, Харків*)

ОЦІНКА СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Питання безпеки відноситься майже до всіх агентів глобального інформаційного середовища. Україна як активний учасник процесів циклу життя інформації не стоїть в стороні від них. Сьогодні цілями кіберзлочинців можуть стати не тільки відомі корпорації, а й будь-які підприємства малого та середнього бізнесу, які обробляють дані кредитних карток або зберігають певну конфіденційну інформацію. Це відбувається як на загальному рівні, так і в середині кожного окремого підприємства [1, с. 1036]. Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства». Так, В. Цимбалюк характеризує інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [2, с. 30]. В. Фурашев вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [2, с. 31]. С. Гуцу пропонує розглядати інформаційну безпеку як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [3, с. 248]. О. Литвиненко, під інформаційної безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [3, с. 249]. Дискусійним є визначення Б. Кормича, який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [4, с. 241]. Л. Харченко, В. Ліпкан, О. Логінов визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [4, с. 242]. Так, інформаційну безпеку підприємства слід розглядати як набір процедур та інструментів, які захищають усю делікатну корпоративну інформацію від неправомірного

використання, несанкціонованого доступу, псування або знищення, що включає безпеку на фізичному й корпоративному рівні, керування доступом та кібербезпеку [3, с. 250].

Інформаційне середовище внутрішнього аудиту підприємства – це «сукупність відомостей та повідомлень, що використовуються в процесі економічного контролю над станом, формуванням та ефективністю використання ресурсів підприємства» [5, с. 96]. Тому, в процесі оцінки ризику внутрішнього аудиту підприємств доцільно здійснювати розрахунок інформаційного ризику, викликаного використанням сучасних інформаційно-комунікаційних технологій в управлінні. Такий ризик є особливо актуальним для вітчизняних підприємств, бази даних яких містять значні обсяги конфіденційної інформації (включаючи банківські реквізити), що найчастіше стає об'єктом інформаційних правопорушень. Крім того, для вітчизняних підприємств характерною рисою є наявність великої кількості паперової документації, яка формується на всіх етапах виготовлення продукції та надання послуг.

Специфіка інформаційного сервісу полягає в тому, що більша частина облікової інформації формується та частково обробляється інженерно-технічними та допоміжними службами, які ведуть оперативний облік на місцях фактичного надання послуг та виготовлення продукції, що створює додаткові загрози цілісності інформаційних масивів. На етапі документування виробничого процесу внутрішній аудит має забезпечити контроль стану інформаційної безпеки підприємства, який пропонується здійснювати за допомогою розрахунку інформаційного ризику [6, с. 194].

В розробленій моделі ризик інформаційних загроз прямо пропорційно впливає на загальний аудиторський ризик інформаційної безпеки, а коефіцієнт стану інформаційної захищеності – обернено пропорційно. Запропонована методика оцінки інформаційної безпеки враховує особливості діяльності підприємств. Проведена за запропонованою методикою оцінка ризику інформаційної безпеки підприємства дозволяє вже на етапі планування перевірки відділом внутрішнього аудиту розробити комплекс процедур для перевірки стану інформаційного сервісу на підприємстві. В ринкових умовах вихід на ринок для кожного виробника означає вступ у конкурентну боротьбу, оскільки на ринку виступає велика кількість товарів та послуг, які пропонують різні способи задоволення однієї й тієї ж потреби споживача на однакових або дещо відмінних цінових умовах. В такій ситуації конкурентоспроможність стає провідною ринковою категорією, оскільки в ній сконцентровано виражені економічні,

науково-технічні, виробничі, організаційно-управлінські та інші можливості не тільки окремого підприємства, але й економіки країни.

Таким чином, на сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки підприємства, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень інформаційної безпеки впливає на розвиток та впровадження науково-технічних інновацій у процеси виробництва, збереження стабільності функціонування можливості економічного зростання. Одним із шляхів усунення цих недоліків у сфері підприємництва є проектування організаційно-функціональної підсистеми інформаційної безпеки підприємства і її ресурсного забезпечення. Саме сфера інформаційної безпеки підприємства потребує безперервно оцінювати вчинки зловмисників, які модифікують, знищують або сприяють крадіжці обліково-фінансової інформації.

Інформаційні джерела:

1. Lysak H., Morozova H., Gorokh O., Maliy O., Nesterenko I. The system of financial control in the management of a small business enterprise: methods and tools of implementation. *Review of Economics and Finance*, 2022, Vol. 20, No. 1. P. 1034-1041 URL: https://repo.btu.kharkov.ua//handle/123456789/26973

2. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2004. №8. С.30-33.

3. Kashchena N, Nesterenko I. Digitalization of the innovative development management information service of the enterprise.Mechanisms for ensuring innovative development of entrepreneurship : monograph. Tallinn: Teadmus OÜ, 2022. P. 238-254 URL: https://repo.btu.kharkov.ua//handle/123456789/31559

4. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса: Юридична література, 2003. 472 с.

5. Nesterenko O. O., Kovalevska N.S., Nesterenko I.V. Audit of integrated reporting in the context of sustainable development: monograph, State Biotechnology University. Tallinn: Teadmus OÜ, 2021. 112 p. URL: https://repo.btu.kharkov.ua//handle/123456789/8624

6. Nesterenko I., Kovalevska N. Formation of accounting policy and its impact on reporting indicators for food industry enterprises. *Economic analysis*, 2021. 31 (3), 190-197. DOI: https://doi.org/10.35774/econa2021.03.190