УДК 330.865:65

І.А. Кораблінова
К.С. Ганжа
О.І. Стоянова

КОНКУРЕНТНІ СТРАТЕГІЇ ТЕХНОЛОГІЧНИХ КОМПАНІЙ У СФЕРІ КІБЕРБЕЗПЕКИ

Державний університет інтелектуальних технологій і зв'язку

Анотація

Проведено аналіз поведінки технологічних компаній у сучасних умовах. Виявлено, що для реалізації своїх конкурентних стратегій вони використовують комплементарний підхід. У фокусі уваги дослідження є технологічні компанії, які виходять на глобальний ринок кібербезпеки.

Ключові слова: технологічні компанії, цифрова галузь, глобальний ринок кібербезпеки, конкуренти, партнери, комплементарний підхід, конкурентні стратегії.

Abstract

An analysis of behavior of technology companies in modern conditions. It has been established that they use a complementary approach to implement their competitive strategies. In the focus of research are technology companies that are entering the global cybersecurity market.

Keywords: tech companies, digital industry, global cybersecurity market, competitors, partners, complementary approach, competitive strategies.

Вступ

Сьогодні технологічний сектор є найбільш потужним у світовій економіці [1]. Він складається з компаній, які продають товари та послуги в галузі електроніки, програмного забезпечення, комп'ютерів, штучного інтелекту та інших галузей, пов'язаних з інформаційними технологіями [2].

Такі компанії вкладають значні кошти в дослідження та розробки і можуть братися за високоризиковані проєкти з великим майбутнім потенціалом [2]. У результаті їх діяльності в останні роки з'явилося багато різних ринкових сегментів у так званій цифровій галузі, межі якої ще досі невизначені [3]. Експерти з маркетингової аналітики зазначають, що у наш час постійно виникають все нові й нові типи технологічних компаній, які спеціалізуються на нових технологіях [4]. Наприклад, у сучасних умовах, коли в усьому світі все більше людей працюють та навчаються за допомогою інформаційних та комунікаційних технологій (ІКТ), все більше з'являється й компаній, які займаються проблемами безпеки у кіберпросторі. Збільшення кількості технологічних компаній, які мають різні або схожі компетенції, говорить про формування нового типу бізнес-середовища. Як об'єкт дослідження воно потребує комплексного вивчення у самих різних аспектах. У фокусі нашої уваги є аналіз характеру взаємовідносин і особливостей реалізації конкурентних стратегій компаній, які працюють у такому сегменті цифрової галузі як кібербезпека.

Результати дослідження

Активне використання сучасними компаніями цифрових технологій для вирішення тих чи інших бізнес-задач означають збільшення вразливості до кібератак. У наш час «все більше і більше цифрових пристроїв підключаються до мережі Інтернет, і всі «розумні» пристрої також є вразливими. Цифровізація зробила кібербезпеку предметом загальної стурбованості» [5]. У зв'язку з підвищеним інтересом суспільства до цієї теми у новій бізнес-літературі почав з'являтися аналіз досвіду існуючих стратегій компаній з вирішення проблем кібербезпеки або рекомендації щодо їх вибору під час реалізації програм з цифрової трансформації. Тобто, найбільшої розробки сьогодні отримали напрацювання науковців та практиків на мінірівні аналізу економіки кібербезпеки (зокрема, питання щодо оптимізації витрат на кібербезпеку, застосування нових технологій управління підприємством з урахуванням впровадження програм кібербезпеки і т.ін.). Проте, як показує моніторинг за діями технологічних компаній, на сьогодні вже сформувалася певна система відносин між різними

економічними суб'єктами, які реалізують свої інтереси у галузі економіки кібербезпеки через традиційну (ринкову) та сучасну (корпоративно-мережеву) форми. З наукової точки зору, це означає відкриття нового кола питань на мікроекономічному рівні аналізу, які потребують фахових досліджень.

Визначаючи об'єкт дослідження, варто звернути увагу на той момент, що на практиці вже почала розповсюджуватися думка, що нібито вже кожну компанію, яка функціонує у сучасних умовах активного застосування ІКТ, можна назвати технологічною [6]. Але для проведення мікроекономічного аналізу, наприклад, поведінки економічних суб'єктів з кібербезпеки, їх конкурентних стратегій і т.ін., слід чітко розуміти, про які саме компанії йде мова. Для виявлення таких компаній, які представляють технологічний сектор, або ту чи іншу його складову, можна скористатися базами даних міжнародних організацій (наприклад, UNCTAD, OECD та ін.), міжнародних видань (Forbes, Fortune та ін.), консалтингових агенцій (BCG, PwC, Gartner та ін.), професійних бізнес-порталів (Crunchbase, Clutch та ін.), онлайн-платформ з опису технологій і продуктів (G2.com, G2 Marketing Solutions, GetApp та ін.).

Наприклад, ми скористалися даними Interbrand, Forbes, UNCTAD, BCG для формування портрету топ-10 технологічний компаній (табл. 1).

Таблиця 1

Топ-10 технологічних компаній світу у міжнародних рейтингах у 2020-2022 рр.*

№ п/п	Компанія	Interbrand «Топ-100 кращих брендів світу» (складова: технології)		Forbes Global 2000 «Топ-2000 найбільших компаній світу»		UNCTAD, «Топ-100 компаній за іноземними активами»		BCG «Топ-50 інноваційних компаній»	«Кращий роботодавець світу» за версією Forbes
		Позиції за рейтингом 2021 року	Вартість бренду, млн дол	Позиції за рейтингом 2022 року	Ринкова капіталізація, млрд дол.	Позиції за рейтингом 2020 р.	Індекс TNI, %	Позиції за рейтингом 2021 року	Позиції за рейтингом 2021 року
1	Apple	1	408,251	7	2,640.32	35	39,8	1	5
2	Amazon	2	249,249	6	1,468.4	38	31,0	3	4
3	Microsoft	3	210,191	12	2,054.37	20	47,3	4	3
4	Alphabet (Google)	4	196,811	11	1,581.72	81	36,8	2	6
5	Samsung Group	5	74,635	14	367.26	39	57,7	6	1
6	Intel	17	35,761	51	190.29	92	53,7	-	69
7	Adobe	21	24,832	376	193.1	-	-	-	9
8	Philips	57	12,088	424	26.39	-	-	-	53
9	Huawei	85	6,196	-	-	80	37,5	8	8
10	Zoom	91	5,536	1184	29.96	-	-	-	-

*Джерело: складено на основі останніх актуальних рейтингів Interbrand, Forbes, UNCTAD, BCG.

На перший погляд здається, що одні компанії, які присутні у складеному рейтингу, не зважаючи на своє технологічне «коріння», є достатньо різними за профілем і не пов'язані між собою, а інші – є конкурентами. Найбільш розповсюджений їх образ серед споживачів такий: Apple – смартфони, планшети, ноутбуки, Amazon – електронна комерція, Microsoft – програмне забезпечення для комп'ютера; Google – пошуковик, застосунки для роботи у мережі Інтернет, Samsung – смартфони і побутова техніка, Intel – мікросхеми, мікрочипи, Adobe – застосунки для комп'ютера, Philips – побутова техніка, Huawei – телекомунікації, смартфони, ноутбуки, Zoom – програма для організації відеоконференцій.

Більш глибокий аналіз надає можливість виявити тісні партнерські зв'язки технологічних компаній між собою й серед тих, хто, на споживацький погляд, ніяк не пов'язані, й серед прямих конкурентів. Наприклад, хоча Apple та Samsung є конкуренти на ринку смартфонів, у той же час вони є партнерами на ринку напівпровідників. Такі комплементарні відносини характерні для більшості провідних технологічних компаній світу. Наприклад, Intel має понад 100 партнерів, серед яких є багато його основних конкурентів. Та ж сама ситуація з Microsoft, Alphabet (Google), Amazon та ін. Компанії обирають комплементарний підхід до реалізації конкурентних стратегій для подальшого розвитку свого бізнесу, керуючись відомою приказкою: «якщо хочеш йти швидко – йди один; якщо хочеш йти далеко – йдіть разом».

Крім того, на сьогодні всі технологічні компанії об'єднує загальна проблема – кібербезпека. Одночасно з розвитком своїх основних продуктів та послуг, вони виходять на новий глобальний ринок кібербезпеки або з боку консультантів та постачальників рішень (наприклад, Microsoft, Amazon, Alphabet (Google), Philips, Huawei та ін.), або як споживачі продуктів та послуг кібербезпеки

(наприклад, Apple, Samsung, Intel, Adobe, Zoom та ін.). Очевидно, що компанії, які пропонують свої послуги та продукти у сфері кібербезпеки, одночасно потребують їх й для споживання у своїх корпоративних інтересах. Крім цього, щороку з'являються компанії, які спеціалізуються суто на кібербезпеці. Наприклад, за даними Crunchbase, саме за напрямом «кібербезпека» у 2021 році було найбільше спрямовано венчурних інвестицій для стартапів.

Попит на рішення та послуги з кібербезпеки неабияк зріс в останній час. За результатами дослідження Accenture [7] стало відомо, що у 2021 році компанії зазнали в середньому 270 нападів, що на 31 % більше, ніж у 2020 р. Очевидно, що чим більше рівень кіберзлочинності, тим більше зростають витрати на кібербезпеку. Відповідно до звіту Cybersecurity Ventures (2021) [8], глобальні витрати, пов'язані з кіберзлочинністю, будуть зростати щорічно на 15% протягом наступних років та сягнуть 10,5 трлн дол. у 2025 році.

Згідно з дослідженням, проведеним SecurityWeek [9], у 2021 році було оголошено про понад 430 злиттів і поглинань (M&A), пов'язаних з кібербезпекою. Експерти SecurityWeek зазначають, що зростання активності M&A у сфері кібербезпеки значною мірою було викликано пандемією (підприємства інвестували більше в кібербезпеку та хмарну архітектуру через співробітників, які працюють віддалено) та серйозними кібератаками. Багато компаній погодилися на угоди M&A, адже така стратегія, особливо для невеликих компаній, є набагато більш реалізованою в порівнянні з IPO (первинним розміщенням акцій), особливо в такі невизначені часи. Тільки у травні 2022 року було оголошено про 36 M&A-угод за участю компаній, компетентних у галузі кібербезпеки [10].

Згідно даних Statista, глобальний ринок кібербезпеки буде продовжувати зростати щороку (рис. 1).

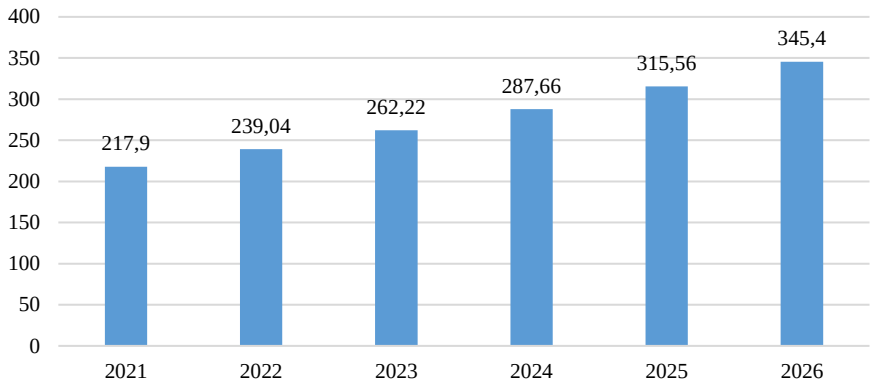

Рис.1. Прогноз щодо зростання розмірів глобального ринку кібербезпеки (млрд дол.) [11]

Незважаючи на те, що на глобальному ринку кібербезпеки спостерігається збільшення нових активних учасників, все ж, цей ринок неможна назвати досконалим. На ньому спостерігаються елементи конкурентної боротьби за клієнтів, але, у той же час, для більшості компаній характерна наявність своїх унікальних підходів до роботи у сфері кібербезпеки. Крім того, різноманітність кіберінцидентів, поява атак нового типу, потребує постійного вдосконалення знань та розвитку з боку компаній. Оскільки події відбуваються дуже швидко, на засвоєння нових знань часу не так багато, тому представники глобального ринку кібербезпеки постійно беруть участь у сумісних форумах, конференціях для обміну досвідом. На сьогодні існує вже понад 100 асоціацій, до яких входять компанії з кібербезпеки. Отже, цей ринок є змішаним, він має елементи і конкуренції, і монополії, і партнерства. Можна сказати, що подібне явище характерно для всіх складових цифрової галузі. За кожним напрямом свого розвитку технологічні компанії формують та реалізують свої унікальні конкурентні стратегії. Але, як показав, наш аналіз, реалізовують вони їх не по одинці, а у партнерській взаємодії з іншими компаніями, часто, навіть з конкурентами. Як приклад, можна навести партнерські програми держави і технологічних компаній у межах реалізації корпоративної соціальної відповідальності (КСО) у галузі кібербезпеки.

Так, технологічні корпорації, які базуються у США, у 2021 році включили до програм КСО проведення заходів з підвищення обізнаності населення США у питаннях кібербезпеки, а також виділення інвестицій на розвиток інфраструктури, зокрема такі [12]:

– Google протягом п'яти років інвестуватиме понад 10 млрд дол. США для посилення кібербезпеки. Їх використають для зміцнення ланцюжка поставок програмного забезпечення та гарантування безпеки

відкритого вихідного коду. Компанія також пообіцяла навчити 100 тисяч американців IT-підтримці та аналітиці даних за допомогою програми Career Certificate;

– Microsoft виділить 20 млрд дол. протягом п'яти років на розробку більш ефективних інструментів безпеки. 150 млн дол. компанія інвестує, щоб допомогти державним установам модернізувати свої системи безпеки та розширити партнерські відносини щодо навчання кібербезпеці.

– Apple створить програму, спрямовану на підвищенню безпеки в ланцюжках поставок в їх технологіях, яка включатиме роботу з постачальниками по впровадженню багатофакторної аутентифікації і тренінгів з безпеки;

– IBM протягом трьох років навчатиме понад 150 тис людей навичкам кібербезпеки;

– Amazon Web Services планує надати власникам облікових записів безкоштовні багатофакторні пристрої автентифікації для кращої безпеки їх даних, також планує запропонувати організаціям та приватним особам тренінги безпеки.

Висновки

Отже, сьогодні технологічні компанії, незважаючи на те, що на окремих ринках, вони є конкурентами, продовжують разом інвестувати в інфраструктуру кібербезпеки, а також у проєкти з розвитку навичок та вмінь співробітників компаній по всьому світу. Комплементарні форми взаємодії технологічних компаній потребують подальших досліджень, адже через їх дії поступово формується новий тип бізнес-середовища, вивчення специфіки якого надасть можливість орієнтуватися у нових умовах та приймати ефективні управлінські рішення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Top 10 World's Most Valuable Technology Companies in 2022 [Electronic resource]. – Mode of access: https://fxssi.com/most-valuable-tech-companies.

2.Technology Sector [Electronic resource]. – Mode of access: https://www.investopedia.com/terms/t/technology_sector.asp.

3. Кораблінова І. А. Компетенції компаній у цифрову епоху: Content & Context: монографія / І. А. Кораблінова. – К.: Кафедра, 2018. – 340 с.

4. Types of Technology Companies [Electronic resource]. – Mode of access: https://tortoiseandharesoftware.com/blog/types-of-technology-companies/.

5. Посилення стратегічних ланцюгів доданої вартості для сучасної промисловості ЄС [Електронний ресурс]. – Режим доступу: https://industryweek.in.ua/docs/Strategic-ForumStrengthening-Strategic-Value-Chains-for-a-future-ready-EU-Industry.pdf.

6. 10 Reasons Why Every Company is a Technology Company [Electronic resource]. – Mode of access: https://www.coxblue.com/10-reasons-why-every-company-is-a-technology-company/.

7. Elevating the Cybersecurity Discussion: Why CEOs need to get more involved in securing the business [Electronic resource]. – Mode of access: https://www.accenture.com/_acnmedia/PDF-177/Accenture-Elevating-the-Cybersecurity-Discussion.pdf#zoom=40.

8. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 [Electronic resource]. – Mode of access: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

9. SecurityWeek Study: Over 430 Cybersecurity Mergers & Acquisitions Announced in 2021 [Electronic resource]. – Mode of access: https://www.securityweek.com/securityweek-study-over-430-cybersecurity-mergers-acquisitions-announced-2021.

10. Cybersecurity M&A Roundup: 36 Deals Announced in May 2022 [Electronic resource]. – Mode of access: https://www.securityweek.com/cybersecurity-ma-roundup-36-deals-announced-may-2022.

11. Size of the cybersecurity market worldwide from 2021 to 2026 [Electronic resource]. – Mode of access: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/.

12. Google і Microsoft планують витратити 30 мільярдів доларів на кібербезпеку США [Електронний ресурс]. – Режим доступу: https://ms.detector.media/kiberbezpeka/post/28041/2021-08-27-google-i-microsoft-planuyut-vytratyty-30-milyardiv-dolariv-na-kiberbezpeku-ssha/.

Кораблінова Ірина Анатоліївна – канд. економ. наук, доцент, доцент кафедри економіки та цифрового бізнесу, Державний університет інтелектуальних технологій і зв'язку, м. Одеса, korablinova.irin@gmail.com

Ганжа Карина Сергіївна – студентка групи ЕП-4.01, факультет бізнесу та соціальних комунікацій, Державний університет інтелектуальних технологій і зв'язку, м. Одеса

Стоянова Олена Іванівна – студентка групи МО-4.01, факультет бізнесу та соціальних комунікацій, Державний університет інтелектуальних технологій і зв'язку, м. Одеса

Korablinova Iryna A. – PhD in Economics, Associate Professor, The Department of Economy and Digital Business, State University of Intelligent Technologies and Telecommunications, Odesa.

Hanzha Karina S. – student, Faculty of Business and Social Communications, State University of Intelligent Technologies and Telecommunications, Odesa.

Stoianova Olena I. – student, Faculty of Business and Social Communications, State University of Intelligent Technologies and Telecommunications, Odesa.