

**Бринзяник Марія Василівна**, *магістрантка,*  
**Ляхович Діана Степанівна**, *викладач кафедри*  
*міжнародної економіки, маркетингу і менеджменту*

## **ПРОМИСЛОВЕ ШПИГУНСТВО ЯК ЗАГРОЗА ФІНАНСОВО-ЕКОНОМІЧНИЙ БЕЗПЕЦІ ПІДПРИЄМСТВ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ**

Промислове шпигунство здійснюється різними компаніями і деякими державними установами. Не викликає жодних сумнівів, що промисловий шпигунство є легітимною формою підприємницької діяльності, оскільки він спрямований на отримання інформації, що безпосередньо відображає діяльність національних компаній. Промислове шпигунство сприймається урядами деяких країн як засіб придбання певного типу технології.

Для того, щоб захистити компанію від актів промислових шпигунів, шахраїв і розчарованих працівників, вище керівництво може прийняти проактивний підхід до контррозвідки. Можна створити підрозділ корпоративної розвідки, який також має вимір безпеки. Підрозділ корпоративної розвідки може діяти як зв'язок між компанією та її складовими частинами, а також різними урядовими установами. Це має забезпечити належне використання різних моделей та інструментів стратегічного управління, що використовуються стратегами та планувальниками компанії щодо розробки та впровадження стратегії.

Розслідування французької автомобільної компанії Renault, розробка електричних автомобілів стала жертвою передбачуваного промислового шпигунства, показало, що задіяно декілька китайських компаній. Учасник розслідування, який виявив бажав залишитися анонімним, показав, що ключі також ведуть до іноземної компанії за межами Китаю. Він відмовився розкривати імена китайських компаній, а другий – учасник промислового шпигунства [1].

Міністерство юстиції США розпочало розслідування справи Huawei за фактом індустріального шпигунства. Це є результатом звинувачення телекомунікацій T-Mobile в США, що китайський технологічний гігант вкрав бізнес-секрети, наприклад, робота для тестування смартфонів. Місцевий суд в Сіетлі вважає, що Huawei, як ключовий постачальник смартфонів, отримала доступ до лабораторій T-Mobile. З них китайський гігант вдалося викрасти програмний код, частини та інші комерційні секрети від американського оператора [2].

На думку Т. Ткачук, “саме поняття “шпигунство” означає одержання або добування якихось відомостей, що становлять певний інтерес. З розвитком бізнесу потреба в інформації про конкурентів, клієнтів або партнерів набуває дедалі більшої актуальності для успішного функціонування підприємства.

Промислове шпигунство щодо бізнесу – це різновид економічного шпигунства, якому властиве звуження масштабів завдань з одержання інформації, що цікавить, від державного масштабу до масштабу однієї або

декількох фірм-конкурентів. Отже, для бізнесу промислове шпигунство – лише спосіб конкурентної боротьби [3, с. 73].

Промислове шпигунство – це добування протизаконним шляхом конфіденційних відомостей про діяльність конкурентів, розкрадання відомостей, зі складових ноу-хау, ведення недобросовісної конкуренції, одержання персональних даних для їх використання в злочинних цілях. Сучасне промислове шпигунство – це ще й свідоме приведення в непридатність виробничого обладнання, інформаційних систем, здійснення психологічного тиску на співробітників з метою дестабілізації діяльності конкурента [4].

Сукупність методів промислового шпигунства зображено на рис. 1.



**Рис. 1 Методи промислового шпигунства**

Таким чином, для ефективної діяльності національних компаній в умовах випереджаючого розвитку технологій, необхідним є процес розробки стратегії захисту господарської інформації, а особливо комерційної таємниці підприємств. Як показує іноземний досвід, процвітання підприємства неможливе без ведення успішної конкурентної діяльності.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. *Китайські компанії са замесени в индустриалния шпионаж над Renault* <https://www.investor.bg/evropa/334/a/industrialen-shpionaj-zastrashava-kliuchovi-aktivi-na-renault-110636/> (дата звернення: 02.05.2019).
2. *САЩ разследват Huawei за индустриален шпионаж* <https://www.techrends.bg/2019/01/17/us-doj-huawei-investigation/> (дата звернення: 02.05.2019).
3. *Ткачук Т. Характерні особливості конкурентної розвідки та промислового шпигунства. Персонал. 2007. № 2. С.72-78.*
4. *Зеркалов Д.В. Безопасность бизнеса. Контрразведка и шпионаж. К.: Наук. світ, 2008. 366 с.*

---

**Брус Олександр Ігорович, магістрант,  
Загурський Олександр Богданович, к.ю.н., доцент,  
доцент кафедри гуманітарних і  
фундаментальних дисциплін**

**ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТІВ  
ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ В РЕСПУБЛІЦІ БОЛГАРІЯ В  
УМОВАХ ГЛОБАЛЬНОЇ КОНКУРЕНЦІЇ**

За оцінками світового рейтингового агентства, в Республіці Болгарія очікується суттєве зростання ВВП у період 2018-2021 рр., зумовлене сильним внутрішнім споживанням та прискоренням інвестицій. Постійне поглинання фондів ЄС та посилення умов на ринку праці сприятимуть підвищенню продуктивності протягом багатьох років.

До того ж, агентство вважає, що ці прагнення до членства в євросоні також підтримуватимуть продовження зусиль країни щодо усунення існуючих інституційних і структурних проблем. S&P Global Ratings підвищить кредитний рейтинг, якщо болгарський лев увійде до ЕРМ II, що сприятиме подальшій довірі та ефективності монетарної політики [1].

У більшості болгарських підприємств, які вирішили прийняти заходи безпеки, економічна безпека закінчується електронними системами безпеки і або контрактом з технічною службою безпеки. Аналізуючи ці дві складові, багато керівників не розуміють, що це лише елементи корпоративної безпеки і, як правило, є останньою лінією захисту, призначеною для роботи, коли інші не працюють.

Компанії, як правило, вирішують питання безпеки в частині, як стосовно окремих елементів, так і стосовно окремих об'єктів і видів діяльності. Інші види загроз для підприємства та бізнесу недооцінюються. Саме тут виникають більшість проблем економічної безпеки.

Економічна безпека підприємства – це комплекс взаємопов'язаних видів діяльності. Все повинно бути заздалегідь узгоджене і розроблене як єдина система під назвою “Концепція економічної безпеки підприємства”. Економічна безпека підприємства може бути визначена як сукупність конкретних дій та структури для фізичного та інформаційного захисту людей,