

Семко О.В.<sup>1</sup>, Данченко О.Б.<sup>1</sup>, Хішам Сафар<sup>2</sup>

<sup>1</sup>Черкаський державний технологічний університет (м. Черкаси)

<sup>2</sup>Університет економіки та права «КРОК» (м. Київ)

## **КОНЦЕПЦІЯ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ В ПРОЄКТАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ**

На даний час спостерігається активне впровадження цифрових проєктів в практику. Міжнародні корпорації з метою збереження конкурентоспроможності та лідируючих позицій реалізують проєкти цифрової трансформації бізнес-процесів та бізнес-моделей.

Цифрова трансформація несе в собі і переваги, які актуальні для будь-якого виду бізнесу, і ризики, які виникають внаслідок невизначеності середовища з порушенням базових характеристик безпеки.

Залежність від інформаційних технологій робить організації більш вразливими по відношенню до інформаційних ризиків, тому захищеність інформації найважливіших момент на всіх рівнях: проєкт, організація, оточення організації (рис.1).

Інформаційна система організації є відкритою системою, яка утворюється за рахунок інформаційних складових (співробітники, інформаційні ресурси, комп'ютерні системи різних класів), що забезпечують отримання, обробку, зберігання та передачу необхідної інформації.



Рис. 1 Вплив інформаційних ризиків на проєкт цифрової трансформації бізнесу

Зовнішнє інформаційне середовище утворюють об'єкти, суб'єкти, процеси, що впливають на складові інформаційної системи організації та на інформацію самого зовнішнього оточення, яке в свою чергу впливає на технологічне, правове інформаційне забезпечення бізнес-процесів, а також пов'язано із захистом своїх інтелектуальних активів та взаємодією із стейкхолдерами організації.

Функція управління ризиками допомагає організаціям домогтися успіхів при впровадженні цифрових ініціатив [1].

Відповідно до методології [2], інформаційні ризики ідентифікують, проводять якісний та кількісний аналіз, розробляють заходи реагування на них. Однак, база даних інформаційних ризиків постійно поповнюється новими специфічними ризиками, що ускладнює «боротьбу» з ними та їх наслідками.

Як правило, сучасні методи аналізу інформаційних ризиків застосовують до окремих проблем та ризикових ситуацій. Не приділяється належної уваги до використання методів м'яких обчислень (інтервальний метод, нейронні мережі, нечіткі множини та нечітка логіка) для вирішення проблем аналізу та синтезу систем управління інформаційними ризиками [3].

На теперішній час запропоновані концепції управління інформаційними ризиками, в яких з різних позицій розглядалися складові безпеки інформації організації, але вони не надають можливості системно та одночасно проаналізувати інформаційні ризики в межах системи організації.

На рис. 2 у вигляді діаграми представлені кола – зони впливу інформаційних ризиків: зовнішнього оточення (1), організації (2) та проєкту (3), які мають області перекриття між собою, тобто ці зони в своїй базі даних містять однаковий «набір» інформаційних ризиків.

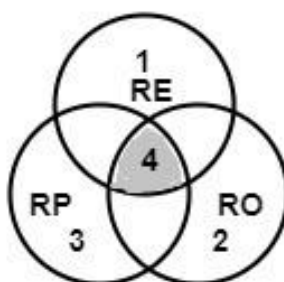


Рис. 2 Інформаційні ризики проєкту цифрової трансформації бізнесу

Кожне коло містить свою множину інформаційних ризиків  $r$ :

$$RE = \{r_1, r_2, \dots, r_k\},$$

$$RO = \{r_1, r_2, \dots, r_n\},$$

$$RP = \{r_1, r_2, \dots, r_i\},$$

де  $RE$  – інформаційні ризики оточення,

$RO$  – інформаційні ризики організації,

$RP$  – інформаційні ризики проєкту.

Для кожного кола застосовують власні методи управління ризиками (методи експертних оцінок, методології RiskWatch, OCTAVE та CRAMM), що потребує додаткових витрат.

Окремо виділена область перекриття (4), яка є спільною для всіх трьох зон.

У відповідності до запропонованої концепції, передбачається, що для інформаційних ризиків які в ході ідентифікації опиняться в області перекриття 4 і є загальними ризиками для усіх досліджуємих рівнів, будуть сплановані заходи реагування з використанням єдиних методів управління ризиками. Ця концепція дозволить проєктним менеджерам зменшити ресурсне, фінансове навантаження та витрати часу ( $K \text{ ® } min, S \text{ ® } min, T \text{ ® } min$ ).

Даний напрям є досить перспективним, тому автори вважають за доцільне продовжити дослідження, а саме, розробити математичну модель управління інформаційними ризиками у відповідності до концепції.

#### Список літератури

1. Данченко О.Б., Ланських Є.В., Семко О.В. Інформаційні ризики цифрового формату. Вісник Черкаського державного технологічного університету. / М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2020. – № 3. С. 58-66.
2. A guide to the project management body of knowledge (PMBOK guide), BISAC: Business & Economics / Project Management, 6 th. edition, Newtown Square, PA, USA: Project Management Institute, pp. 395-458, 2017.
3. Завгородний В.И. Системное управление информационными рисками. Выбор механизмов защиты. Серия: Информационные технологии в управлении. Проблемы управления, 2009. – № 1. С.53-58.