Література:

2. Association of Certified Fraud Examiners. Occupational fraud 2024: a report to the nations. URL: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

3. Deloitte. Fighting the newest trends in business fraud. Which are the most exposed processes and how can companies stay ahead of fraudsters. URL: https://www2.deloitte.com/ro/en/pages/about-deloitte/articles/combaterea-fraudei-organizatie-care-sunt-cele-mai-expuse-procese-si-cum-pot-companiile-sa-fie-cu-un-pas-inaintea-fraudatorilor.html

4. KPMG. Supply chain fraud. URL: https://assets.kpmg.com/content/dam/kpmg/be/pdf/Markets/supply-chain-fraud.pdf

Гнибіденко В.О.
здобувач гр. УФЕБ-23М
Чередніченко Н.Ю.
доктор пед. наук., професор
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

УДОСКОНАЛЕННЯ МЕХАНІЗМУ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ З УРАХУВАННЯМ ПОТРЕБ ЙОГО ВЛАСНИКІВ

Забезпечення економічної безпеки підприємства є складною багатофункціональною системою, яка залежить від його фінансово-економічного стану, а також від впливу внутрішніх і зовнішніх факторів. У ринкових умовах кожен суб'єкт господарювання діє автономно, застосовуючи інструменти для ідентифікації можливих загроз, які можуть негативно вплинути на його економічні інтереси та розвиток.

Економічна безпека підприємства може бути досягнута лише за умов побудови системи, яка дозволяє своєчасно виявляти, попереджувати та усувати реальні й потенційні загрози та має враховувати потреби власників підприємства, спрямовані на забезпечення його сталого функціонування.

Ефективне управління фінансово-економічною безпекою ґрунтується на чіткому розумінні ключових понять, таких як:

- економічна безпека – стан захищеності підприємства від впливу дестабілізуючих факторів;
- загроза – потенційна чи реальна небезпека для його економічних інтересів;
- ризик – ймовірність виникнення негативних наслідків;
- оцінка – визначення рівня загроз і ризиків.

Безпека є базовою умовою, яка дозволяє підприємству досягати поставлених цілей і створювати передумови для подальшого розвитку. Вважаємо, що рівень фінансово-економічної безпеки будь-якого підприємства визначається на основі:

- аналізу та діагностики діяльності, яку можливо досягти шляхом проведення оцінки технологічного рівня виробництва, конкурентоспроможності продукції та забезпеченості ресурсами, а також дослідження фінансового стану, включаючи ретроспективний аналіз і прогнозування перспектив розвитку;
- застосування різних методів оцінки. До ефективних інструментів належать експертний, рейтинговий, факторний та статистичний аналіз.

Особливу роль відіграє метод моніторингу, який дозволяє систематично спостерігати за змінами фінансово-економічного стану підприємства. Моніторинг фінансово-економічної безпеки передбачає:

- виявлення негативних тенденцій у діяльності підприємства;
- оцінку динаміки його розвитку та визначення причин загроз;
- прогнозування наслідків дії загроз;
- розробку заходів для їх усунення.

Моніторинг дозволяє своєчасно ідентифікувати фактори, що впливають на безпеку підприємства, а також створити основу для прийняття ефективних управлінських рішень.

Побудова системи економічної безпеки вимагає врахування специфіки підприємства, зокрема його галузевих особливостей, що сприяє формуванню стратегій захисту від загроз і забезпечує стабільність функціонування в умовах впливу зовнішніх і внутрішніх ризиків.

Таким чином, забезпечення фінансово-економічної безпеки підприємства повинно враховувати потреби його власників і відповідати специфіці його діяльності.

Системний підхід до моніторингу загроз, оцінки ризиків і прийняття управлінських рішень дозволяє зберігати стабільність, мінімізувати втрати та сприяти розвитку підприємства навіть в умовах економічної нестабільності.

Горбаченко С. А.
доктор економічних наук, професор
Національний університет «Одеська юридична академія»
м. Одеса, Україна

ОСОБЛИВОСТІ РЕКЛАМНИХ КАМПАНІЙ ПРОДУКТІВ ТА ПОСЛУГ У СФЕРІ КІБЕРБЕЗПЕКИ

Відповідно до вітчизняного законодавства рекламою вважається інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо відповідної особи чи товару [1].

На сучасному етапі окремі рекламні активності, як правило, використовуються в якості складових рекламних кампаній, які, у свою чергу виступають основним інструментом реалізації суб'єктом підприємництва власної рекламної стратегії. Розробка стратегії рекламної кампанії ґрунтується на програмі її маркетингу та цілях маркетингу. Основною метою рекламної кампанії є досягнення певної, необхідної репутації фірми/товару/особи, а також ефективне просування товарів та брендів на ринку з метою отримання певного ефекту (економічного, соціального та ін.) [2, с. 352].

Особливості кожної рекламної кампанії залежать від об'єкта просування, поставлених завдань та цільової аудиторії. Основні характеристики продуктів та послуг кібербезпеки, як об'єктів просування, пов'язані із тим, що вони торкаються таких критичних аспектів діяльності підприємств, як захист даних, забезпечення конфіденційності, фінансова безпека та репутація. Тому будь-які маркетингові інструменти у цій галузі (зокрема, й реклама) мають бути одночасно інформативним, переконливим і надійним, підкреслюючи важливість захисту від потенційних кіберзагроз [3].

Що стосується цільової аудиторії, основними споживачами товарів та послуг кіберзахисту є військово-промисловий комплекс, банки та кредитно-фінансові організації, підприємства у сфері енергетики, розробники програмного забезпечення, представники транспортної сфери, торгівельні підприємства. Особливості зазначених споживачів створюють «портрет клієнта», обумовлюють особливості попиту у досліджуваному сегменті і, в кінцевому рахунку впливають на основні параметри рекламних кампаній (табл. 1).

З огляду на характеристики замовників, рекламні кампанії продуктів та послуг у сфері кібербезпеки мають виконувати наступні завдання. По-перше, безпосередньо, інформування. Адже найчастіше будь-яка рекламна кампанія використовується саме для представлення нового продукту чи послуги на ринку, пояснення конкурентних переваг, створення іміджу бренду чи розробника, збільшення поінформованості про наявну пропозицію чи акцію. В сегменті кібербезпеки інформування, зазвичай, супроводжується технічною деталізацією для професіоналів, у вигляді, наприклад, рекламних матеріалів з глибоким технічним контентом для IT-фахівців, CISO та керівників безпеки.