Роль інформаційного менеджменту у забезпеченні стійкості організації до цифрових ризиків

Євген Грицай
здобувач освітньої програми
«Agile-технології розробки програмного забезпечення»,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: HrytsaiYD@krok.edu.ua
Сергій Мічківський
к.е.н., доцент, с.н.с., зав. кафедрою комп'ютерних наук,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: MichkivskyySM@krok.edu.ua,
ORCID: 0000-0002-9343-2317

В умовах стрімкого розвитку інформаційних технологій та цифровізації бізнес-процесів, організації дедалі більше стикаються з ризиками кіберзагроз та витоків інформації. Стійкість організації у цифровому просторі стає ключовим фактором збереження конкурентоспроможності та стабільності бізнесу.

Згідно з дослідженням IBM Security, витік інформації у 2022 році обходився компаніям у середньому в 4,35 млн доларів США [1], що визначає необхідність посилення ролі інформаційного менеджменту, як ефективного інструменту управління ризиками цифровізації. Важливість проблематики додатково зумовлена посиленням державного регулювання у сфері інформаційної безпеки, зокрема в Європейському Союзі через стандарти GDPR (General Data Protection Regulation) та в Україні у зв'язку з ухваленням нормативних актів щодо захисту персональних даних. Це зобов'язує компанії переглядати власні підходи до управління інформаційними активами та ризиками, що виникають при їх обробці та зберіганні.

Відсутність систематизації підходів та визначення ролі інформаційного менеджменту в усіх процесах організації та, зокрема, в забезпечені безпеки (кіберзагроз та витоків інформації) призводить до порушення роботи організації та вагомих втрат. Наприклад, наслідки від шкоди що були заподіяні Petya.A, кількість юридичних і фізичних осіб, які стали жертвами цього вірусу, становить понад півтори тис., при цьому написали офіційні заяви в поліцію 178 особи (152 заяви – приватний сектор, 26 – державні структури) [2].

Сформульовано рекомендації з системного використання інформаційного менеджменту, які дозволять керівниками та менеджерами організацій мінімізувати ризики кіберінцидентів та підвищити ефективність управління інформаційною безпекою, зокрема:

• впровадження інтегрованих систем управління інформаційною безпекою (ISMS), що відповідають міжнародному стандарту ISO/IEC 27001;

• регулярне проведення аудитів інформаційної безпеки для раннього виявлення потенційних ризиків;

• організація постійних тренінгів для персоналу щодо правил інформаційної безпеки та протидії соціальній інженерії;

• використання сучасних технологій моніторингу й аналізу інформаційних загроз в реальному часі (SIEM-рішення);

• активніше впроваджувати політики "zero trust" (нульової довіри), які передбачають перевірку кожного запиту до інформаційних ресурсів організації, незалежно від внутрішнього чи зовнішнього походження запиту.

Використання подібних підходів та політик в організації системи інформаційного менеджменту суттєво знижує ризики несанкціонованого доступу та ускладнює потенційні атаки.

Системний підхід до організації інформаційного менеджменту є важливим елементом забезпечення стійкості сучасних організацій до цифрових ризиків, а також збільшує показники науково-технічного рівня [3] будь якої організації. Організації, які активно застосовують рекомендації з інформаційного менеджменту, можуть скоротити збитки від кіберінцидентів у середньому на 30-40%, а також значно швидше відновлювати роботу після атак. Організації, які застосовують комплексний підхід до управління інформаційною безпекою, поєднуючи технологічні рішення, систематичну роботу з персоналом та регулярне оновлення політик і процедур відповідно до актуальних викликів, досить стійкі до кіберзагроз та усуненню їх наслідків.

Подальші дослідження варто спрямовувати на поглиблений аналіз специфічних методів і технологій інформаційного менеджменту для окремих галузей, а також на розробку гнучких моделей управління ризиками у відповідності з темпами цифровізації бізнесу.

Ключові слова: інформаційний менеджмент, цифрові ризики, кібербезпека, інформаційна безпека, стійкість організації.

Список використаних джерел

1. IBM Security. Cost of a Data Breach Report 2022. URL: https://www.ibm.com/security/data-breach

2. Бараненко Р.В., Арутюнова К.А. До питання протидії кібертероризму // Інтеграція освіти, науки та бізнесу в сучасному середовищі: літні диспути: тези доп. II Міжнародної науково-практичної інтернет-конференції, 17-18 серпня 2020 р. – Дніпро, 2020. – 562 с. – С 60-62

3. Мічківський С.М., Шамарін Ю.В. Методи визначення НТР перепроектованих процесів // Торгівля і ринок України / Тематичний збірник наукових праць з проблем торгівлі і громадського харчування. – Донецьк: ДонДУЕТ. – 2001. – Т.2, № 12. – С. 119-125