УДК 339.166:343.534(045)

Якубівська Ю. Є., *к.е.н., ст. викладач кафедри фінансово-економічної безпеки Тернопільського національного економічного університету*

ВПЛИВ ПРОМИСЛОВОГО ШПИГУНСТВА НА СФЕРУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Розглянуто особливості промислового шпигунства як загрози для сфери інтелектуальної власності, дано характеристику факторів, що сприяють розвитку даного явища в Україні, проаналізовано прояви промислового шпигунства на світовому рівні. На основі отриманих результатів визначено основні форми промислового шпигунства та шляхи боротьби з ними.

Ключові слова: *промислове шпигунство, інтелектуальна власність, економічна безпека, кіберзлочинність, програмне забезпечення.*

Літ. *10.*

Якубивская Ю. Е., *к.э.н., ст. преподаватель кафедры финансово-экономической безопасности Тернопольского национального экономического университета*

ВЛИЯНИЕ ПРОМЫШЛЕННОГО ШПИОНАЖА НА СФЕРУ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Рассмотрены особенности промышленного шпионажа как угрозы для сферы интеллектуальной собственности, дана характеристика факторов, способствующих развитию данного явления в Украине, проанализированы проявления промышленного шпионажа на мировом уровне. На основе полученных результатов определены основные формы промышленного шпионажа и пути борьбы с ними.

Ключевые слова: *промышленный шпионаж, интеллектуальная собственность, экономическая безопасность, киберпреступность, программное обеспечение.*

Yakubivska Yuliya*, PhD, Senior Lecturer of Financial and Economic Security Department in Ternopil National Economic University*

THE INFLUENCE OF INDUSTRIAL ESPIONAGE ON THE INTELLECTUAL PROPERTY SPHERE

The article is concerned with an industrial espionage features as a threat for intellectual property sphere; the characteristic of factors that contribute this phenomenon development in Ukraine is given; industrial espionage in the context of the global economic level is analyzed. According to the results the main forms of industrial espionage and ways of its combating are determined.

Keywords: industrial espionage*, intellectual property, economic security, cybercrime, software.*

Постановка проблеми. У сучасних умовах інтелектуальної незахищеності промислове шпигунство, як цілеспрямований збір інтелектуальних і конфіденційних даних у неетичній та незаконній формі, стрімко процвітає та включає в себе співробітників, що працюють в якості таємних агентів, хакерів, найнятих команд зломщиків, збору, вивчення сміттєвих контейнерів, прослуховування приладів зв'язку тощо. Українські компанії не володіють інформацією про практику промислового шпигунства. Адже національне законодавче забезпечення захисту від даного прецеденту перебуває на стадії розробки. У той же час акти промислового шпигунства підпадають під компетенцію кримінального законодавства, що стосується крадіжки, незаконного проникнення тощо. Основна філософія промислового шпигунства полягає в гіпотезі – «навіщо витрачати час та кошти на дослідження, розробку та розвиток, якщо можливо підкупити співробітника серед персоналу конкурента».

Аналіз останніх досліджень і публікацій. Питання впливу промислового шпигунства на сферу інтелектуальної власності лежить в основі таких вчених, як: Н. Андерсон [4], М. Ахмед [8], П. Бреіген [7], Т. Гловер [6], С. Девіс [9], Н. Волкер [5], Т.Райт [3] та ін. Зважаючи на

той факт, що категорія промислового шпигунства в українській економічній літературі ще не є достатньо висвітленою, дослідження за темою даної наукової статті побудоване переважно на опрацюванні зарубіжних джерел. Переважна більшість наукових праць присвячена нормативно-правовому захисту від промислового шпигунства. Однак потребують детальнішого аналізу економічні аспекти, пов'язані з явищем промислового шпигунства, яке особливо активно розвивається з боку Китаю, Росії, України та інших країн. Даний процес негативно відображається не лише на системі економічної безпеки високорозвинених, але й країн з перехідною економікою. На основі опрацювання публікацій та національних нормативно-правових актів по даній тематиці можемо зробити висновок про негативний вплив промислового шпигунства на економіки країн світу, а результативність впливу даного явища на ринок інтелектуальної власності не може вважатися повністю дослідженим та потребує детальнішого аналізу як на міжнародному, так і на національному рівнях, чим і пояснюється **актуальність** теми даної наукової статті.

Метою статті є дослідження впливу промислового шпигунства на сферу інтелектуальної власності. Задля досягнення вищевказаної мети потребують вирішення наступні **завдання**:

- сформулювати фактори виникнення промислового шпигунства в Україні;
- дослідити категоріальний апарат промислового шпигунства, цілі й форми його здійснення;
- проаналізувати випадки промислового шпигунства на міжнародному рівні;
- сформулювати висновки, в яких визначити основні форми промислового шпигунства, а також шляхи боротьби з ним.

Виклад основного матеріалу. Промислове шпигунство є комерційним шпигунством на шляху незаконного отримання бізнес-інформації та новітніх технологій для досягнення конкурентної переваги. Більшість компаній в Україні постійно стають жертвами одного з видів діяльності кіберзлочинів – промислового шпигунства. Це пов'язано з чотирма факторами.

По-перше, рівень економічної безпеки України є дуже ненадійним, коли мова йде про кіберзлочинність. За винятком банків, українські компанії зробили дуже мало для зниження рівня промислового шпигунства, який в здійснюється переважно через так званий комп'ютерний злом.

По-друге, в Україні не вистачає фахівців з інформаційної безпеки і таким чином дана функція покладається на іноземні компанії. У деяких випадках ці іноземні компанії, які видають себе за приватні охоронні фірми, насправді виступають в ролі промислових «розвідників», що проводять моніторинг незахищених об'єктів права інтелектуальної власності на території України, співпрацюючи з вітчизняними конкурентами в своїй країні.

По-третє, хоча уряд України усвідомлює, що національні суб'єкти господарювання та органи державної влади доволі часто виступають жертвами промислового шпигунства, в установах державної влади не вистачає технічних фахівців для боротьби з кіберзлочинністю.

По-четверте, національна законодавча база у сфері захисту від промислового шпигунства потребує гармонізації та вдосконалення. Важливим позитивним кроком на шляху захисту від промислового шпигунства для нашої держави стало схвалення Кабінетом Міністрів 06.03.2013 р. змін до Закону України «Про основи національної безпеки України» [1] щодо питання про кібербезпеку. Одне з положень цього Закону визначає поняття «кібернетична безпека (кібербезпека)» і «кібернетичний простір (кіберпростір)», що є новими у сфері економічної безпеки для України. Однак, недотримання Закону провокує Інтернет-сайти на величезний ризик. Даний проект Закону був розроблений Міністерством внутрішніх справ на виконання доручень Кабінету Міністрів, поданих відповідно до рішення Ради національної безпеки і оборони України від 25.05. 2012 р. «Про заходи щодо посилення боротьби з тероризмом в Україні» [2].

Наведені чотири фактори характеризують зростання рівня промислового шпигунства в Україні, але водночас і вказують на потребу посилення інтересу органів державної влади до вирішення даної проблеми. Необхідним є державно-приватне партнерство для боротьби з зазначеним явищем, а також співпраця органів державної влади, підприємницьких структур та університетів у контексті формування кваліфікованих людських ресурсів, що були б залучені у

боротьбі з промисловим шпигунством, кіберзлочинністю та порушенням права інтелектуальної власності загалом. Якщо Україна прагне процвітати в умовах жорсткої конкуренції та глобалізації, необхідно розглядати такі дії, щоб захистити національну інтелектуальну власність.

Промислове шпигунство в Україні відбувається як прийнятний спосіб ведення бізнесу, без наявності ефективного чинного законодавства для запобігання цьому. В Україні була спроба використовувати кримінальні закони з метою протидії промисловому шпигунству, однак останні не охоплюють понять крадіжки або неправильного збору конфіденційної інформації зокрема. Очевидно, що в сфері бізнесу на сьогодні інформація є більш цінною ніж колинебудь. Кожне підприємство є вразливим до крадіжки інформації. Близько 85% випадків промислового шпигунства здійснюються співробітниками підприємств, безпека котрих стосується насамперед захисту від зовнішніх загроз, не зважаючи на витік інформації через внутрішні елементи. У зв'язку з цим компанії повинні змінити спосіб формування безпеки у сфері інтелектуальної власності, визначити свої цінні інформаційні ресурси, а також потенційний перелік конкурентів, що зацікавлені в них. Крім того, необхідним є проведення перевірок керівниками підприємств, що володіють конфіденційною інформацією чи комерційними таємницями, фахівців програмного забезпечення. Адже, маючи безпосередній доступ до бази даних компанії, можливим стає підкуп недобросовісних програмістів, занесення «троянів» в корпоративну комп'ютерну систему, і тим самим створення можливого шляху для витоку конфіденційної інформації з підприємства. Законодавство, однак, не завжди захищає від протиправних дій, вчинених промисловим шпигуном, що підлягає цивільному або кримінальному переслідуванню. Особливості конфіденційної інформації, що є вкраденою, широко оприлюднюються в ході судового процесу, який є наслідком правових норм з метою досягнення справедливості, в результаті чого компанія, що постраждала від протиправного промислового шпигунства, повинна оприлюднити той же обсяг інформації, який вона намагається захистити, в результаті чого значення конфіденційної інформації нівелюється.

Крадіжка комерційних таємниць здійснюється шляхом видалення, копіювання або запису конфіденційної та цінної інформації в компанії для використання конкурентами. Промислове шпигунство ведеться в комерційних цілях, а не національних цілях безпеки, і повинно бути диференційованим від конкурентної розвідки, яка є юридичною категорією, що характеризує збір інформації шляхом вивчення корпоративних видань, сайтів, патентних заявок тощо, щоб визначити специфіку діяльності корпорації. Промислове шпигунство включає таємні операції, такі, як: розкрадання комерційних таємниць, підкуп, шантаж і технологічний нагляд. Економічне шпигунство ведеться або організовується урядом і набуває рис міжнародного масштабу, у той час як промислове та корпоративне шпигунство здійснюється на національному рівні і відбувається між компаніями або корпораціями. Конкурентна розвідка та економічний шпіонаж хоч і є доволі схожими поняттями, однак володіють відмінностями, що залежать насамперед від особливостей досягнення поставленої мети. Конкурентна розвідка описує специфіку правової та етичної діяльності щодо систематичного збору, аналізу та управління інформацією про промислових конкурентів. Це включає в себе такі види діяльності, як вивчення газетних статей, корпоративних видань, сайтів, патентних заявок, спеціалізовані бази даних, інформації на виставках, що дає змогу визначити інформацію про корпорацію. В економічних реаліях «конкурентна розвідка» була описана як «застосування принципів та практики військової та національної розвідки у сфері глобального бізнесу» [5]. Різниця між конкурентною розвідкою та економічним чи промисловим шпигунством не є чітко окресленою та потребує гармонізації як у нормативно-правовому плані, так і в економічному категоріальному апараті. Науковці, дослідження котрих присвячені вивченню особливостей боротьби із промисловим шпигунством, стверджують, що іноді дуже важко відрізнити легальні й нелегальні методи боротьби, особливо якщо зважати на етичний бік збору інформації.

Економічний і промисловий шпіонаж найчастіше пов'язані з технологією важкої промисловості, включаючи комп'ютерне програмне забезпечення та апаратне забезпечення, біотехнології, аерокосмічну промисловість, телекомунікації, транспорт і технології двигунів, виро-

бництво автомобілів, верстатів, енергії, матеріалів і покриття. Силіконова долина, одна з найактивніших у світі територій за кількістю звинувачень у промисловому шпигунстві. Останнім часом економічний або промисловий шпіонаж розглядаються в широкому значенні. Наприклад, підприємство, котре намагається саботувати, може вважатися промисловим шпигуном, і в цьому значенні термін «саботаж» прирівнюється до порушення законодавства. У зв'язку з цим промислове шпигунство і саботаж (напр., корпоративний) стали більш чітко пов'язані один з одним, підтвердженням чого стали дослідження, що проводилися урядами країн. Уряд США в даний час здійснює перевірку на детекторі брехні під назвою «Тест у шпигунстві і саботажі» (TES), сприяючи вивченню та впровадженню можливих контрзаходів при виникненні шпигунства і саботажу, визначаючи взаємозв'язки між ними [8].

Економічне або промислове шпигунство зазвичай відбувається в одному з двох способів. По-перше, незадоволений працівник присвоює інформацію для просування своїх власних інтересів або з метою завдання шкоди компанії. По-друге, конкурент або іноземний уряд шукає інформацію для просування своїх власних технологічних або фінансових інтересів. Залучення довірених інсайдерів, як правило, вважається кращим джерелом економічного і промислового шпигунства. Причинами такої поведінки є не лише добровільні засади, але й засоби примусу та тиску (наприклад, під загрозою вчинення злочину, підкупу в передачі матеріалу). Такі випадки є доволі поширеними, однак у результаті призводять до подачі судових позовів.

Деякі країни світу залучають зовнішні людські ресурси для виконання завдань, що стосуються промислового шпигунства, а не використовують свої власні спецслужби. Такими суб'єктами найчастіше виступають учені, бізнес-делегати та студенти, що використовуються урядами в зборі інформації. У деяких країнах, наприклад, в Японії, проводять опитування студентів по поверненні додому з інших країн. Промисловим шпигуном може бути турист, що, наприклад, перебуває на екскурсії на фабриці, після чого передає отримані дані заінтересованій стороні, якою найчастіше виступає конкурент підприємства, інженер, технік з обслуговування, страховий агент або інспектор, тобто в основному ті, хто мають законний доступ до приміщення. Способів отримання необхідної інформації є безліч: шпигун може увірватися у приміщення для крадіжки даних, шукати в макулатурі, інформація може бути скомпрометована через небажані запити про інформацію, маркетингові дослідження або використання технічних засобів підтримки, дослідження специфіки програмного забезпечення тощо.

Розвиток Інтернету та комп'ютерних мереж розширив діапазон та деталізацію інформації, водночас полегшивши доступ до неї з метою промислового шпигунства. У всьому світі близько 50000 компаній в день підпадають під кібератаку, і даний показник характеризується щорічним подвоєнням [6]. Зазначений тип операції, як правило, надає незаконний доступ до особистої, фінансової та аналітичної інформації зловмисникам або окремим хакерам. Конфіденційна інженерна, військова чи оборонна інформація не може мати безпосереднього грошового вираження при скоєнні злочину в порівнянні з банківськими реквізитами, оскільки підпадає під гриф секретності. Кібератака, як кримінальна категорія, вимагає від зловмисника глибокого знання мережі Інтернет, стратегій цілеспрямованих атак, підзвітних кваліфікованих людських ресурсів, діючих організовано.

Зростання показника використання Інтернету також розширило можливості для промислового шпигунства з метою саботажу. На початку XXI сторіччя було відмічено, що енергетичні компанії все частіше підпадають під атаку хакерів. Бази даних у сфері енергетичних систем містять інформацію про моніторинг електричних мереж та води, що є відокремленою від інших даних у системі комп'ютерних мереж; у даний час такі бази даних підключені до системи Інтернет, залишаючись уразливими, якщо за ними не закріплені вбудовані функції безпеки. Використання методів промислового шпигунства все частіше стає проблемою для уряду у зв'язку з потенційною атакою з боку терористичних груп чи ворожих іноземних урядів.

Одним із факторів, що спричиняє виникнення промислового шпигунства є незахищеність програмного забезпечення комп'ютера, а саме використання шкідливих програм, як інструменту для промислового шпигунства, що здійснюється з метою передачі цифрових копій комер-

ційних таємниць, клієнтських баз даних, стратегічних планів і контактів. Нові види шкідливих програм таємно фіксують необхідну інформацію на камеру мобільного телефону чи записуючі пристрої. З метою вирішення таких незаконних нападів на інтелектуальну власність компанії все частіше зберігають важливу інформацію поза мережею Інтернет, використовують спеціальні електромагнітні пристрої, щоб не допустити передачі даних через мобільний телефон.

Висновки з дослідження і перспективи подальших розвідок у даній темі. Отже, економічне або промислове шпигунство на даний час відбувається в двох основних формах:

1. Збір знань та придбання такої інтелектуальної власності як: інформація про промислове виробництво, ідеї, методи і процеси, рецепти, формули.

2. Отримання матеріального права власності на об'єкти інтелектуальної власності, оперативної інформації (бази даних на клієнтів, ціноутворення, обсяги продажу, особливості маркетингу, проекти для досліджень і розробок, політику, перспективні пропозиції, планування і маркетингові стратегії або зміна композиції і місця виробництва). Даний аспект включає такі види правопорушень, як крадіжка комерційної таємниці, підкуп, шантаж і технологічний нагляд. Суб'єктами промислового шпигунства виступають не лише підприємства, але й урядові організації (наприклад, щоб визначити умови тендеру на державний контракт таким чином, що інший учасник торгів на перспективу зможе знижувати ціну).

Уряди високорозвинених країн світу ведуть активну боротьбу з промисловим шпигунством: впроваджують використання різного роду кодів доступу до інформації, захищають комерційні таємниці, перевіряють працівників підприємств, рекомендують підписання договорів про нерозголошення конфіденційної інформації, фінансово підтримують високотехнологічний сектор, акцентують увагу на стратегічному управлінні у воєнній та оборонній сферах. Україна потребує впровадження передового досвіду цих країн на шляху гармонізації законодавства у сфері інтелектуальної власності, що стосується мінімізації рівня промислового шпигунства, як в контексті захисту від посягань на конфіденційну інформацію, так і відносно унеможливлення виконання корупційних схем щодо отримання такого роду інформації на шляху промислового шпигунства, формування урядових програм підтримки інноваційного та високотехнологічного секторів. Перспективними вважаються подальші дослідження особливостей промислового шпигунства та шляхів уникнення правопорушень у сфері інтелектуальної власності в Україні.

Література

1. Закон України «Про основи національної безпеки України» від 19.06.2003 р. № 964-IV [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15
2. Рішення Ради національної безпеки і оборони України «Про заходи щодо посилення боротьби з тероризмом в Україні» від 25.05. 2012 р. [Електронний ресурс]. –Режим доступу: http://zakon4.rada.gov.ua/laws/show/n0001525-12
3. Wright P. Spycatcher. New York / Peter Wright // Viking, 2013. – 270 p.
4. Anderson N. Massive DDoS attacks target Estonia; Russia accused [Електронний ресурс] / Nate Anderson // Ars Technica. Retrieved, 2007. – Режим доступу: http://arstechnica.com /security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/
5. Walker N. Marketing: Know your enemy / Nick Walker // The Independent. Retrieved, 2010.
6. Glover T. Chinese hackers blamed for cyber attack wave [Електронний ресурс] / Tony Glover // This is Money, 2012. – Режим доступу: http://www.thisismoney.co.uk/ money/news/article-1687393/Chinese-hackers-blamed-for-cyber-attack-wave.html
7. Branigan T. Google to end censorship in China over cyber attacks [Електронний ресурс] / Tania Branigan // The Guardian. Retrieved, 2010. – Режим доступу: http://www.guardian.co.uk /technology/2010/jan/12/google-china-ends-censorship
8. Ahmed M. Google cyber-attack from China 'an inside job / Murad Ahmed // The Times. Retrieved, 2013.
9. DeWeese S. Capability of the People's Republic of Conduct Cyber Warfare and Computer Network Exploitation: Prepared for The US-China Economic and Security Review Commission / Steve DeWeese, Bryan Krekel, George Bakos, Christopher Barnet, Virginia McLean // USA: Northrop Grumman Corporation. Dongxiau Yue, et al., v. Chordiant Software, Inc., 2009. – 630 p.
10. Blakely R. MI5 alert on China's cyberspace spy threat / Rhys Blakely // The Times. 2013.

Стаття надійшла до редакції 9. 10. 2013 р.