

## РИЗИКИ ВИКОРИСТАННЯ СТРАТЕГІЇ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

**Корнілова Ірина Миколаївна**

ORCID ID: 0000-0003-0715-5825

канд. екон. наук, доцент, доцент кафедри менеджменту  
інноваційної та інвестиційної діяльності

*Київський національний університет імені Тараса Шевченка, Україна*

**Приймак Василь Михайлович**

ORCID ID: 0000-0002-6525-7988

канд. екон. наук, доцент, доцент кафедри менеджменту  
інноваційної та інвестиційної діяльності

*Київський національний університет імені Тараса Шевченка, Україна*

Посилення ролі інтелектуальної власності у забезпеченні конкурентоспроможності інноваційних компаній на ринках наукоємної продукції обумовлюють потребу виваженого підходу до формування портфелю об'єктів інтелектуальної власності, забезпечення збалансованості його структури та напрямів використання, розробки й реалізації стратегій інтелектуальної власності.

У наборі стратегій інтелектуальної власності сучасних інноваційних компаній останнім часом збільшується увага до стратегій комерційної таємниці, що логічно пов'язано з зростанням її значення у забезпеченні конкурентних переваг у сучасному інноваційному просторі. Комерційна таємниця перетворюється на важливий інструмент захисту результатів інтелектуальної діяльності поряд з патентами, торговельними марками та авторськими правами.

Водночас, не дивлячись на значні переваги, які надає своєму власнику комерційна таємниця, є ряд застережень, які потрібно враховувати при прийнятті рішень щодо збереження результатів своїх досліджень та розробок як комерційної таємниці.

Серед вагових ризиків використання формату комерційної таємниці є ризик розкриття змісту конфіденційної інформації про науково-технічні розробки внаслідок реінжинірингу (зворотного проектування). Ступінь цього ризику визначається рівнем очевидності об'єкту інтелектуальної власності, який втілений у наукоємному продукті або технології. Неочевидність, складність розкриття сутності певної науково-технічної розробки створюють суттєві бар'єри процесу відтворення (копіювання) іншими учасниками ринку відповідного нововведення. У протилежному випадку власник комерційної таємниці незахищений від конкурентів через зворотне проектування. В управлінській практиці слід враховувати, що гальмуючий ефект для копіювання посилюють випадки поєднання у складній наукоємній продукції різних видів некодифікованих ноу-хау.

Певну загрозу для компаній, що зберігають результати своєї інноваційної діяльності як комерційна таємниця, становлять ризики паралельної, незалежної розробки. Ймовірність таких ризиків знаною мірою пов'язана зі рівнем конкуренції, інноваційної активності гравців у відповідному сегменті ринку, з трендами та швидкістю морального старіння. Компанії бажано оцінити рівень свого дослідницького лідерства у відповідному напрямку науково-технічних розвідок. При відсутності суттєвих часових переваг щодо випередження конкурентів існує ризик

розробки тотожного нововведення іншими компаніями, отже, використання ними стратегії патентування. Її наслідком є оприлюднення, розголошення сутності інформації, яка зберігається як комерційна таємниця, руйнування її статусу (комерційної таємниці), отже, й платформи для отримання доходу та конкурентних переваг.

Певним інструментом, протидіючим цим загрозам, фахівцями [1] вважається використання стратегії добровільного розкриття. Вона орієнтована на те, щоб змусити конкурента вийти з патентної гонки. Часто інноваційні лідери використовують цю стратегію у комбінації зі стратегією комерційної таємниці через механізм часткового розкриття певної науково-технічної інформації, щоб зняти у потенційних розробників мотивацію до реалізації стратегії патентування у відповідній площині досліджень.

Не слід нехтувати ризиками промислового шпигунства. Результати аналітичних досліджень [2] засвідчують, що збитки від крадіжки комерційної таємниці оцінюються в розмірі 1-3%% ВВП розвинених країн, при цьому лише для США вони становить від 180 до 540 млрд. доларів. Сучасна практика промислового шпигунства демонструє наявність широкого арсеналу інструментів, технологій його проведення. В умовах інтенсивного поширення процесів діджиталізації, яка набуває глобального характеру, промислове шпигунство набуває нового характеру, перетворюючись значною мірою на кіберпромислове шпигунство. Останнє часто називається «тихим злочином», вважається кращим методом для тих, хто займається промисловим шпигунством [3] і розглядається фахівцями [4] як крадіжка або копіювання фізичного документа чи предмета з оцифруванням інформації (що зберігається як комерційна таємниця) через незаконний доступ до комп'ютерних мереж. Вже зараз, за експертними оцінками [5], втрати від кіберзлочинності становлять до 0,8 відсотка світового ВВП, або 600 млрд. доларів на рік. Ризики втрати комерційної таємниці внаслідок успішних кібератак можуть стосуватися як оперативних, так і стратегічних негативних наслідків. Так, у кіберкрадіжці комерційної таємниці лише 10% витрат є негайними та прямими наслідками, решта 90% – це довгострокова втрата ноу-хау, конкурентної переваги та робочих місць [6]. Загалом, згідно зі звітом, підготовленим для Європейської комісії [7] серед негативних наслідків крадіжки комерційної таємниці компаній, насамперед, виділяються: втрати продажів; репутаційні збитки, додаткові витрати на внутрішнє розслідування; збільшення витрат на захист; витрати на ведення переговорів; витрати на моніторинг, судовий розгляд тощо.

Таким чином, усвідомлення можливих ризиків компанії щодо об'єктів інтелектуальної власності при обранні формату комерційної таємниці потребує посиленої уваги до створення дієвих механізмів режиму її захисту. Збільшується значення здійснення дієвого контролю доступу до інформації, що зберігається як комерційна таємниця, створення надійного технічного, нормативного, юридичного забезпечення відповідної системи управління. Комплексне вирішення цих завдань сприятиме підвищенню ефективності використання комерційної таємниці компанії.

### Список використаних джерел:

1. Crass, D., Valero, F. G., Pitton, F., Rammer, C. (2019) Protecting Innovation Through Patents and Trade Secrets: Evidence for Firms with a Single Innovation. *International Journal of the Economics of Business*, 26:1, 117-156. <https://doi.org/10.1080/13571516.2019.1553291>.
2. Ciuriak, D., Ptashkina, M. (2021) Quantifying Trade Secret Theft: Policy Implications. Centre for International Governance Innovation. <https://www.cigionline.org/static/documents/documents/no.253.pdf>.

3. Searle, N. (2021) The economic and innovation impacts of trade secrets. Intellectual Property Office. <https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets>.
4. European Commission (н.д.). FAQ: Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets). [https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/trade-secrets/faq-protection-against-unlawful-acquisition-undisclosed-know-how-and-business-information-trade\\_en](https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/trade-secrets/faq-protection-against-unlawful-acquisition-undisclosed-know-how-and-business-information-trade_en).
5. The economic impacts of cybercrime: how it costs us all. (2022) <https://mitigatecyber.com/the-economic-impacts-of-cyber-crime-how-it-costs-us-all/>.
6. Study on the scale and impact of industrial espionage and theft of trade secrets through cyber. (2019) Pwc. <https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf>.
7. Study on Trade Secrets and Confidential Business Information in the Internal Market. (2013) Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs Prepared for the European Commission. 150 p.