УДК 339.166:347.77
DOI: https://doi.org/10.32782/business-navigator.74-10

Корнілова І.М.
кандидат економічних наук, доцент,
доцент кафедри менеджменту інноваційної та інвестиційної діяльності
Київський національний університет імені Тараса Шевченка
ORCID: https://orcid.org/0000-0003-0715-5825

Kornilova Iryna
Ph.D. in Economics, Associate Professor,
Senior Lecturer at the Department of Innovation and Investment Management
Taras Shevchenko National University of Kyiv

ПРОМИСЛОВЕ ШПИГУНСТВО: ТЕРМІНОЛОГІЧНИЙ АСПЕКТ

INDUSTRIAL ESPIONAGE: TERMINOLOGICAL ASPECT

У статті розглядаються теоретичні аспекти промислового шпигунства в термінологічному контексті. Обґрунтовується значення захисту комерційної таємниці від промислового шпигунства на фоні збільшення її внеску у забезпечення конкурентоспроможності інноваційних компаній у світовому економічному просторі. Розглядається сутність промислового шпигунства через призму співставлення з іншими категоріями, а саме, економічним шпигунством, корпоративним шпигунством, конкурентною розвідкою. Досліджуються різні підходи до їх трактування. Встановлюється самостійність, нетотожність цих категорій при наявності певних спільних ознак. Виділяються важливі риси, сутнісні характеристики промислового шпигунства, надається його розуміння на основі виокремлених основних ознак, що сприятиме прийняттю управлінських рішень щодо розбудови дієвої системи захисту від його здійснення.

Ключові слова: інтелектуальна власність, комерційна таємниця, промислове шпигунство, економічне шпигунство, корпоративне шпигунство, конкурентна розвідка.

The article examines the theoretical aspects of industrial espionage in the terminological context. It substantiates the importance of protecting trade secrets from industrial espionage against the background of an increase in their share in the structure of the intellectual property portfolio and strengthening their contribution to the competitiveness of innovative companies in the global economic space. The paper also examines the essence of industrial espionage through the prism of comparison with other categories, namely, economic espionage, corporate espionage, and competitive intelligence. It explores different approaches to the interpretation of these categories. The analysis reveals the existence of variants of their identification, synonymous use, and a certain intersection of essential features. Based on the results of the comparison of industrial espionage, economic espionage, corporate espionage, and competitive intelligence, it is established that these categories are independent and non-identical, with certain common features, which is a manifestation of the dialectical combination of the general and the particular for various forms of gaining access to commercially valuable information. The publication highlights important features of industrial espionage that reveal its essential characteristics, including: systematic, planned nature of implementation; typically, a high level of organisation and preparation; targeted focus on gaining competitive advantage/income; unauthorised access to information that constitutes a trade secret; violation of legal and ethical standards by individuals and legal entities for private purposes; hidden nature; a wide range of types and tools; no sectoral restrictions on the scope of the activity; a significant range and duration of negative consequences; difficulty in assessing actual losses, etc. The identification of the main features of industrial espionage is the basis for its understanding as a distinct category, which will help to strengthen the theoretical and methodological basis for innovative companies to make effective management decisions on building an effective system of protection against industrial espionage.

Key words: intellectual property, trade secrets, industrial espionage, economic espionage, corporate espionage, competitive intelligence.

Постановка проблеми. Одним з провідних сучасних економічних трендів є перетворення інновацій у домінантний фактор зростання, досягнення системи цілей розвитку. Інтелектуальна власність стає потужним мотиваційним підґрунтям інтенсифікації інноваційної діяльності та джерелом збільшення прибутковості інноваційно орієнтованих компаній, забезпечення конкурентоспроможності на національному ринку та у світовому економічному просторі.

Важливим проявом посилення значення інтелектуальної власності є високий динамізм зростання та збільшення масштабів операцій з правами інтелекту-

альної власності, яка перетворюється на «четвертий кошик» у світовій торгівлі, поряд з товарами, роботами і послугами. Так, темпи зростання ринку інтелектуальної власності значно вище, ніж «матеріальних» ринків та перевищують 10% річних. Участь у світовій торгівлі інтелектуальною власністю для багатьох економічно розвинених країн доходить до 10% ВВП [1].

Розширене відтворення та використання портфелю інтелектуальної власності компаній характеризується збільшенням у його структурі частки комерційної таємниці, яка розглядається в стратегічному контексті скоріше не в якості альтернативи патентуванню, а в розрізі його доповнення, органічного поєднання та комбінованого використання з іншими інструментами захисту інтелектуальної власності. Посилення вагомості комерційної таємниці у забезпеченні конкурентних переваг на внутрішньому та зовнішніх ринках наукоємної продукції, на фоні збільшення обсягів і прискорення зростання міжнародної торгівлі правами інтелектуальної власності актуалізує завдання її захисту від несанкціонованого використання. Важливість вивчення даної проблематики підтверджується обсягами збитків від крадіжки комерційної таємниці, які, за оцінками експертів [2], оцінюються в розмірі 1-3% ВВП розвинених країн (що становить від 180 до 540 млрд дол. лише для США). Означене обумовлює потребу вивчення питань сутності промислового шпигунства для вироблення компаніями ефективних управлінських рішень щодо протидії його здійсненню.

Аналіз останніх досліджень і публікацій. Проблематика промислового шпигунства має міждисциплінарний характер, перетинаючись з широким колом питань, пов'язаних із забезпеченням набуття, захисту комерційної таємниці, використання відповідної інформації для отримання конкурентних переваг. Теоретичні та практичні аспекти конкурентної розвідки досліджують Г. Андрощук, Е. Блументаль, В. Бадрак, Л. Березіна, В. Богданович, Б. Братанов, І. Воловельська, В. Дикань, З. Живко, В. Зянько, І. Керницький, М. Копитко, М.Л. Мюллер, Т. Ткачук та інші. Важливими векторами дослідження є питання економічного, промислового шпигунства, організації захисту комерційної таємниці, які вивчаються в працях фахівців, серед яких, Г. Андрощук, В. Бадрак, Л. Березіна, Е. Блументаль, Е. Бітті, В. Богданович, Б. Братанов, В. Ван, А. Вашіст, Б. Віммер, Р.Е. Вагнер, Е. Гіббс, Р. Дарвін, Д.А. Джеймсон, Е. Джонс, О. Івченко, В.Ч. Істтом, З. Живко, В. Зянько, І. Керницький, М. Копитко, Е. Крейн, А. Кумар, М.Л. Мюллер, В. Кентон, Г.Л. Ковачич, Д. Ліберто, Г. Малицька, Х. Нашері, Д. Пулі, А. Рейсман, І. Сазерленд, Т. Ткачук, Л. Федулова, Т. Хоу, Г. Цифра, Ю. Якубівська та інші дослідники. Водночас, збільшення обсягів втрат від несанкціонованого використання комерційної таємниці на фоні зростання її значення в економічному розвитку інноваційно орієнтованих компаній обумовлює потребу поглибленого вивчення питань промислового шпигунства.

Формулювання завдання дослідження. Метою дослідження є сприяння поглибленому розумінню сутності промислового шпигунства для створення теоретико-методологічного підґрунтя розробки інноваційними організаціями дієвої системи протидії його здійсненню.

Досягнення мети наукових розвідок спирається на використання методів: абстрагування, наукової дескрипції, теоретичного узагальнення, індукції й дедукції, порівняння, діалектичного поєднання загального та особливого; декомпозиції та структурування. Використання означених методів сприятиме розвитку концепту управління комерційною таємницею у частині визначення напрямів формування організаційного забезпечення захисту комерційної таємниці від промислового шпигунства.

Виклад основного матеріалу дослідження. Важливою ознакою сучасних інноваційних компаній є збільшення частки комерційної таємниці в структурі їх портфелю інтелектуальної власності. Комерційна таємниця, як об'єкт інтелектуальної власності, все частіше обирається в якості провідного інструменту досягнення цілей у сфері комерційного використання результатів інтелектуальної діяльності. Вона відтягує на себе частину функцій управління інтелектуальною власністю, які раніше переважно виконувалися через патентування та отримання інших охоронних документів. Так, наприклад, за даними опитування 7000 американських фірм, проведеного Комісією з міжнародної торгівлі США, було встановлено, що 56% компаній, які здійснюють міжнародну діяльність, вважають комерційну таємницю «дуже важливою», порівняно з 48% для торгових марок, 37% – для патентів і 31 % – для авторських прав [3]. Означене обумовлює посилення виваженості прийняття управлінських рішень щодо забезпечення реалізації можливостей використання потенціалу конкурентоспроможності комерційної таємниці, зокрема, у площині її захисту від несанкціонованого використання.

Розгляд промислового шпигунства неможливий без висвітлення його співставлення з іншими категоріями проблематики отримання доступу до конфіденційної інформації, комерційної таємниці, як її різновиду, і спирається на діалектичне поєднання загального та особливого, що дозволяє в методологічному контексті визначити сутнісні риси, притаманні промисловому шпигунству.

У загальній логіці дослідження промислове шпигунство є різновидом шпигунства загалом, яке розглядається в різних ракурсах – як: діяльність з таємного отримання важливої політичної чи військової інформації про іншу країну або з'ясування секретів іншої компанії за допомогою шпигунів [4]; практика для отримання інформації про плани та діяльність, особливо іноземного уряду або конкуруючої компанії [5]; доступ до конфіденційної інформації без отримання дозволу власника інформації [6].

У широкому розумінні промислове шпигунство можна розглядати як використання шпигунських методів для з'ясування ключової інформації, яка має економічну цінність [7]. У фаховій літературі трактування промислового шпигунства відрізняються неоднозначністю тлумачення, що часто проявляється у ототожненні з іншими поняттями, зокрема, конкурентною розвідкою, економічним й корпоративним шпигунством.

Виокремленому розумінню промислового шпигунства сприяє його наступні визначення:

– шпигунство, яке організовується корпораціями [8];

– шпигунство з комерційною метою, зазвичай однією компанією за іншою [9];

– шпигунство однієї компанії за іншою з метою викрадення комерційної таємниці або іншої інформації, що є власністю [10];

– випадок, коли одна компанія викрадає секрети іншої компанії, з якою вона конкурує [11];

– викрадення комерційної таємниці шляхом видалення, копіювання або запису конфіденційної або цінної інформації в компанії для використання конкурентом [12];

– таємне отримання комерційної таємниці компанії або іншої конфіденційної інформації без дозволу та з нечесних мотивів [13];

– шпигунство у високотехнологічному середовищі, спрямоване як на отримання інформації, що стосується конкретної організації, так і на більш загальний збір корисної корпоративної інформації, яка може бути продана зацікавленим групам або окремим особам [14];

– збір інтелектуальних і конфіденційних даних у неетичний та незаконний спосіб для того, щоб отримати перевагу на ринку в контексті недобросовісної конкуренції [15];

– спонсорування або координація розвідувальної діяльності окремими особами або приватними суб'єктами господарювання з метою посилення їхніх переваг на ринку [16];

– незаконне та неетичне викрадення комерційної таємниці бізнесу для використання конкурентом для досягнення конкурентної переваги [17] тощо.

На відміну від наведених поглядів щодо промислового шпигунства, в науковій літературі представлені його розуміння з певним ототожненням з іншими категоріями. Зокрема, поширеним є синонімічне використання категорій промислового та економічного шпигунства, чи розгляд останнього як більш широке поняття. В такому ракурсі промислове шпигунство, наприклад, розглядається як: не тільки шпигунство (у найпростішому варіанті) за конкурентами, щоб отримати ринкову перевагу, що, ймовірно, тягне за собою крадіжку (або копіювання) комерційної таємниці та/або конфіденційної чи цінної інформації з метою використання її у власних цілях, але й шпигунство уряду за корпорацією з метою отримання інформації, яка буде корисною для його власної національної військової, промислової або комерційної бази [18]; як діяльність, що здійснюється іноземним урядом або іноземною компанією за прямого сприяння іноземного уряду проти приватної…компанії з метою отримання комерційної таємниці [19].

Доречним вважається виокремлення категорій промислового та економічного шпигунства. Економічне (державне) шпигунство здійснюється за участю та фінансової підтримки державних служб, що знаходить своє розширене відображення в наведених нижче тлумаченнях:

– зусилля уряду зі збору інформації, привласнення комерційної таємниці та викрадення знань [20];

– шпигунство, яке здійснюється за участю державних спецслужб з метою просування економічних інтересів своєї країни [9];

– шпигунство, яке зазвичай фінансується державою [21];

– шпигунство, яке організовується іноземними спецслужбами [8];

– шпигунство, що здійснюється або організовується урядами, і зазвичай має міжнародний характер [22];

– спонсорована або скоординована іноземною владою розвідувальна діяльність, спрямована на уряд … або …корпорації, установи чи осіб, призначена для незаконного чи таємного впливу на важливі рішення щодо економічної політики або незаконного отримання конфіденційної фінансової, торговельної чи економічної інформації; службова економічна інформація; або критичні технології [12];

– (1) крадіжка, несанкціоноване привласнення, приховування, отримання шляхом обману або шахрайства комерційної таємниці; (2) неавторизоване копіювання, фотографування, відтворення, змінювання, знищення, скачування, передача, надсилання, повідомлення комерційної таємниці; (3) отримання, купівля комерційної таємниці з усвідомленням того, що вона була присвоєна, отримана, перетворена без дозволу, з метою надання вигоди іноземному уряду, державному органові чи агенту [23] тощо.

Отже, промислове шпигунство – це те саме, що й економічне шпигунство, за винятком того, що замість того, щоб приносити користь іноземному уряду, воно приносить користь іншій приватній структурі [24]; це те ж саме, але без прямої участі уряду [25]; ті ж дії, але з метою нанесення шкоди власникові інформації, що становить комерційну таємницю, пов'язаної з виробництвом продукту, що поставляється на внутрішній і міжнародний ринок шляхом надання економічної вигоди суб'єкту, яка не є власником інформації, що становить комерційну таємницю [1]; здійснюється компаніями з комерційною метою, а не урядами з метою національної безпеки [17]; частіше є більш внутрішньо-національними і відбуваються між компаніями або корпораціями, які є конкурентами [22].

Поширеним у літературі є використання терміну корпоративне (бізнес) шпигунство, яке часто за сутнісними ознаками: чи ототожнюється з економічним шпигунством; чи розглядається як синонім промислового шпигунства; чи трактується більш широко, фактично включаючи і економічне, і промислове шпигунство. Останнє бачення пропонується вважати більш логічним, враховуючи високий рівень співпраці корпорацій з владою, їх вагомий вплив та внесок у розвиток економіки країн (насамперед, економічно розвинених), зростання їх ВВП.

Означені ракурси корпоративного шпигунства представлені, зокрема, у наступних трактуваннях:

– проникнення або викрадання даних, документів та інформації, що належать одній компанії, фізичній особі чи державному суб'єкту, для використання іншою компанією, фізичною особою чи державним суб'єктом [26];

– викрадення конфіденційної інформації, комерційних таємниць або інтелектуальної власності компанії та передача або продаж її іншій особі, щоб використати отриману інформацію для отримання конкурентної переваги [21];

– несанкціоноване та неетичне отримання конфіденційної або конфіденційної інформації від однієї компанії чи організації іншою для недобросовісної ділової практики [27];

– незаконна та неетична діяльність, що здійснюється організаціями для систематичного збору, аналізу та управління інформацією про конкурентів з метою отримання конкурентної переваги на ринку [28];

– незаконне викрадення/придбання інтелектуальної власності, наприклад ключової комерційної таємниці

та патентної інформації, а також методів і процесів промислового виробництва, ідей і формул [12];

– шпигунство, яке може охоплювати обидва сектори, … ведеться з метою національної безпеки, з комерційною або діловою метою, коли уряд безпосередньо залучений у бізнес-сектор, і, … це трапляється в багатьох місцях по всьому світу [22];

– незаконне придбання конфіденційних комерційних таємниць або інтелектуальної власності, зокрема виробничих процесів, списків клієнтів, проектних пропозицій, результатів досліджень і розробок і навіть тактики ведення переговорів, часто компаніями-конкурентами, які прагнуть отримати конкурентну перевагу,….і представлено двома типами економічним та промисловим шпигунством [9].

Важливим аспектом розуміння сутності промислового шпигунства є з'ясування питання його співставлення з конкурентною розвідкою, яке характеризується неоднозначністю бачень фахівців. Існують більш широкі трактування конкурентної розвідки без виокремлення способу (легального, етичного/нелегального, неетичного) набуття необхідної інформації, які, за змістовним наповненням можуть включати і промислове шпигунство. В такому розрізі конкурентна розвідка розглядається, зокрема, як: аналіз ринку підприємства, щоб зрозуміти, що відбувається, що станеться і що це означає для підприємства [29]; збір інформації про конкурентів і ринок загалом, яка пропонує розуміння, які можуть використовуватися для адаптації та вдосконалення стратегії, продуктів, маркетингу, планів та інших частин бізнесу [30]; здатність збирати та використовувати інформацію про фактори, які впливають на конкурентні переваги компанії, … для сприяння прийняттю більш обґрунтованих рішень і підвищення ефективності організації шляхом виявлення ризиків і можливостей до того, як вони стануть очевидними [31]; безперервний процес моніторингу галузі чи ринку фірми для виявлення поточних і майбутніх конкурентів, їхньої поточної та оголошеної діяльності, того, як їхні дії вплинуть на фірму та як на це реагувати [12]. Також у фахових публікаціях [32] наводяться тлумачення, згідно з якими конкурентна розвідка …може використовувати як незаконні способи промислового шпигунства, так і легальні методи конкурентної розвідки.

Вважається доречним чітке відокремлення цих категорій, насамперед, за критерієм законності та етичності здійснення діяльності. На відміну від промислового шпигунства конкурентна розвідка характеризується дотриманням законодавчих та етичних норм. В такому контексті конкурентна розвідка розглядається як:

– правова та етична діяльність щодо систематичного збору, аналізу та управління інформацією про промислових конкурентів [33];

– систематична та етична програма збору, аналізу та управління зовнішньою інформацією, що сприяє процесу стратегічного управління на підприємствах [34];

– не передбачає отримання інформації за допомогою неетичних або незаконних методів [21];

– законний збір загальнодоступної інформації шляхом вивчення корпоративних публікацій, веб-сайтів і заявок на патенти з метою визначення діяльності корпорації; етична практика, коли інформація може збиратися з одного або кількох джерел, що допомагає корпораціям зрозуміти конкурентний ландшафт, а також усі виклики, які він може створити [17] тощо.

Отже, проведене співставлення з іншими категоріями у сфері отримання доступу до комерційно цінної інформації дозволяє виокремити сутнісні риси промислового шпигунства, серед яких можна виділити: цільову спрямованість, пов'язану з прагненням отримати конкурентні переваги/ дохід від передачі інформації зацікавленим особам; несанкціонований доступ до інформації, що становить комерційну таємницю; порушення законодавчих та етичних норм, що визначає промислове шпигунство різновидом недобросовісної конкуренції; здійснення фізичними, юридичними особами в приватних цілях; систематичний, спланований характер здійснення; зазвичай, високий рівень організації та підготовки; прихований характер; широкий спектр видів, інструментарію здійснення; відсутність галузевих обмежень щодо сфери проведення (при пріоритетній увазі високотехнологічним галузям); значний діапазон і пролонгованість негативних наслідків, більшість яких проявляється з часом; складність оцінювання реальних збитків та інші характеристики.

Спираючись на визначені в літературі [19] кілька ключових ознак промислового шпигунства (намір, суб'єкт, характер, метод), пропонується його розглядати як прихований системний процес збору, управління конфіденційною інформацією, що становить комерційну таємницю, який здійснюється окремою особою/ організацією з приватною метою її використання для отримання конкурентних переваг/доходу від продажу зацікавленим особам без дозволу власника інформації з порушенням законодавчих та етичних норм.

Висновки. Проведене дослідження підтверджує важливість вивчення питань промислового шпигунства в умовах збільшення частки комерційної таємниці в структурі портфелю інтелектуальної власності та підвищення її значення у посиленні конкурентоспроможності компаній у національному та світовому інноваційному просторі.

Розгляд промислового шпигунства у площині його співставлення з іншими категоріями в означеній сфері показує неоднозначність їх трактування у фаховій літературі, з наявністю варіантів ототожнень, взаємозамінного, синонімічного використання, певного перетину сутнісних ознак, що є свідченням складності, багатоаспектності досліджуваної проблематики.

З'ясування існуючих підходів до розуміння промислового, економічного, корпоративного шпигунства, конкурентної розвідки дозволяє встановити їх самостійність як окремих категорій, водночас, визначити наявність спільних та відмінних ознак як форм отримання доступу до комерційно цінної інформації. Це допомагає більш чіткому розумінню промислового шпигунства, виділенню його ключових ознак та сутнісних характеристик.

Отримані результати в теоретико-методологічному контексті сприятимуть подальшому дослідженню теоретичних та прикладних аспектів даної теми, зокрема, в контексті більш глибокого вивчення сутнісних характеристик промислового шпигунства; виділення та розгляду його видів й інструментів, особливо в умовах діджиталізації; розробки системи захисту комерційної таємниці від несанкціонованого доступу, що є напрямами подальших розвідок у визначеній сфері досліджень.

Список використаних джерел:

1. Андрощук Г. Економічне шпигунство: зростання масштабів і агресивності. Частина 1. *Наука, технології, інновації.* 2018. № 3. С. 39–49. URL: http://dspace.nbuv.gov.ua/handle/123456789/162638
2. Ciuriak D., Ptashkina M. Quantifying Trade Secret Theft: Policy Implications. Centre for International Governance Innovation. 2021. URL: https://www.cigionline.org/static/documents/documents/no.253.pdf
3. Linton K. The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research. *Journal of International Commerce and Economics.* Published electronically September 2016. URL: https://www.usitc.gov/publications/332/journals/katherine_linton_importance_of_trade_secrets_0_0.pdf
4. Oxford Learners Dictionaries.Espionage. URL: https://www.oxfordlearnersdictionaries.com/definition/english/espionage
5. Merriam-Webster's Dictionary. Espionage. URL: https://www.merriam-webster.com/dictionary/espionage
6. Crane A. In the company of spies: when competitive intelligence gathering becomes industrial espionage. *Business Horizons*. 2005. No. 48 (3). P. 233–240. DOI: https://doi.org/10.1016/j.bushor.2004.11.005
7. Easttom W.C. Industrial Espionage in Cyberspace. *Computer Security Fundamental.* 2023. 5th Edition. 576 p. URL: https://www.pearsonitcertification.com/articles/article.aspx?p=3172433
8. Reisman A. A taxonomic view of illegal transfer of technologies: a case study. *Journal of Engineering and Technology Management.* 2006. Volume 23 (4). P. 292–312. DOI: https://doi.org/10.1016/j.jengtecman.2006.08.001
9. Neta D. Corporate Espionage: Prevent, Detect, and Respond. 2024. URL: https://axeligence.com/corporate-espionage-prevent-detect-and-respond/
10. Garner B.A. Black's Law Dictionary. (8th Edition). 2004. Thomson West. 1810 p.
11. Cambridge Dictionary. Industrial espionage. URL: https://dictionary.cambridge.org/dictionary/english/industrial-espionage
12. Counterintelligence:CorporateEspionage.NWCLibrary's.URL:https://usnwc.libguides.com/c.php?g=661096&p=5258510
13. Jameson D.A. The rhetoric of industrial espionage: the case of Starwood v. Hilton. *Business Communication Quarterly*. 2011. Volume 74 (3). P. 289–297. DOI: https://doi.org/10.1177/1080569911413811
14. Sutherland I. Industrial espionage from residual data: risks and countermeasures. Proceedings of the 6th Australian Digital Forensics Conference. Edith Cowan University. 2008. P. 167–172. DOI: https://doi.org/10.4225/75/57b2771540cc2
15. Якубівська Ю.Є. Цільові атаки в контексті промислового шпигунства. 2014. URL: http://dspace.wunu.edu.ua/jspui/bitstream/316497/1537/1/10_%D1%84%D0%B0%D1%85.pdf
16. Kovacich G. L. Netspionage – the global threat to information, Part I: what is it and why i should care? *Computers & Security.* 2000. Volume 19 (4). P. 326–336. DOI: https://doi.org/10.1016/S0167-4048(00)04020-7
17. Kenton W. Industrial Espionage: Definition, Examples, Types, Legality. 2022. URL: https://www.investopedia.com/terms/i/industrial-espionage.asp
18. Jones A. Industrial espionage in a hi-tech world. *Computer Fraud & Security*. 2008. Volume 1. P. 7–13. DOI: https://doi.org/10.1016/S1361-3723(08)70010-1
19. Hou T., Wang V. Industrial espionage – A systematic literature review. *Computer & Security*. 2020. Volume 98. URL: https://www.sciencedirect.com/science/article/pii/S0167404820302923
20. Nasheri H. Economic Espionage and Industrial Spying. 2005. Cambridge University Press. 288 p.
21. Beattie A. Corporate Espionage: Fact And Fiction. 2022. URL: https://www.investopedia.com/financial-edge/0310/corporate-espionage-fact-and-fiction.aspx
22. Wimmer B. Business Espionage: Risks, Threats, and Countermeasures. 2015. Butterworth-Heinemann. 1st edition. 204 p.
23. EEA. The Economic Espionage Act (1996). Public Law 104–294-OCT. 11, § 183. URL: https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf
24. Wagner R.E. Bailouts and the potential for distortion of federal criminal law: industrial espionage and beyond. *Tulane Law Review.* 2012. Volume 86 (5). P. 1017–1055.
25. Søilen K. S. Economic and industrial espionage at the start of the 21st century–status quaestionis. *Journal of Intelligence Studies in Business.* 2016. Volume 6 (3). P. 51–64. DOI: https://doi.org/10.37380/jisib.v6i3.196
26. Gibbs E. The new face of corporate espionage and what can be done about. 2022. URL: https://www.securitymagazine.com/articles/98087-the-new-face-of-corporate-espionage-and-what-can-be-done-about-it
27. What is Corporate Espionage? URL: https://securiti.ai/glossary/corporate-espionage/
28. Vashisth A., Kumar A. Corporate espionage: the insider threat. *Business Information Review*. 2013. No. 30 (2). P. 83–90. DOI: https://doi.org/10.1177/0266382113491816
29. Gartner Glossary. Competitive Intelligence. URL: https://www.gartner.com/en/information-technology/glossary/ci-competitive-intelligence
30. Watchmycompetitor. The 10 benefits of using competitive intelligence in 2023. URL: https://www.watchmycompetitor.com/resources/the-10-benefits-of-using-competitive-intelligence/
31. Bloomenthal A. Competitive intelligence: definition, types, and uses. 2022. URL: https://www.investopedia.com/terms/c/competitive-intelligence.asp
32. Андрощук Г. Економічне шпигунство: масштаби і агресивність зростають. Частина 1. 2018. URL: http://surl.li/paxbn
33. Якубівська Ю.Є. Вплив промислового шпигунства на сферу інтелектуальної власності. *Зовнішня торгівля: економіка, фінанси, право.* 2013. № 4 (69). С. 158–162. URL: http://zt.knute.edu.ua/files/2013/4(69)/uazt_2013_4_24.pdf
34. SCIP. Code of ethics for CI professionals. strategic and competitive intelligence professionals. URL: https://www.scip.org

References:

1. Androshchuk H. (2018) Ekonomichne shpyhunstvo: zrostannia masshtabiv i ahresyvnosti. Chastyna 1. *Nauka, tekhnolohii, innovatsii,* no. 3, pp. 39–49. Available at: http://dspace.nbuv.gov.ua/handle/123456789/162638
2. Ciuriak D., Ptashkina M. (2021) Quantifying Trade Secret Theft: Policy Implications. Centre for International Governance Innovation. Available at: https://www.cigionline.org/static/documents/documents/no.253.pdf

3. Linton K. (September, 2016) The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research. *Journal of International Commerce and Economics.* Available at: https://www.usitc.gov/publications/332/journals/katherine_linton_importance_of_trade_secrets_0_0.pdf

4. Oxford Learners Dictionaries (n.d.) Espionage. Available at: https://www.oxfordlearnersdictionaries.com/definition/english/espionage

5. Merriam-Webster's Dictionary (n.d.) Espionage. Available at: https://www.merriam-webster.com/dictionary/espionage

6. Crane A. (2005) In the company of spies: when competitive intelligence gathering becomes industrial espionage. *Business Horizons*, no. 48 (3), pp. 233–240. DOI: https://doi.org/10.1016/j.bushor.2004.11.005

7. Easttom W. C. (2023) Industrial Espionage in Cyberspace. *Computer Security Fundamentals,* 5th Edition. 576 p. Available at: https://www.pearsonitcertification.com/articles/article.aspx?p=3172433

8. Reisman. A. (2006) A taxonomic view of illegal transfer of technologies: a case study. *Journal of Engineering and Technology Management*, vol. 23 (4), pp. 292–312. DOI: https://doi.org/10.1016/j.jengtecman.2006.08.001

9. Neta D. (2024) Corporate Espionage: Prevent, Detect, and Respond. Available at: https://axeligence.com/corporate-espionage-prevent-detect-and-respond/

10. Garner B. A. (2004) *Black's Law Dictionary*. (8th Edition). Thomson West. 1810 p.

11. Cambridge Dictionary (n.d.) Industrial espionage. Available at: Available at: https://dictionary.cambridge.org/dictionary/english/industrial-espionage

12. Counterintelligence: Corporate Espionage (n.d.) NWC Library's. Available at: https://usnwc.libguides.com/c.php?g=661096&p=5258510

13. Jameson D. A. (2011) The rhetoric of industrial espionage: the case of Starwood v. Hilton. *Business Communication Quarterly*, vol. 74 (3), pp. 289–297. DOI: https://doi.org/10.1177/1080569911413811

14. Sutherland I. (2008) Industrial espionage from residual data: risks and countermeasures. *Proceedings of the 6th Australian Digital Forensics Conference*. Edith Cowan University, pp. 167–172. DOI: https://doi.org/10.4225/75/57b2771540cc2

15. Yakubivska Yu. (2014) Tsilovi ataky v konteksti promyslovoho shpyhunstva. Available at: http://dspace.wunu.edu.ua/jspui/bitstream/316497/1537/1/10_%D1%84%D0%B0%D1%85.pdf

16. Kovacich G. L. (2000) Netspionage – the global threat to information, part I: what is it and why i should care? *Computers & Security,* vol. 19 (4), pp. 326–336. DOI: https://doi.org/10.1016/S0167-4048(00)04020-7

17. Kenton W. (2022) Industrial Espionage: Definition, Examples, Types, Legality. Available at: https://www.investopedia.com/terms/i/industrial-espionage.asp

18. Jones A. (2008) Industrial espionage in a hi-tech world. *Computer Fraud & Security*, vol. 1. pp. 7–13. DOI: https://doi.org/10.1016/S1361-3723(08)70010-1

19. Hou T., Wang V. (2020) Industrial espionage – A systematic literature review. *Computer & Security*, vol. 98. Available at: https://www.sciencedirect.com/science/article/pii/S0167404820302923

20. Nasheri H. (2005) Economic Espionage and Industrial Spying. Cambridge University Press. 288 p.

21. Beattie A. (2022) Corporate Espionage: Fact And Fiction. Available at: https://www.investopedia.com/financial-edge/0310/corporate-espionage-fact-and-fiction.aspx

22. Wimmer B. (2015) Business Espionage: Risks, Threats, and Countermeasures. Butterworth-Heinemann. 1st edition. 204 p.

23. EEA. The Economic Espionage Act (1996). Public Law 104–294-OCT. 11, § 183. Available at: https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf

24. Wagner R. E. (2012) Bailouts and the potential for distortion of federal criminal law: industrial espionage and beyond. *Tulane Law Review,* vol. 86 (5), pp. 1017–1055.

25. Søilen K. S. (2016) Economic and industrial espionage at the start of the 21st century–status quaestionis. *Journal of Intelligence Studies in Business,* vol. 6 (3), pp. 51–64. DOI: https://doi.org/10.37380/jisib.v6i3.196

26. Gibbs E. (2022) The new face of corporate espionage and what can be done about. Available at: https://www.securitymagazine.com/articles/98087-the-new-face-of-corporate-espionage-and-what-can-be-done-about-it

27. What is Corporate Espionage? (n.d.). Available at: https://securiti.ai/glossary/corporate-espionage/

28. Vashisth A., Kumar A. (2013) Corporate espionage: the insider threat. *Business Information Review*, no. 30 (2), pp. 83–90. DOI: https://doi.org/10.1177/0266382113491816

29. Gartner Glossary (n.d.) Competitive Intelligence. Available at: https://www.gartner.com/en/information-technology/glossary/ci-competitive-intelligence

30. Watchmycompetitor (n.d.) The 10 benefits of using competitive intelligence in 2023. Available at: https://www.watchmycompetitor.com/resources/the-10-benefits-of-using-competitive-intelligence/

31. Bloomenthal A. (2022) Competitive intelligence: definition, types, and uses. Available at: https://www.investopedia.com/terms/c/competitive-intelligence.asp

32. Androshchuk H. (2018) Ekonomichne shpyhunstvo: masshtaby i ahresyvnist zrostaiut. Chastyna 1. *Oboronno-promyslovyi kurier*. Available at: http://surl.li/paxbn

33. Yakubivska Yu. (2013) Vplyv promyslovoho shpyhunstva na sferu intelektualnoi vlasnosti. *Zovnishnia torhivlia: ekonomika, finansy, pravo,* no. 4 (69), pp. 158–162. Available at: http://zt.knute.edu.ua/files/2013/4(69)/uazt_2013_4_24.pdf

34. SCIP (n.d.) Code of ethics for CI professionals. strategic and competitive intelligence professionals. Available at: https://www.scip.org