УДК 159.923.2:004.056

РОЛЬ КІБЕРБЕЗПЕКИ У РОЗВИТКУ КОРПОРАТИВНОГО ІМІДЖУ ІТ-КОМПАНІЇ

Богаченко О. В.
e-mail: olha.bohachenko@nure.ua
Харківський національний університет радіоелектроніки, каф. СГН
м. Харків, Україна

The paper analyzes the role of cybersecurity in developing the corporate image of IT companies. Cybersecurity is considered not only as a technical function but as a strategic asset and a key factor of digital trust. High security standards, international certifications, and the "Security by Design" principle form a positive brand image among customers, investors, and employees. Effective communication during cyber incidents and ethical data processing are essential for maintaining competitiveness and minimizing reputational risks in the IT market.

Сьогодні ринок ІТ-послуг перенасичений: користувача вже складно здивувати лише дизайном чи функціоналом. На перший план виходить інше – довіра. Саме тому кібербезпека поступово перестає бути просто технічною складовою і перетворюється на важливу частину іміджу компанії.

Коли ми говоримо про корпоративний імідж, ми маємо на увазі не просто гарний логотип чи вдалу рекламу. Це те, як компанію «відчуває» ринок: від її надійності до цінностей, які вона транслює. У цифрову епоху цей образ будується на впевненості клієнта в тому, що він не ризикує, обираючи саме цей бренд. Для ІТ-сфери імідж – це передусім обіцянка безпеки. Якщо компанія демонструє, що вона поважає приватність і вміє захищати дані, її імідж стає «бронею», яка допомагає витримувати конкуренцію та будувати тривалі стосунки з людьми [1].

Водночас важливо розуміти, що кіберінциденти мають довготривалі наслідки. Втрата довіри може коштувати компанії значно дорожче, ніж прямі фінансові збитки. Виникає «токсичність» бренду: коли назва компанії асоціюється з витоком даних, інвестори уникають співпраці, а талановиті розробники не хочуть пов'язувати кар'єру з незахищеним брендом. На додачу вищезгаданого, хочеться ще згадати про «ефект пам’яті». Незважаючи на всі переваги компанії, люди будуть пам’ятати про один інцидент, який стане плямою на репутації [2].

Саме тому дедалі більшого значення набуває підхід «Security by Design». Його суть полягає в тому, що питання безпеки враховуються ще на етапі розробки продукту, а не додаються пізніше. Такий підхід свідчить про зрілість компанії та її системне мислення [3].

Окрім технічних аспектів, велике значення має комунікація з користувачами. Людям важливо розуміти, як саме захищаються їхні дані. Просте пояснення складних речей допомагає сформувати відчуття

контролю і знижує рівень тривоги. У підсумку це позитивно впливає на загальне сприйняття бренду.

Для IT-компанії, яка хоче вийти на міжнародний ринок, наявність таких сертифікатів, як ISO 27001, SOC2 або дотримання вимог GDPR, є дуже важливою складовою корпоративного іміджу. На практиці це працює як своєрідний «знак довіри», який зрозумілий у різних країнах. Більше того, для великих компаній чи державних установ відсутність таких підтверджень може стати причиною відмови від співпраці, адже питання безпеки для них є принциповим [4; 5].

При цьому сертифікація вже давно сприймається не просто як формальність. Вона показує, що компанія відповідально ставиться до захисту даних і поважає право користувачів на приватність. Для клієнтів це важливо ще й з психологічної точки зору – з'являється відчуття спокою та впевненості у сервісі. Коли користувач бачить інформацію про сертифікати або проведені перевірки, у нього автоматично формується асоціація з надійністю.

У результаті це дає компанії не лише можливість утримувати клієнтів, а й відкриває шлях до більш серйозних і масштабних проєктів, де вимоги до безпеки значно вищі. Таким чином, сертифікація стає не просто вимогою ринку, а реальною конкурентною перевагою.

Зі сказаного нами раніше випливає, що у формуванні корпоративного іміджу перевагу отримують ті компанії, які здатні гарантувати клієнту не лише якісний результат, а й повний захист його даних. Кібербезпека – це дзеркало внутрішньої культури компанії та її поваги до прав людини в цифровому просторі і майбутнє належить брендам, для яких цифрова безпека є частиною їхньої соціальної відповідальності.

Список використаних джерел:

1. Митцева О. С. Класифікація типів іміджу // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 5: Педагогічні науки: реалії та перспективи: зб. наук. праць. Київ: Вид-во НПУ ім. М. П. Драгоманова, 2018. Вип. 63. С. 121-124.

2. Звіт IBM Security «Cost of a Data Breach Report 2025». URL: https://www.ibm.com/reports/data-breach

3. Шнайєр Б. Секрети та брехня. Цифрова безпека в мережевому світі. — К.: Наш Формат, 2023.

4. Міжнародний стандарт ISO/IEC 27001:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. URL: https://www.iso.org/standard/27001

5. Загальний регламент про захист даних (GDPR). Регламент ЄС 2016/679. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj