Кравченко О.О., Бойко С.О.

ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Державний університет інфраструктури та технологій

Використання цифрових технологій на користь бізнесу і населення та організація цифрового доступу до товарів і послуг є цифровою економікою, розвиток якої є пріоритетним напрямком для сучасних держав. Термін «цифрова економіка» відноситься виключно до незавершеної трансформації всіх секторів економіки, що відбувається зараз, завдяки цифровізації інформації за допомогою комп'ютерних технологій [1].

Цифровізація впливає на економічний розвиток будь-якої держави та підприємства і навіть змінює соціальні стереотипи громадян. У сучасних умовах використання цифрових інструментів ведення бізнесу стає одним з суттєвих факторів забезпечення економічної безпеки підприємств.

Особливістю цифрової економіки є те, що її основним ресурсом стають дані, знання, інформація, що не виробляються та не споживаються у звичайному розумінні, як інші ресурси, а також не оцінюються з позицій рідкості та виснажування. Розвиток цифрової економіки призвів до формування специфічних загроз для підприємств.

У 2024 р. експерти Оксфордського університету та UNSW Canberra вперше оприлюднили Світовий індекс кіберзлочинності ('World Cybercrime Index'). Країнами, які мають найбільшу загрозу кібербезпеки, є рф, Україна, Китай, США, Нігерія та Румунія [2] (рис. 1). Однією з причин зростання кіберзлочинності є початок повномасштабної агресії рф проти України. Так, у 2022 р. Україна стикнулася з 7000 кібератак на інформаційну інфраструктуру, що у 2,8 рази більше кіберінцидентів, ніж у 2021 р.

Так, з 24 лютого і до кінця 2022 р. урядова команда реагування на комп'ютерні надзвичайні події CERT-UA опрацювала 2194 кіберінциденти. З них 120 стосувалися фінансового сектору, 156 – комерційних організацій та 92 – сектору телекомунікацій і розробки програмного забезпечення. Україна є другою серед найбільш атакованих країн світу після США [3].

Ranking	Country	WCI score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	United States	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	United Kingdom	9.01
9	Brazil	8.93
10	India	6.13
11	Iran	4.78
12	Belarus	3.87
13	Ghana	3.58
14	South Africa	2.58
15	Moldova	2.57
16	Israel	2.51
17	Poland	2.22
18	Germany	2.17
19	Netherlands	1.92
20	Latvia	1.68

Рис. 1. Ранжування країн за Світовим індексом кіберзлочинності у 2024 р. [2]

Фінансово-економічна безпека в умовах цифрової економіки спрямована на забезпечення протидії викликам і загрозам, пов'язаних з новими технологіями та особливостями цифрової економіки. Аналіз наукових публікацій показує, що процес цифровізації економіки здійснює вплив практично на всі сфери життєдіяльності не лише окремого підприємства та держави, а й всього світу загалом. Існують ризики появи нових, раніше неідентифікованих загроз фінансово-економічній безпеці підприємств. Ризики та загрози фінансово-економічній безпеці підприємства можна умовно розділити на чотири основні групи.

Група 1. Ризики та загрози політичного характеру. Так, гонка за новітніми технологіями цифрової економіки, нові ринки, масові закордонні сервіси, інвестиції, бізнес-моделі, стартапи, нові гроші, нові індустрії породжують залежність різних аспектів виробничої та фінансово-економічної діяльності, а також можливості розвитку від експорту інвестицій, технологій і товарів (сировини, матеріалів) від іноземних держав.

Також існує можливість інформаційно-технічного впливу з боку інших країн на інформаційну інфраструктуру економіки в політичних, економічних та військових цілях. Оскільки інформація є одним з головних ресурсів при цифровій економіці, то саме вона створює нові загрози фінансово-економічній безпеці

підприємств. В контексті ризиків і загроз політичного характеру особливе значення отримують гібридні загрози, вплив яких може мати відстрочений характер, що знижує можливості нівелювання їхнього негативного впливу.

Група 2. Ризики та загрози фінансово-економічного характеру. В умовах цифрової економіки змінюються підходи до оцінки результатів операційної, інвестиційної та фінансової діяльності підприємств, а також їхнього розвитку. Крім того, існуючі методики обліку та прогнозування фінансово-економічної діяльності відстають від вимог цифрової економіки, що призводить до виникнення небезпечних дисбалансів в оцінці рівня фінансово-економічної безпеки підприємств, а також ідентифікації впливу виникаючих ризиків і загроз.

Група 3. Ризики правового характеру – це, перш за все, юридична невизначеність законодавства, що регулює діяльність у віртуальному просторі та правил використання нових цифрових технологій економіки, а також відставання нормативно-правового регулювання економічних відносин у віртуальному просторі від швидкості цифровізації. Наслідком цього може стати зростання шахрайства та корупції.

Група 4. Технологічні ризики та ризики інформаційної безпеки. Найновіші технології, такі як штучний інтелект, Big Data, блокчейн, криптовалюти, інтернет речей (включаючи промисловий інтернет речей) віртуальна реальність є запозиченими технологіями, що також створює додаткові загрози стабільному функціонуванню підприємств.

Таким чином, у мовах цифрової економіки забезпечення фінансово-економічної безпеки підприємств має здійснювати комплексно, безперервно, своєчасно, планово та із дотриманням принципу економічної доцільності.

Література:

1. Bukht R., Heeks R. Defining, Conceptualising and Measuring the Digital Economy. *International Organisations Research Journal*. 2018, vol. 13, no 2, pp. 143–172. DOI: 10.17323/19967845-2018-02-07.

2. World-first “Cybercrime Index” ranks countries by cybercrime threat level. URL: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.

3. Forbes.ua. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. URL: https://forbes.ua/news/.