

РОЗДІЛ 3.
СОЦІАЛЬНО-ПОЛІТИЧНІ УМОВИ ФОРМУВАННЯ
КІБЕРПРОСТОРУ

Горбаченко Станіслав Анатолійович

*Національний університет «Одеська юридична академія»
завідувач кафедри кібербезпеки, доктор економічних наук, доцент*

НЕДОБРОСОВІСНА КОНКУРЕНЦІЯ ЯК ПРОБЛЕМА
КІБЕРБЕЗПЕКИ

В останні роки у світовому кіберпросторі поширюються небезпечні тенденції щодо зростання кількості кіберзлочинів, кібератак та випадків кібершпигунства. Вони, в свою чергу, обумовлюють постійний пошук та впровадження ефективних дій у відповідь, як на міжнародному та державному рівнях, так і у межах окремих бізнес-одиниць. Паралельно із класичними кіберзлочинами, що вже достатній час є об'єктами правового регулювання, кіберпростір починають використовувати також і як середовище для недобросовісної конкуренції. Означена проблема поки що далека від вирішення і потребує не стільки залучення інноваційних технологій скільки ефективних управлінських рішень.

Згідно із ст. 1 Закону України «Про захист від недобросовісної конкуренції» недобросовісною конкуренцією вважаються будь-які дії в конкуренції, що суперечать торговим та іншим чесним звичаям у господарській діяльності [1]. Головною метою подібних дій є досягнення неправомірних переваг над конкурентами. Під неправомірними перевагами слід розуміти такі, що супроводжується порушенням чинного законодавства.

Одним з частих порушень законодавства про захист від недобросовісної конкуренції з боку суб'єктів господарювання, який є до того ж найбільш використовуваним у кіберпросторі, відповідно до ст. 15-1 Закону України «Про захист від недобросовісної конкуренції», є поширення інформації, що вводить в

оману. Зокрема, мова йде про відомості які містять неповні, неточні або неправдиві дані про походження товару, виробника, продавця, спосіб виготовлення, джерела та спосіб придбання, реалізації, кількість, споживчі властивості, якість, комплектність, придатність до застосування, стандарти, характеристики, особливості реалізації товарів, робіт, послуг, ціну та знижку на них, а також про суттєві умови договору.

Основною метою поширення в мережі Інтернет неправдивих, неточних, неповних відомостей, які можуть вводити в оману споживачів, контрагентів, органи державної влади є вплив на клієнтську базу: зменшення лояльності, перехід до іншого продавця чи постачальника, зменшення середньої суми чеку тощо. Окремим напрямом для кібератак з боку конкурентів виступає особистий бренд засновника або керівника суб'єкта господарювання, особливо в сегментах, де продажі ґрунтуються саме на довірі до особистості.

Серед форм поширення неправдивої інформації, яка вводить в оману споживачів, є не тільки ті, що безпосередньо пов'язані із кіберпростором, а й зовнішні рекламні носії, поліграфічна продукція, реклама в роликах на телебаченні та радіо, реєстрація торгової марки із завідомо оманливою інформацією тощо. Проте саме Інтернет середовище виступає найбільш сприятливою платформою для розповсюдження подібної інформації.

Як результативні інструменти недобросовісної конкуренції в кіберпросторі можуть використовуватися фейкові статті в Інтернет – виданнях, поширення неправдивої інформації із залученням лідерів думок у соціальних мережах негативні відгуки на сайті або коментарі на бізнес – сторінках, штучно створенні замовлення в Інтернет – формах або за допомогою чат – ботів (наприклад, з метою порушення нормальної роботи в сфері послуг).

В останні роки в конкурентній боротьбі активно почали використовуватися й фішингові атаки. Зокрема на початку 2021 року спеціалісти виявили масову розсилку фішингових електронних листів по державних установах нібито від Адміністрації Держспецзв'язку. Листи було надіслано з електронної поштової скриньки, домен якої зовні був схожим зі справжнім доменним ім'ям Адміністрації Держспецзв'язку. Файл, який містився у цих електронних листах,

надавав доступ зломисникам до віддаленого управління ураженим комп'ютером. Тобто особа, яка отримала доступ, мала можливість знищувати, копіювати, змінювати дані, які містяться на уражених комп'ютерах [2].

Метою фішингових атак з боку конкурентів є, насамперед, доступ до персональних дані клієнтів. Персональними або особовими даними вважають відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Адже переважна більшість бізнес структур зберігає та використовує щонайменше такі особові дані клієнтів як ідентифікаційні дані (прізвище, ім'я, по батькові, адреса, телефон тощо); паспортні дані; особисті відомості (вік, стать, сімейний стан тощо); склад сім'ї; освіта; професія; житлові умови; фінансова інформація тощо. Деякі суб'єкти господарювання, які вважають себе клієнтоорієнтованими можуть також формувати, структурувати та зберігати дані щодо способу життя, інтересів та захоплень, споживчих звичок тощо.

Виходячи з вищесказаного побудова ефективної системи кіберзахисту від недобросовісної конкуренції має ґрунтуватися на наступних засадах.

1. Система аудиту згадувань підприємства чи бренду за ключовими словами.
2. Наявність власного юридичного відділу для протистояння недобросовісній конкуренції у правовому полі.
3. Безперервний моніторинг конкурентів з огляду на конкурентні дії які вони використовували раніше у ретроспективі.
4. Постійна робота з персоналом на предмет поведінки в Інтернет середовищі та засвоєння співробітниками основ інформаційної та кібербезпеки.
5. Формування системи контрзаходів у випадку спроб застосувати інструменти недобросовісної конкуренції.
6. Надійний захист основних нематеріальних активів підприємства.
7. Застосування кількісних методів оцінки ризиків від недобросовісної конкуренції (зокрема, аналізу сценаріїв або моделювання методом Монте-Карло).

Вказані засади мають стати основою для побудови суб'єктами господарювання комплексу конкретних заходів щодо прогнозування, ідентифікації та протидії загрозам недобросовісних дій з боку конкурентів на основі наявних технічних можливостей, людських та інформаційних ресурсів, а також нормативно-правового базису.

Список використаних джерел:

1. Про захист від недобросовісної конкуренції: Закон України № 236/96-ВР в редакції від 11.12.2019, підстава - 286-IX. URL: <https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text>
2. Харченко О., Яремич В. Протидія кібератакам, базованим на прийомах соціальної інженерії URL: <http://surl.li/arnjt>

Ключові слова: конкуренція, кібербезпека, особистий бренд, персональні дані.

Ключевые слова: конкуренция, кибербезопасность, личный бренд, персональные данные.

Key words: competition, cybersecurity, personal brand, personal data.

Трофименко Олена Григорівна

*Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук,
доцент*

Чепендюк Олександр Олександрович

*Національний університет «Одеська юридична академія»,
студент 2-го курсу факультету кібербезпеки та інформаційних технологій*

ЧОМУ C++?

Хоча мова програмування C++ з'явилася в далеких 80-х [1], ще й досі вона актуальна, завдяки своїм унікальним перевагам. Не зважаючи на поширені і