

БОДНАР О. А., к.е.н,
доцент кафедри фінансів, банківської справи та страхування
Миколаївський національний аграрний університет, м. Миколаїв

БАГАТОВИМІРНІСТЬ КОНЦЕПЦІЇ ЦИФРОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Актуальність. Забезпечення фінансово-економічної безпеки в умовах цифровізації має базуватися на цифровій безпеці – тобто формуванні якісно нових факторів участі підприємств в єдиній інформаційній системі для забезпечення фінансово-економічної безпеки підприємств та зниження зовнішніх і внутрішніх ризиків. Звідси виникає потреба в окресленні основних вимог до концепції цифрової безпеки підприємства.

Результати дослідження. Враховуючи багатфакторність та багатовимірність концепції цифрової безпеки підприємства, доцільно розглянути відсутність єдиного визначення та визнати можливість різних інтерпретацій цього поняття. При цьому в даному випадку виникає ще одна проблема: таке розмаїття концепцій породжує різноманітність методологічних підходів до визначення цифрової безпеки підприємств. Оцінка цифрової безпеки підприємства є відносним показником, що відображає стан цифровізації, дає змогу забезпечити економіку підприємства, виміряну за певний період.

Для зручності та цінності практичного використання методичний підхід має відповідати ряду вимог [1]:

- відображувати ключові фактори цифрової трансформації в контексті сучасних економічних умов;
- забезпечувати простоту розрахунків та економічну інтерпретацію отриманих оціночних значень;
- не викликати труднощів щодо значень окремих показників, які входять до підсумкового показника;
- виключити зайвий суб'єктивізм у розрахункових значеннях.

Орієнтуючись на виконання вищевказаних вимог до оцінки цифрової безпеки підприємств, можна використовувати коефіцієнтний метод оцінки. Його суть полягає в розрахунку конкретних показників, що характеризують ефективність застосування елементів цифровізації підприємств. У цьому випадку кінцевий показник виходить як середнє арифметичне відповідних коефіцієнтів. Відповідно до цього підходу розраховуються показники цифрової безпеки підприємств країн-членів ЄС [2].

Досліджуючи частку компаній, які проводять оцінку ризиків цифрової безпеки, було встановлено, що показник зростає зі збільшенням розміру компанії (менше 1/3 серед малих компаній, наближається до 3/4 серед великих).

Передача ризику (страхування) складає від 4 % у Литві до понад 56 % у Данії. В більшості країн ЄС схильність до передачі ризику зростає з розміром



підприємств.

Частка підприємств, на яких працюють люди, які знають про свої зобов'язання щодо безпеки ІКТ коливається від 1/3 у Греції до понад 3/4 в Ірландії, де також спостерігається висока концентрація бізнесу в секторі ІКТ. Ця частка також зростає з розміром підприємств: менше 60% серед малих підприємств, але більше 90% серед великих.

У Європейському Союзі, згідно з даними ОЕСД на основі Eurostat, методи оцінки ризиків цифрової безпеки для підприємств тісно пов'язані з тестами безпеки або процедурами резервного копіювання. У цілому можна зробити висновок, що великі компанії здійснюють цю діяльність в середньому набагато частіше, ніж малі.

Загалом тенденцію до страхування можна розглядати як ознаку серйозного ставлення компанії до цифрової безпеки. Однак це також залежить від наявності в країні страхових полісів, що покривають ризик цифрової безпеки. Традиційні страхові поліси або індивідуальні поліси кіберстрахування можуть покрити ризики. Створення середовища для цифрової трансформації підприємств, що працюють у традиційних секторах економіки, має включати низку спеціалізованих технологічних та бізнес-консультацій, які можуть проводитися відповідними центрами компетенції. Існує також попит на державно-приватну співпрацю щодо загальнонаціональних ініціатив (тобто, розвиток навичок і спільних стандартів) і комплексну фінансову структуру для підтримки підприємств. [3].

Висновки. Впровадження цифрових технологій в бізнес-процеси підприємств несуть нові ризики та загрози, не властиві традиційним (нецифровим) процесам; вони зумовлені новими технологіями та особливостями цифрової економіки. Виявлення можливих ризиків і загроз є однією з найважливіших цілей забезпечення економічної безпеки підприємства в умовах цифрової економіки. Підхід до аналізу ризиків і загроз підприємства в цифровій економіці має бути комплексним, що обумовлено багатовимірністю концепції цифрової безпеки підприємства та її залежністю від внутрішніх та зовнішніх факторів впливу.

Список використаних джерел:

1. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O. and Vodnar, O. (2022). Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Econ. Aff.*, 67(04): 619-629.
2. Eurostat (2022). Digital Economy and Society Statistics, Comprehensive Database. URL: <https://ec.europa.eu/eurostat/web/digital-economy-and-society>. (дата звернення: 10.03.2023).
3. Яниогло А.И. Проблемы обеспечения экономической безопасности на предприятии // *Науково-виробничий журнал «Інноваційна економіка»*, 1-2'2018 [73]. С. 201-211.

