to be a common element of conducting competitive intelligence, since it promotes capitalization and commitment among partners and consumers. By performing reputation, management functions and the function of developing corporate culture, the code builds trust in the organization, because the moral responsibility of employees means reliability and stability.

The main objectives of the research are: 1) to clarify the role of competitive intelligence in the information support of competitive organizations; 2) to study the practical application of competitive intelligence ethics; 3) to make recommendations to assess the level of professionalism and ethics of the competitive intelligence professionals. To solve the problems of the research several approaches were used, including: information approach (collection and analysis of information), system approach (study of the structure, relationships, function, nature and characteristics of system elements), synergetic approach (analysis of ways, results of future interactions).

The author discovered the importance and role of the ethics code in competitive intelligence; analyzed and identified the correct behavior of CI professionals at work; the research evaluation criteria of professionalism of CI professionals made it possible to determine the characteristics and skills that a professional should posses. It was emphasized that CI professionals should have the necessary ethical and professional skills, in particular, analytical, communication, ethical, network skills. On the basis of the SWOT-analysis, an assessment of the level of professionalism and the use of ethical norms in the work of CP-professionals has been conducted.

**Key words:** competitive intelligence, information ethics, CI-professional, code of ethics, infoethics..

Стаття надійшла до редколегії
05.05.2017 р.

**УДК 334:343.534**

**Тетяна Міщук,**
**Антоніна Митко**

# Особливості конкурентної розвідки та шпіонажу на підприємствах

У статті досліджено процеси промислового шпигунства та конкурентної розвідки як прихованих форм отримання конфіденційної

інформації конкурентів. Мета статті – проаналізувати особливості конкурентної розвідки й шпигунства на підприємствах. Із цією метою схарактеризовано понятійний апарат конкурентної розвідки й промислового шпигунства та їхні відмінності, розглянуто тенденції розвитку промислового шпигунства на світовому рівні на прикладах найбільших світових компаній. За допомогою історико-порівняльного методу здійснено ретроспективний аналіз конкурентної розвідки й шпіонажу на підприємствах. Розкрито прояви шпигунства в політичній сфері, зокрема на прикладі міжнародного соціального мережевого проекту «ВікіЛікс», а також проаналізовано наслідки політичної розвідки. На основі отриманих результатів запропоновано способи протидії шпигунству й розвідці на мікро- та макрорівнях.

Доведено, що в країнах із ринковою економікою завжди існували шпіонаж і конкурентна розвідка, мета яких – вивчення секретів, що лежать в основі досягнень та успіхів чужих підприємств і країн. Від них потерпають усі сфери економіки й не захищені навіть стратегічні компанії, що мають подвійний, воєнно-цивільний характер. Активною конкурентна розвідка та шпіонаж існують і в політичній сфері. Сьогодні різні кризи, які накладаються одна на одну, змушують політиків усе частіше звертатися до закулісних можливостей отримання інформації, ідей чи навіть прямого саботування дій інших країн.

Світовий досвід підтверджує неминуче виникнення загроз економічній безпеці країни в контексті поширення процесу промислового шпигунства. На сьогодні гостро стоїть завдання розробки єдиних механізмів захисту від інсайдерських загроз. Автори вважають, що у подальшому слід розробити методики оцінювання економічної ефективності впровадження систем захисту комерційної інформації та промислового шпіонажу.

**Ключові слова:** конкурентна розвідка, промисловий шпіонаж, інформаційна безпека, цільові атаки, кібершпіонаж, інсайдерська загроза.

**Постановка наукової проблеми та її значення.** У світі постійно відбувається інформаційна боротьба. Вона ведеться між державами, підприємствами та фірмами за захист власних інтересів. Очевидно, щоб не програти в цій боротьбі, потрібно вміти й знати способи протидії постійним «інформаційним нападам супротивника». Нинішній етап розвитку суспільства характеризується збільшенням ролі інформаційної сфери, яка є системоутворювальним фактором життя суспільства та значно впливає на стан політичної, економічної, соціальної й інших

складників безпеки комерційного підприємства.

Глобалізація зумовила необхідність не лише високої якості інформації, ефективності її накопичення, а й уміння належним чином її опрацьовувати та оптимально використовувати. Це передбачає визначення й уведення відповідних структур на підприємстві, які відповідатимуть за отримання, переробку та обіг інформації. Обмеження ризику стосовно діяльності підприємства безпосередньо пов'язано з наявністю інформаційних ресурсів й умінням оптимально їх використовувати. Потреба в упорядкованій інформації про оточення зумовлює необхідність системного інструменту, який передбачає відповідні зміни в структурі та функціонуванні підприємства. Таким інструментом може бути конкурентна розвідка підприємства.

Із розвитком суспільства масштаби промислового шпигунства різко зростають. Інформація про результати чужих досліджень щодо певного підприємства заощаджує власні сили й кошти та дає змогу зосередити всю увагу на виробництві й маркетингу. На сучасному етапі розвитку бізнесу потреба в інформації про конкурентів, клієнтів або партнерів надзвичайно важлива та актуальна для успішного функціонування підприємства.

**Мета статті** – проаналізувати особливості конкурентної розвідки й шпигунства на підприємствах, **завдання –** охарактеризувати категорію конкурентної розвідки та її відмінність від промислового шпіонажу, проаналізувати джерельну базу дослідження цієї проблеми, здійснити ретроспективний аналіз конкурентної розвідки й шпіонажу на підприємствах, їх дії в політичній сфері; запропонувати способи протидії розвідці та шпіонажу.

**Аналіз досліджень цієї проблеми.** Проблемі конкурентної розвідки та шпіонажу на підприємствах велику увагу приділяли як вітчизняні, так і зарубіжні фахівці. Д. Зеркалов у книзі «Безопасность бизнеса. Разведка» [7] описав міжнародний і вітчизняний досвід забезпечення безпеки на підприємстві, методи та способи ведення розвідки й контррозвідки, засоби здобуття конфіденційної інформації. У працях О. Деревицького [4], Є. Ющука [26] подано методи використання конкурентної розвідки, збору інформації, просування продукту та спостереження за становищем конкурента.

Т. Ткачук [22] розкрив низку питань з організаційно-правового й методичного забезпечення безпеки бізнесу, інформаційної безпеки держави та суб'єктів господарювання, розробив механізми захисту таємної інформації, оптимальні напрями взаємодії державного й недержавного сектору безпеки в Україні. У дослідженні кандидата економічних наук Ю. Якубівської розглянуто особливості цільових атак та показники їхньої результативності в мережі Інтернет.

О. Миронова визначає позитивні й негативні аспекти використання інформаційних ресурсів сучасними підприємствами, аналізує основні типи інформаційних конфліктів у кіберпросторі та пропонує способи захисту інформаційних систем підприємств [15]. Заслуговує на увагу праця В. Богдановича й В. Бадрака [2], у якій висвітлено історичне виникнення конкурентної розвідки та шпигунства, основні принципи та методи їх здійснення.

А. Гілад акцентував, що той, хто не усвідомлює ролі конкурентної розвідки як інструменту управління підприємством, не може бути конкурентоспроможним на ринку [30, с. 6].

**Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.** Поняття «конкурентної розвідки» (competitive intelligence) професійно закріпилося на Заході з його більш розвиненими ринками. У вітчизняному бізнесовому середовищі більш уживаними є терміни «ділова розвідка», «бізнес-розвідка». Конкурентна розвідка – постійний процес збору, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії задля своєї переваги на ринку. Конкурентна розвідка здійснює збір інформації лише законними методами. Тобто цьому процесу невластива крадіжка чужих секретів, використання інших «нечистих» способів отримання необхідної комерційної таємниці. Також для неї характерна робота з різноманітними джерелами та носіями інформації відкритого типу [31, с. 319].

Існує два основні завдання конкурентної розвідки: перше – забезпечення об'єктивною інформацією про реальне становище підприємства; друге – надання інформації про загрози та можливості в бізнесовому просторі [26].

Мета розвідки – отримання інформації, яка для підприємця є основою для прийняття виважених управлінських рішень.

В. Богданович розділяє методи конкурентної розвідки на

«кабінетний» (не виходячи з офісу) і «польовий» (із виходом на конкурентну територію) [2, с. 19].

*«Кабінетний» метод збору інформації.* Аналітики використовують відомості з офіційних джерел (державної статистики, аналітичних звітів, у ЗМІ, коментарів і прогнозів фахівців, річних звітів конкурентів, їхніх офіційних сайтів та ін.).

До *«польового» методу* відносять замовлення товару конкурента, маскування під клієнта, маскування під людину, яка прийшла на співбесіду або хоче влаштуватися на роботу.

На противагу конкурентній розвідці, під промисловим шпіонажем слід розуміти вид недобросовісної конкуренції, діяльність із незаконного здобуття та вивідування відомостей, що представляють промислові та ділові секрети конкурентів, їхню комерційну таємницю, із закритих від широкого доступу (та сторонніх осіб) джерел в інтересах досягнення економічних переваг [16, с. 145]. Промисловий шпіонаж ведеться всіма доступними засобами (коли мета виправдовує засоби), уключаючи застосування спеціальних технічних пристроїв та підкуп посадових осіб.

Промисловий шпіонаж дає змогу недобросовісним керівникам отримувати інформацію, що коштує мільйони доларів, за безцінок. Замість того, щоб збирати дані про ринок, удосконалювати виробничий процес та систематизувати відомості про контракти, вони вважають і вигідним, і відносно безпечним обкрадати своїх конкурентів. Таким чином, практикуючі промисловий шпіонаж підприємці не тільки отримують інформацію за номінальною вартістю, але й разом із нею одержують безцінні дані про стратегію конкурента [32].

Промислове шпигунство, зазвичай, має дві мети:

- отримання конфіденційної інформації конкурентів;
- здобуття конкурентної переваги на ринку через витіснення або знищення конкурента [23, с. 73].

Щодо методів шпигунства на підприємстві, то В. Ю. Богданович об’єднує їх у дві групи – агентурний метод одержання інформації й технічні методи промислового шпигунства [2, с. 19].

*Агентурний метод* одержання інформації здійснюється через вербування або впровадження своєї людини.

*Технічні методи промислового шпигунства* застосовують

техніку, виробництво й збут якої врегульовані законодавчо. Для цього використовують мікрофони, електронні стетоскопи, радіомікрофони, апарати магнітного запису, а також підключення до телефонних ліній.

Але, на жаль, на сучасному етапі розвитку ринкових відносин, конкурентна розвідка та промисловий шпіонаж існують переважно в неподільному вигляді, із поєднанням відкритих і прихованих методів збору інформації.

Ще з давніх часів та аж до сьогодні конкурентна розвідка й промисловий шпіонаж залишаються основними ситуаціями, які можуть порушувати економічну і інформаційну безпеку сучасних підприємств і викликати конфлікти [15, с. 54].

Зародки сучасної конкурентної розвідки та промислового шпіонажу виникли ще задовго до появи самих цих понять. Одним із найпоширеніших методів, що застосовували розвідники, було маскування під мирних жителів. Найчастіше для прикриття використовували рід занять (торговець, священик, монах, іноді – жебрак тощо) [6, с. 14].

Початковим етапом конкурентної розвідки, що розвивалася разом із ремеслом і торгівлею, було приватне шпигунство. Ще купці Стародавнього Єгипту та Греції збирали важливу для їхнього успіху конфіденційну інформацію. Вони шукали дані про товар конкурента, його якість, кількість і ціну. Удавалися також до таких методів, як псування товару, пускання пліток про неохайність, несумісність ціни з його якістю тощо.

У XIV ст. створено першу приватну розвідслужбу, засновниками якої стали флорентійські купці-банкіри. Пізніше з'явилася служба, створена одними з найбільших промисловців XV і XVI ст. – Фуггерами з Аусбурга [2].

Варто також відзначити розвідслужбу, створену наприкінці XVIII ст. п'ятьма братами Ротшильдами. Їхні банки були в Лондоні, Відні, Парижі, Неаполі та Франкфурті.

У XX ст. конкурентна розвідка й шпіонаж відзначилися численними випадками порушення авторського та патентного права. Найгучніші скандали відбулися з такими великими компаніями:

1. *«Unilever» і «Procter & Gamble».* Компанія «Procter & Gamble» зізналася в тому, що протягом шести місяців здійснювала

промислове шпигунство, а саме оглядала сміття компанії-конкурента «Unilever». Розвідка стосувалася засобів із догляду за волоссям. Зрештою «Procter & Gamble» заборонили використовувати отриману конфіденційну інформацію компанії «Unilever» у виробництві своєї продукції [28].

2. *«Opel» та «Volkswagen».* «Opel» звинуватила «Volkswagen» у відсутності конфіденційних документів компанії після того, як керівник і сім заступників «Volkswagen» перейшли в компанію «Opel». Судова справа, що тривала чотири роки, завершилася зобов'язанням «Volkswagen» сплатити 100 млн дол. США, а також зробити замовлення запчастин для автомобілів на понад 1 млрд дол. США [28].

3. *«DuPont» і Майкл Мітчелл («Kolon Industries»).* Майкла Мітчелла було звинувачено в передачі конфіденційної інформації компанії «DuPont Kevlar», де його звільнено, на своє нове місце працевлаштування. Корейська компанія з виготовлення волокон «Kolon Industries Inc» отримувала інформацію про свого конкурента, яку Мітчеллу передавали колеги з «DuPont». У результаті Мітчелл поніс покарання у вигляді 18 місяців тюремного ув'язнення й виплати грошової компенсації понад 180 тис. дол. США [28].

4. *«Kodak» та Гарольд Уорден.* Після завершення контракту на 30 років з «Eastman Kodak» Г. Уорден створив консалтингову компанію, інформаційна діяльність якої ґрунтувалася на конфіденційній документації, отриманій нелегальним способом у «Kodak». Кримінальним законнодавством його засуджено до одного року ув'язнення й штрафу в 30 тис. дол. США. Однак, за підсумками аналітиків, оцінна вартість викраденої інформації «Kodak» становить мільйони доларів [28].

5. *«Starwood» та «Hilton».* Компанія «Hilton» була звинувачена в промисловому шпигунстві щодо компанії «Starwood». Як повідомлялося, вона викрала ідею люксового бренду під час перевезення конфіденційної інформації. Компанія «Hilton» сплатила певну суму «Starwood» і була зобов'язана утримуватися від розробки конкуруючих брендів розкішних готелів протягом трьох років від дати інциденту [28].

6. *«Google» та операція «Aurora».* Компанія «Google» оголосила, що оператори з території Китаю здійснили крадіжку

інтелектуальної власності, зокрема облікових записів електронної пошти від захисників прав людини. Керівники «Google» зазначили, що цей злочин був частиною більш широкої кібератаки від компанії в Китаї, яка стала відома як операція «Aurora». Зловмисники розпочали кібернапад, використовуючи незахищеність браузера Microsoft Internet Explorer, запустивши нову модифікацію трояна «Hydraq». Деякі коментатори стверджували, що кібернапад був частиною узгодженого китайського промислового шпигунства, спрямованого на отримання високотехнологічної інформації для стимулювання економіки Китаю. Через місяць компанія «Google» вирішила припинити діяльність стосовно високотехнологічного сектору в Китаї, що призвело до закриття операції «Aurora» [28].

Отже, у країнах із ринковою економікою завжди існували шпіонаж і конкурентна розвідка, мета яких – вивчення секретів, що лежать в основі досягнень та успіхів чужих підприємств і країн. Від них потерпають усі сфери економіки й не захищені навіть стратегічні компанії, що мають подвійний, воєнно-цивільний характер.

Активною конкурентна розвідка та шпіонаж існують і в політичній сфері. Сьогодні різні кризи, які накладаються одна на одну, змушують політиків усе частіше звертатися до закулісних можливостей отримання інформації, ідей чи навіть прямого саботування дій інших країн.

Політичні конфлікти, будь-яка нестабільність створюють ідеальні умови для роботи оперативних співробітників й аналітиків спецслужб, а також потребу в результатах їхньої діяльності. У зв'язку з цим актуальним стає такий вид політичного шпигунства, як кібершпіонаж.

Серед кібершпіонажу провідне місце посідає ВікіЛікс (wiki і leak – «витік») – міжнародний соціальний мережевий проект, створений у 2007 р. Засновником ВікіЛіксу є австралієць Д. Ассанж. Він створив унікальний кріптосервер – віртуальну «поштову скриньку». Будь-хто може покласти в неї документи й ніхто – навіть сам Ассанж – не дізнається, хто це зробив.

Мета ВікіЛіксу – «невідслідкована публікація та аналіз документів, що стали доступними внаслідок витоку інформації». Завдання ВікіЛіксу – це доведення важливих новин та інформації до громадськості [18].

Гучний скандал навколо ВікіЛіксу вибухнув після публікації на сайті документів дипломатичної служби США в кінці листопада 2010 р. Було опубліковано копії телеграм, які надходили в держдепартамент з американських посольств по всьому світу. Депеші містили відверті, часто неприємні відгуки про закордонних лідерів та оцінки проведеної ними політики.

ВікіЛікс опубліковувала компрометуючі документи на правлячі еліти різних країн. Найбільш гостра реакція була від населення, переважно молоді, країн північної Африки. Народні невдоволення спалахнули в Тунісі після того, як ВікіЛікс розкрив небачені масштаби корупції правлячого режиму. Сотні тисяч безробітних молодих людей піднялися проти соціальної несправедливості. Ланцюгова реакція аналогічних подій знайшла відгуки в Марокко, Єгипті, Сирії, Ємені, Бахрейні й інших країнах регіону. У Лівії соціальне протистояння переросло в громадянську війну із залученням збройних сил НАТО.

Глобальність впливу ВікіЛіксу випливає з двох фактів. По-перше, це стосується практично ключових гравців у форматі state nation. Публікації Wikileaks торкнулися не тільки США й Китаю, а й більшості провідних суверенних держав. По-друге, до аналізу широкого інформаційного масиву, виставленого Wikilleaks у мережу, підключилися журналісти й блогери майже всіх країн світу.

На думку, В.Соловйова, феномен ВікіЛіксу руйнує старий світовий порядок. «Total transparency» («тотальна прозорість»), запропонована ВікіЛіксом, – це і технології трансформації світового порядку. Світові політичні еліти вбачають у ВікіЛіксі небезпеку, а в їхніх діях щодо інтелектуальних послуг проглядається позиція, яка полягає в тому, щоб адаптуватися до нового світового порядку, у якому «злив» компромату стане нормою: або через залякування й загрозу кримінального переслідування, або через комплементарні оцінки його дій.

Серед експертів не викликає сумніву той факт, що в недалекому майбутньому кількість таких структур, як ВікіЛікс, зросте. Їх присутність в Інтернеті забезпечить розгортання й постійне розширення зони «total transparency» («тотальна прозорість»), у якій гарантуватиметься, що розміщена там інформація буде завжди доступа в мережі.

Отже, потенціал шпигунства у політичній сфері, як засвідчує приклад ВікіЛіксу, є настільки високим, що може викликати кризу влади одночасно на територіях декількох держав (Єгипет, Сирія, Туніс та ін.). Тобто регіональні масштаби здатні перерости в глобальні.

Усі наведені вище приклади свідчать про те, що конкурентна розвідка та шпіонаж є реальною загрозою, котра може вплинути на будь-який тип бізнесу – від невеликих до передових компаній у міжнародному списку Fortune. Сьогодні у сфері бізнесу інформація вважається більш цінним об'єктом, ніж будь-коли.

На сьогодні підприємства, установи та організації, які хочуть ефективно працювати в умовах інформаційної економіки, потребують розроблення заходів щодо підвищення безпеки їхніх інформаційних систем і ресурсів.

На мікрорівні керівництва компаній повинні зосереджувати свою увагу не лише на реактивних методах забезпечення економічної безпеки, а й формувати систему превентивних заходів, щоб уникнути випадків виникнення факту промислового шпигунства:

– здійснювати постійний моніторинг потенційних загроз у вигляді шкідливого програмного забезпечення;

– здійснювати періодичну та неперіодичну атестацію персоналу для визначення рівня його надійності;

– обов'язково підписувати договори про нерозголошення комерційної таємниці між керівниками підприємств і працівниками, чия професійна діяльність пов'язана з такою інформацією.

На макрорівні необхідними умовами формування системи захисту від промислового шпигунства є:

– створення ефективного механізму державного регулювання експорту-імпорту товарів, які містять отриману незаконним способом інтелектуальну власність;

– податкове регулювання процесу переміщення через кордон продукції, що порушує права інтелектуальної власності;

– гармонізація законодавства, що стосується захисту від недобросовісної конкуренції , охорони та захисту комерційної таємниці;

– стимулювання розвідувальної й контррозвідувальної діяльності в контексті боротьби з промисловим шпигунством як на

національному, так і на міжнародному рівні, контроль за дотриманням чинного законодавства [27, с. 371].

Для запобігання розголошенню комерційної таємниці організаційні й адміністративні засоби захисту потрібно підсилювати соціально-психологічними. Правильний підбір і розстановка кадрів дають змогу підприємствам зменшити ризики розголошення комерційної таємниці та гідно протистояти промисловому шпигунству.

**Висновки й перспективи подальших досліджень.** Учені розуміють конкурентну розвідку як нову сферу досліджень, інструмент управління в бізнесі, у ширшому сенсі цього слова – інструмент у сфері безпеки. Промислове шпигунство потрібно відрізняти від конкурентної розвідки, оскільки в них різні методи й способи отримання інформації. Посилення конкурентної розвідки в політичній сфері являє собою певну загрозу для традиційної державної влади, тому завдання вчених сьогодні полягає в збереженні загальнонаціональної стабільності й державної безпеки. Світовий досвід підтверджує неминуче виникнення загроз економічній безпеці країни в контексті поширення процесу промислового шпигунства. На сьогодні гостро стоїть завдання розробки єдиних механізмів захисту від інсайдерських загроз. У подальшому слід розробити методики оцінювання економічної ефективності впровадження систем захисту комерційної інформації та промислового шпіонажу.

**Список використаних джерел**

1. Богданович В. Ю. Конкурентна розвідка та промислове шпигунство / В. Ю. Богданович, В. В. Бадрак // Сучасний захист інформації. ? 2014. ? ? 1. – С. 16–22.

2. Єгоров В. З історії розвитку промислового шпигунства / В. Єгоров // Дзеркало тижня. – 1994. ? ? 13. – С. 14–17.

3. Зеркалов Д. В. Безопасность бизнеса. Разведка : науч. пособие / Д. В. Зеркалов. – Киев : Наук. свит, 2008. – 108 с.

4. Миронова О. М. Економічна безпека інформаційних ресурсів підприємства [Електронний ресурс] / О. М. Миронова // Управління розвитком. ? 2010. ? ? 18. ? С. 51–54. ? Режим доступу : http://www.nbuv.gov.ua/old_jrn/ Soc_Gum/Uproz/2010_18/u1018mir.pdf (05.02.2017)

5. Остапенко Г. Г. Корпоративна розвідка як механізм забезпечення

економічної безпеки підприємства [Електронний ресурс] / Г. Г. Остапенко // Вчені записки. ? С. 144–147. ? Режим доступу : http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Vzuk/2008_18/tom_4/144_147.pdf (05.02.2017)

6. Поправко О. Феномен под названием WIKILEAKS [Електронний ресурс] / О. Поправко // Нова стратегічна концепція Північноатлантичного альянсу: перспективи для держав Центральної та Східної Європи : матеріали та виступи осінньої академії (м. Донецьк, 30 лист. – 2 груд. 2010 р.). ? Режим доступу : http://www.intsecurity.org/stat/zmist5_2.php (05.02.2017)

7. Ткачук Т. Ю. Конкурентна розвідка : навч. посіб. / Т. Ю. Ткачук. ? Київ : НАСБ України, 2010. – 219 с.

8. Ткачук Т. Ю. Характерні особливості конкурентної розвідки та промислового шпигунства / Т. Ю. Ткачук // Персонал. ? 2007. ? ? 2. – С. 72–78.

9. Ющук Е. Л. Конкурентная разведка: маркетинг рисков и возможностей : учеб. пособие / Е. Л. Ющук. ? Москва : Вершина, 2006. – 240 с.

10. Якубівська Ю. Є. Цільові атаки в контексті промислового шпигунства [Електронний ресурс] / Ю. Є. Якубівська // Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект : сб. науч. тр. ? Донецк : ДонНУ, 2014. ? Т. 2. – С. 368–372. ? Режим доступу : http://dspace.tneu.edu.ua/bitstream/316497/1537/1/10_%D1%84%D0%B0%D1%85.pdf (05.02.2017)

11. Якубівська Ю. Є. Тенденції розвитку промислового шпигунства у світі [Електронний ресурс] / Ю. Є. Якубівська // Ефективна економіка. ? Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=5383 (05.02.2017)

12. Gilad B. Cl Certification: Do We Need It? / B. Gilad, J. Herring // Competitive Intelligence Magazine. ? Cambridge : Fuld-Gilad-Herring Academy of Competitive Intelligence, 2011. ? Vol. 6. ? ? 4.

13. Secker R. 10 key sources of competitive data / R. Secker. – SCIP online.

14. Weiss A. Competitive strategies – the dog fight! / A. Weiss. – SCIP online.

**Мищук Татьяна, Мытко Антонина. Особенности конкурентной разведки и шпионажа на предприятиях.** В статье исследованы процессы промышленного шпионажа и конкурентной разведки как скрытых форм получения конфиденциальной инфор¬мации конкурентов. Цель статьи - проанализировать особенности конкурентной разведки и шпионажа на

предприятиях. С этой целью охарактеризован понятийный аппарат конку¬рентнои разведки и промышленного шпионажа и их различия, рассмотрены тенденции развития промышленного шпионажа на мировом уровне на примерах крупнейших мировых компаний. С помощью историко-поривня¬льного метода осуществлен ретроспективный анализ конкурентной разведки и шпионажа на предприятиях. Раскрыто проявления шпионажа в политической сфере, в частности на примере международного социального сетевого проекта «Викиликс», а также проанализированы последствия политической разведки. На основе полученных результатов предложены способы противодействия шпионажу и разведке на микро- и макроуровне.

Доказано, что в странах с рыночной экономикой всегда существовали шпионаж и конкурентная разведка, цель которых - изучение секретов, лежащие в основе достижений и успехов чужих предприятий и стран. От них страдают все сферы экономики и не защищены даже стратегические компании, имеющие двойной, военно-гражданский характер. Активной конкурентная разведка и шпионаж существуют и в политической сфере. Сегодня различные кризисы, которые накладываются друг на друга, заставляют политиков все чаще обращаться к закулисным возможностей получения информации, идей или даже прямого саботажа действий других стран.

Мировой опыт подтверждает неизбежно возникновение угроз экономической безопасности страны в контексте распространения процесса промышленного шпионажа. На сегодня остро стоит задача разработки единых механизмов защиты от инсайдерских угроз. Авторы считают, что в дальнейшем следует разработать методики оценки экономической эффективности внедрения систем защиты коммерческой информации и промышленного шпионажа.

**Ключевые слова:** конкурентная разведка, промышленный шпионаж, информационная безопасность, целевые атаки, кибершпионаж, инсайдерская угроза.

**Mishchuk Tetyana, Mytko Antonina. Characteristics of Competitive Intelligence and Espionage in Enterprises.** The article investigates the processes of industrial espionage and competitive intelligence as hidden forms of obtaining confidential information of competitors. The purpose of the article is to analyze the features of competitive intelligence and espionage at the enterprises. To this end, the conceptual apparatus of competitive intelligence and industrial espionage and their differences are described, the trends of industrial espionage development at the world level are considered at the examples of the world's

largest companies. Using a historical-comparative method, a retrospective analysis of competitive intelligence and espionage at the enterprises was carried out. The manifestations of espionage in the political sphere, in particular, on the example of the international social networking project "WikiLeaks", were analyzed and the consequences of political intelligence have been analyzed. Based on the obtained results, methods have been proposed for dealing with espionage and intelligence at micro and macro levels.

It has been proved that in countries with a market economy there has always been espionage and competitive intelligence, the purpose of which is to study the secrets that underlie the achievements and successes of other companies and countries. All sectors of the economy suffer from them, and even strategic companies with a double, military-civilian character are not protected. Active competitive intelligence and espionage exist in the political sphere. Today, the various overlapping crises make politicians ever more likely to turn to behind-the-scenes opportunities to get information, ideas, or even direct sabotage of other countries.

World experience confirms the inevitable emergence of threats to the country's economic security in the context of the spread of the process of industrial espionage. Today, the task of developing common mechanisms for protection against insider threats is acute. The authors believe that in the future it is necessary to develop methods for assessing the economic efficiency of introducing systems for the protection of commercial information and industrial espionage.

**Keywords:** competitive intelligence, industrial espionage, information security, targeted attacks, cyber spyware, insider threat.

Стаття надійшла до редколегії
06.08.2017 р.