УДК 330.34

Корват О.В., к.е.н., доцент
Харківський національний економічний
університет ім. Семена Кузнеця

ІНФОРМАЦІЙНІ РИЗИКИ ВЕДЕННЯ БІЗНЕСУ В УМОВАХ ЦИФРОВОГО РОЗВИТКУ

Цифрові технології швидкими темпами впроваджуються у всі сфери діяльності й поступово трансформують «біологічні та фізичні системи у кібербіологічні та кіберфізичні» [1]. Значна частина бізнес-процесів переходить в онлайн. Цифровізація економіки створює нові технологічні можливості для суб'єктів господарювання, зокрема в реалізації продукції без посередників, оптимізації витрат і бізнес-процесів, у швидкому реагуванні на ринкові зміни, відстеженні потреб споживачів, удосконаленні продукції [2, с. 82]. Проте однією із зворотних сторін діджиталізації є те, що діяльність підприємств у цифровому середовищі стає уразливою до інформаційних ризиків.

Безперечно, проблема забезпечення інформаційної безпеки бізнесу сьогодні – одна з актуальних. У підприємств існує потенційна загроза понесення збитків внаслідок неадекватного функціонування інформаційних систем, порушення цілісності й доступності даних, їх виток тощо. Досліджуючи сутність ризиків діяльності [3; 4] інформаційний ризик, на думку автора, доцільно визначити як можливість збитків суб'єкта господарювання, пов'язаних з отриманням, обробкою, передачею, втратою або витоком інформації. Технічні й технологічні проблеми в роботі програмного й апаратного забезпечення, засобів зв'язку також можуть призвести до порушення конфіденційності, доступності та цілісності даних. Враховуючи це, ризик інформаційно-комунікаційних технологій являється складовою інформаційного ризику, яка з розвитком інновацій набуває більшої ваги у якості фактору, що впливає на величину ризику.

Важливою характеристикою ризику інформаційно-комунікаційних технологій є поступове посилення його суб'єктності. Якщо нещодавно

порушення цілісності даних відбувалось переважно від чинників ненавмисного характеру (помилок персоналу, технічних і технологічних збоїв, пошкоджень, втрат), то з розширенням можливостей електронних комунікацій і штучного інтелекту, швидкостей та обсягів передачі інформації, постає потреба у захисті від навмисних дій злочинців у кіберпросторі, спрямованих на порушення роботи інформаційних систем та/або доступності, конфіденційності, цілісності електронних даних [5]. Зростання рівня кіберзагроз поставило питання забезпечення кібербезпеки в Україні одним із пріоритетів національної безпеки [5], що означає визнання кіберризику системним ризиком для національної економіки.

У цифровій економіці дані являються активом, а їх оперативний аналіз – основним джерелом конкурентоспроможності. Одночасно з цим дані стають все більш вільнодоступними [0]. Використання бізнесом технологій Big Data в плануванні, дослідженні попиту, підвищенні сервісу клієнтів тощо породжує специфічні інформаційні ризики Big Data [6, с. 88], зокрема ризики некоректних даних, некоректного аналізу, порушення інтелектуальної власності, виникнення етичних дилем.

Окремим аспектом інформаційних ризиків є ризики, пов'язані зі зберіганням даних підприємства в хмарних сховищах. Власники та адміністратори хмарних серверів мають необмежений доступ до розташованій на них інформації, що потребує запобіганню витоку приватних інформаційних активів.

Таким чином, інформаційні ризики у цифровому середовищі набули нових характеристик і стали значущими для функціонування підприємств, що актуалізує вивчення питань управління ними.

Література

1. Україна 2030Е – країна з розвинутою цифровою економікою. Економічна стратегія України 2030 // Український інститут майбутнього. URL : https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення: 30.09.2021).

2. Піщуліна О. Цифрова економіка: тренди, ризики та соціальні детермінанти. Центр Разумкова. Видавництво «Заповіт». 2020. 274 с. URL : https://razumkov.org.ua/uploads/article/2020_digitalization.pdf.

3. Энциклопедия финансового риск-менеджмента. Москва : Альпина Паблишер. 2019. 932 с.

4. McMillan R., Proctor P. Cybersecurity and digital risk management: CIOs must engage and prepare. Gartner Research. 2018. URL : https://www.gartner.com/en/doc/3846477-cybersecurity-and-digital-risk-management-cios-must-engage-and-prepare (accessed; 30.09.2021).

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення: 01.08.2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.09.2021).

6. Шандрівська О. Є., Кириленко А. А. Особливості ідентифікації ризиків ринку Big Data. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*, 2021. № 3. С. 82-95.