

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.

Таблиця 1 - Особливості клієнтів в сегменті продуктів та послуг кібербезпеки

Характеристика	Опис
Індивідуальність запитів.	Майже кожний замовник бажає придбати персоніфіковане рішення, наприклад, з урахуванням особливостей власних бізнес-процесів.
Варіативність.	На ринку присутня значна кількість готових рішень, а також розробники та інтеграторів, які пропонують власні послуги у сфері кіберзахисту. Отже клієнт обирає з декількох варіантів, які можуть відрізнятися, навіть, концептуально.
Технічна обізнаність.	Кожне замовлення обов'язково погоджується із технічним відділом або іншими профільними фахівцями.
Значні бюджети замовлень/велика середня сума чеку.	Основними замовниками є представники великого та середнього бізнесу, діяльність яких залежить від рівня захищеності комп'ютерних та інформаційних мереж.
Прагнення до комплексного захисту.	Джерела кіберзагроз можуть бути дуже різними, але замовник зазвичай вимагає рішення, яке захистить від усіх, що призводить до формування системи кіберзахисту суб'єкта підприємництва.
Бажання швидкого виконання	Інколи замовник розуміє потребу у кібербезпеці після інциденту і підрахування втрат від нього. І, отже бажає негайного отримання надійного кіберзахисту, щоб унеможливити втрати у майбутньому.

*Джерело: складено автором*

По-друге, ефективна рекламна кампанія дозволяє сформувати або змінити ставлення потенційних клієнтів до окремих продуктів чи послуг переконати їх у необхідності здійснити покупку чи замовлення, посилити конкурентні переваги бренду тощо. Наприклад, кіберзагрози постійно змінюються, тому в рекламній кампанії важливо підкреслювати, що запропонований продукт чи послуга забезпечує захист саме від найсучасніших типів загроз.

При цьому необхідно створити у клієнта відчуття терміновості. Адже зловмисні атаки можуть статися будь-коли, тому важливо донести до клієнта, що діяти потрібно негайно. Однак цей підхід потребує делікатного балансу: надмірний тиск або залякування можуть, навпаки, викликати у потенційного клієнта відторгнення. Тому рекламна кампанія має поєднати обізнаність клієнта про ризики з позитивними емоціями від вирішення проблеми. Цього можна досягти, наприклад, за допомогою акценту в рекламній кампанії на дотриманні розробником міжнародних стандартів (GDPR, ISO/IEC 27001) конфіденційності даних.

По-третє, метою рекламної кампанії може бути нагадування користувачам про бренд або бізнес-структуру, для дублювання ключових повідомлень чи пропозицій, стимулювання повторних замовлень, збільшення частоти та середнього чеку. Зокрема, маркетологи у сегменті кібербезпеки намагаються зробити фокус на наслідках і ризиках. Основна мотивація до покупки при цьому виглядає наступним чином: кіберзлочини можуть призводити до серйозних негативних наслідків, тому вкрай важливим є постійне оновлення та модернізація системи кіберзахисту.

Щодо конкретних рекламних інструментів при просуванні продуктів та послуг у сфері кібербезпеки найкращу ефективність, зазвичай, демонструє Інтернет-реклама. Серед переваг Інтернет-реклами в контексті використання її в рекламних кампаніях у сегменті продуктів та послуг у сфері кібербезпеки можна відзначити наступні. По-перше, широке охоплення, адже реклама в мережі Інтернет спрямовується на більш ніж 4,3 млрд користувачів по всьому світу. По-друге, вона підходить для будь-якого бюджету, а такі види реклами, як, наприклад, email розсилка, взагалі не потребують інвестицій на початковому етапі. По-третє, на відміну від традиційної реклами, яку можуть бачити всі без винятку, оголошення в мережі Інтернет можна таргетувати. Продукти та послуги в сфері кібербезпеки можна рекламувати на тематичних форумах або в соціальних мережах у відповідних групах, щоб заохочувати коментарі, лайки, репости. По-четверте, Інтернет-реклама забезпечує чітку статистику і дозволяє отримувати кількісні показники ефективності за допомогою платформ вебаналітики, як-от Google Analytics.

Ще одним важливим елементом рекламних кампаній у сегменті продуктів та послуг у сфері кібербезпеки є гейміфікація. Адже з огляду на зростаючу кількість кіберзагроз, деякі підприємства вдаються до створення симуляцій атак, що дозволяють потенційним клієнтам відчувати себе в ролі захисника і на власному досвіді переконатися в ефективності рішень підприємства [4]. Застосування гейміфікації не тільки привертає увагу до окремих безпекових продуктів, а й створює емоційний зв'язок із брендом, оскільки клієнти краще запам'ятовують саме інтерактивний досвід.

У підсумку можна зазначити, що успішна рекламна кампанія у сфері кібербезпеки потребує поєднання кількох ключових елементів: інформативності, довіри, терміновості та відповідного балансу технічних і спрощених пояснень. При цьому основними результатами ефективних рекламних кампаній у сфері кібербезпеки мають стати, по-перше формування в потенційних покупців переконання про якість та корисність продуктів та послуг, спрямованих на кіберзахист, по-друге, донесення інформації щодо конкурентних переваг окремих суб'єктів підприємництва в даній сфері і, по-третє, своєчасне повідомлення про технічні інновації в сфері протидії кіберзагрозам.

### Література:

1. Про рекламу: Закон України в редакції від 27.04.2024 № 270/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text>
2. Хаустов М. М. Теоретичні аспекти проведення рекламних кампаній у мережі Інтернет. *Бізнес Інформ*. 2019. №7. С. 350–361.
3. Дяченко В. С., Дяченко Н. П., Буток М. В. Кібербезпека як базовий пріоритет digital-маркетингу. *Сучасні проблеми науки, освіти та суспільства* : матеріали 6-ої Міжнар. наук.-практ. конф. 14-16 серпня 2023 р. НВЦ “Sciconf.com.ua”, м. Київ, Україна, 2023. С. 146-152.
4. Толстик О.А. Застосування методів гейміфікації для підвищення рівня обізнаності співробітників підприємства з питань кібербезпеки. *Free and Open Source Software* : матеріали XV Міжнар. наук.-практ. конф., 13-14 лютого 2024 р., Харків: Харківський національний економічний університет імені Семена Кузнеця, 2024. С. 46.

**Горпинченко О.В.**

кандидат економічних наук, доцент

Центральноукраїнський національний технічний університет

м. Кропивницький, Україна

## **TRANSITION TO FLEXIBLE MODELS OF PROFESSIONAL DEVELOPMENT: THE ROLE OF DIGITAL TOOLS AND GLOBAL TRENDS**

In the modern world, professional development has become not only an important aspect of one's career but also a necessity for adapting to rapidly changing economic and technological conditions. Globalization, digitalization, and changes in the labor market require organizations and employees to adopt new approaches to learning and development. One of these approaches is the transition to flexible models of professional development, which provide greater adaptability, personalization, and accessibility of the learning process. In this context, digital tools and global trends play a key role in transforming learning and development processes [1].

Traditional models of education and professional development often relied on fixed courses, predetermined schedules, and physical locations. In contrast, flexible models allow employees to choose the pace and form of learning according to their needs and schedules. This is particularly important in the context of globalization, where the labor market is becoming increasingly competitive and multicultural, and where it is crucial to quickly adapt to new demands.

Thanks to digital platforms and adaptive technologies, learning has become more personalized. For example, Learning Management Systems (LMS) use algorithms to monitor students' progress and provide them with personalized recommendations for further development.