Основні підходи до оцінювання економічної безпеки ІТ-сектору

Володимир Блинков
аспірант кафедри економіки,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: juisfan@bigmir.net,
ORCID: 0009-0001-3409-5955

Сучасний ІТ-сектор є каталізатором стрімкого економічного розвитку, ставши не тільки технологічним мотором, а й ключовим фактором в глобальному економічному ландшафті. За останні десятиліття цей сектор зазнав значних трансформацій, розвиваючись в такт із стрімким темпом інновацій та зростанням цифрової залежності. Проте, разом із зростанням можливостей, з'явились і нові виклики, пов'язані з економічною безпекою. Зростання кількості кіберзагроз, нестабільність фінансових ринків та швидкий технологічний прогрес створюють непередбачувані умови для компаній у ІТ-секторі. Для забезпечення стійкості і вдалого функціонування організацій необхідно вдосконалювати методи оцінювання економічної безпеки. Поряд із традиційними підходами, новітні техніки та індикатори стають важливим інструментарієм для розуміння та керування ризиками.

Аналізуючи наявні засоби та методи оцінювання економічної безпеки ІТ-сектору можна виділити два основні напрями: традиційні методи оцінювання такі як SWOT-аналіз та аналіз ризиків і сучасні техніки та індикатори які включають Cyber threat intelligence і Data Envelopment Analysis.

SWOT-аналіз є одним із найпоширеніших інструментів для визначення внутрішніх сильних та слабких сторін, а також зовнішніх можливостей та загроз для організації. У контексті економічної безпеки ІТ-сектору, SWOT-аналіз може розкрити важливі аспекти, такі як кількість і якість інновацій, резерви кадрів, а також відносини з клієнтами та конкурентами.

Традиційний аналіз ризиків включає ідентифікацію можливих загроз, оцінку ймовірності їх виникнення та визначення потенційного впливу на фінансовий стан і репутацію підприємства. Враховуючи швидкі зміни в технологічному ландшафті, аналіз ризиків дозволяє ідентифікувати та нейтралізувати можливі загрози забезпечення економічної стабільності.

Cyber threat intelligence використовується для кількісної оцінки кібербезпеки та виявлення вразливостей в інформаційних системах. Визначення ключових показників ефективності та ризиків в ІТ-секторі, ця техніка дозволяє компаніям вчасно реагувати на потенційні загрози та покращувати свою кібербезпеку, що потенційно може напряму впливати на економічну стабільність ІТ підприємства.

Data Envelopment Analysis (DEA) - це методологія для вимірювання продуктивності підприємства. В ІТ-секторі вона може застосовуватися для визначення ефективності використання ресурсів, таких як технічні та людські, що дозволяє забезпечити економічну стійкість за допомогою оптимізації внутрішніх процесів.

SWOT-аналіз в контексті IT-підприємства:

• Сильні сторони: аналіз потужних сторін організації, таких як висока кваліфікація персоналу та інноваційні продукти.

• Слабкі сторони: визначення аспектів, де підприємство може покращити ефективність, наприклад, управління ризиками та залученням талантів.

• Можливості: визначення перспективних тенденцій у галузі, таких як розширення ринків або нові технології.

• Загрози: оцінка можливих загроз, таких як конкурентність чи зміни в законодавстві.

Аналіз ризиків може бути використаний для багатьох аспектів підприємства один із прикладів впровадження нового продукту:

• Ідентифікація ризиків: визначення можливих негативних наслідків при введенні нового продукту на ринок.

• Оцінка ймовірності та впливу: кількісна оцінка ймовірності виникнення ризиків та їхнього впливу на фінансові та репутаційні показники компанії.

• Управління ризиками: розробка стратегій для зменшення ймовірності виникнення ризиків або зменшення їхнього впливу.

Підхід до оцінювання за допомогою Threat Intelligence

• Збір і аналіз інформації про загрози: систематичний моніторинг та аналіз поточних кіберзагроз, включаючи нові види атак та вектори зловживань.

• Класифікація за рівнем небезпеки: визначення ступеня небезпеки кожної ідентифікованої загрози відповідно до її потенційного впливу на економічну стійкість.

• Планування та реалізація заходів безпеки: розроблення та впровадження стратегій забезпечення захисту від конкретних загроз, ідентифікованих завдяки Threat Intelligence.

Використання DEA для вимірювання продуктивності:

• Ідентифікація вхідних та вихідних параметрів: визначення ключових факторів, що впливають на ефективність підприємства.

• Вимірювання продуктивності: застосування DEA для визначення, наскільки ефективно підприємство використовує свої ресурси.

• Впровадження оптимізаційних стратегій: розробка стратегій для оптимізації внутрішніх процесів та підвищення продуктивності.

Проаналізовані підходи до оцінки рівня економічної безпеки IT-сектору та сценарії їх застосування допомагають створити комплексний підхід до аналізу ризиків в IT-секторі, що дозволяє бізнесу ефективно управляти ймовірністю та наслідками можливих проблем. Ці сценарії дозволяють організаціям не лише аналізувати економічну безпеку, але і приймати конкретні кроки для покращення їхньої стійкості та ефективності в динамічному середовищі IT-сектору.

Список використаних джерел

1. Шершньова З. Є. Стратегічне управління : Підручник. – 2-ге вид, 2004. 143 с.

2. Балабанова Л.В. SWOT-аналіз – основа формування маркетингових стратегій: навчальний

посібник. – 2-ге вид., 2005. 301 с.
3. Кучеренко О. О. Аналіз оцінки ризиків як інструмент сталого розвитку підприємництва в умовах глобальних викликів та коронакризи // Приазовський економічний вісник. 2021. С. 72–76.
4. Kurt Baker. What is Threat Intelligence? // Cybersecurity 101. 2023. URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.
5. Robert M. Hayes. Data Envelopment Analysis. 2005. URL: https://www.scribd.com/presentation/287066870/Data-Envelopment-Analysis-ppt.