

том продукції машинобудування збільшувався та становив за даними 2011 р. 1,89 (табл. 7).

Таблиця 7

**Співвідношення експорту та імпорту продукції машинобудування в Україні у 2009-2011 рр., тис. дол. США**

Рік	Експорт	Імпорт	Співвідношення імпорт/експорт
2009 р.	5014319,1	6257044,8	1,25
2010 р.	5670416,3	8166974,9	1,44
2011 р.	6758995,2	12795104,9	1,89

Більш високі темпи росту імпорту продукції машинобудування порівняно з обсягами її експорту, а також збільшення коефіцієнту співвідношення імпорту та експорту продукції машинобудування свідчить про низький рівень конкурентоспроможності продукції вітчизняних підприємств та слабкість конкурентних позицій господарюючих суб'єктів як на зовнішньому так і на внутрішньому ринках.

**Висновок.** Таким чином, у статті було розглянуто основні фактори впливу на конкурентний потенціал. Виявлено, що макроекономічні чинники безпосередньо впливають на той чи інший локальний потенціал, який є складовою конкурентного потенціалу. Дослідження було проведено на підприємствах машинобудування. У подальшому пропонується вимірювати вплив цих факторів на конкурентний потенціал.

**БІБЛІОГРАФІЧНИЙ СПИСОК:**

1. Мескон М. Х. Основы менеджмента / Мескон М. Х., Альберт М., Хедоури Ф. ; пер с англ. – М. : Дело, 2000. – 704 с.
2. Портер М. Международная конкуренция. Конкурентные преимущества стран / Портер М. – М. Международные отношения, 1993. – 956 с.
3. Боумен К. Основы стратегического менеджмента / Боумен К. – М. : Банки и биржи, ЮНИТИ, 1997. – 175 с.
4. Даниелс Джон Д. Международный бизнес: внешняя среда и деловые операции / Даниелс Джон Д., Радеба Ли Х. – М.: Дело, 1998. – 456 с. 5. Томпсон А. А. Стратегический менеджмент. Искусство разработки и реализации стратегии / Томпсон А. А., Стрикленд А. Дж. – М. : Банки и биржи. – ЮНИТИ, 1998. – 576 с.
5. Іванова Ю. Б. Конкурентні перги підприємства: оцінка, формування та розвиток : монографія / Іванова Ю. Б., Орлов П. А., Іванова О. Ю. – Х. : ВД ІНЖЕК, 2008. – 352 с.
6. Фатхутдинов Р. А. Стратегический маркетинг / Фатхутдинов Р. А. – СПб. : Питер, 2007. – 352 с.
7. Оценка влияния факторов внешней среды на экспортную стратегию предприятия [Электронный ресурс] / Ю. Е. Кислова // Менеджмент в России и за рубежом. – 2002. – № 1. – Режим доступа : <http://www.cfin.ru/press/management/2002-1/04.shtml>.
8. Державна служба статистики України [Електронний ресурс]. – Режим доступу : <http://www.ukrstat.gov.ua/>.
9. Оценка бизнес-регулирующего: (легкость ведения бизнеса в Украине) [Электронный ресурс]. – Режим доступа : <http://russian.doingbusiness.org/data/exploreeconomies/ukraine>.
10. Концепція Державної цільової науково-технічної програми розвитку прогресивних технологій, нових матеріалів та технологічного обладнання для машинобудування на 2011-2015 року (Проект) : [Електронний ресурс]. – Режим доступу : [http://industry.kmu.gov.ua/control/uk/publish/article.jsessionid=1B4B3DCFF09173FF119DFFEF07E375E?art\\_id=83310&cat\\_id=42148](http://industry.kmu.gov.ua/control/uk/publish/article.jsessionid=1B4B3DCFF09173FF119DFFEF07E375E?art_id=83310&cat_id=42148).
11. Маслак О. І. Про основні проблеми та заходи щодо активізації інноваційної діяльності підприємств / О. І. Маслак, В. В. Костін. Журнал «Регіональні перспективи». № 5(24). – 2002. – м. Кременчук.
12. Лощина Л. В. Комплексна оцінка інноваційної діяльності підприємства в контексті антикризового управління/ Л. В. Лощина // Проблеми і перспективи розвитку банківської системи України : зб. тез доповідей XIII Всеукраїнської науково-практичної конференції, 28-29 жовтня 2010 р. – Суми : ДВНЗ «УАБС НБУ», 2010. – Т. 2. – 233 с.
13. Александров И. В. Стратегия инновационного развития машиностроительного комплекса на основе формирования интеллектуального потенциала (на примере ЗАО «НКМЗ») / И. В. Александров // Экономика промышленности. – 2006. – № 5. – С. 62–70.

УДК 65.012.8 (045)

**Скібіцька Л.І.**  
старший викладач кафедри менеджменту  
зовнішньоекономічної діяльності підприємств,  
Національний авіаційний університет

**ЕКОНОМІЧНА РОЗВІДКА  
В АНТИКРИЗОВОМУ УПРАВЛІННІ ПІДПРИЄМСТВОМ  
ECONOMIC INTELLIGENCE IN CRISIS MANAGEMENT NOW**

**АНОТАЦІЯ**

Стаття присвячена питанням організації системи економічної розвідки, як засобу отримання комерційної інформації та забезпеченню захисту власної економічної інформації підприємства.

**Ключові слова:** економічна безпека, інформаційна безпека, розвідка, конкурентна розвідка, контррозвідка, макроекономічна розвідка, мікроекономічна розвідка, економічна контррозвідка, промислове шпигунство, бенчмаркінг, комерційна таємниця, конкуренція, конкурентоздатність.

**АННОТАЦИЯ**

Статья посвящена вопросам организации системы экономической разведки, как средства получения коммерческой информации и обеспечению защиты собственной экономической информации предприятия.

**Ключевые слова:** экономическая безопасность, информационная безопасность, разведка, конкурентная разведка, контрразведка, макроекономическая разведка, микроэкономическая разведка, экономическая контрразведка, промышленный шпионаж, бенчмаркинг, конкуренция, конкурентоспособность.

**ANNOTATION**

The article is devoted to the questions of system economic secret service creation, as facilities of receipt of commercial information and to providing of defence of own economic information of enterprise.

**Key words:** economic security, informative safety, secret service, competition secret service, counter-intelligence, macroeconomic secret service, mikroekonomicheskaya secret service, economic counter-intelligence, industrial espionage, benchmarking, competition, competitiveness.

**Постановка проблеми.** Конкурентоспроможність підприємства все більше визначаються його здатністю швидко відтворювати, нарощувати й поновлювати інформацію щодо потенціалу й намірів конкурентів та секретити свою внутрішню інформацію у вигляді комерційної таємниці, щоб забезпечити принаймні тимчасове монополієне становище на ринку. Разом із тим, питання організації систем економічної розвідки, використання автоматизованих систем для аналізу її да-

них та організації контр-розвідувальних заходів для попередження криз та/або пом'якшення їх проявів у вітчизняному бізнесі ще не набули належної уваги, що й обумовлює певну новизну дослідження.

Для підтримання стійкої роботи підприємства більш важливим стала наявність своєчасної достовірної інформації не тільки про стан потенціалу свого підприємства, а й про постачальників, конкурентів, споживачів, про новітні технології та інші параметри зовнішнього середовища. В цих умовах важливим ресурсом, що забезпечує ефективну діяльність підприємства є інформація та комунікаційні зв'язки.

Втім, деякі аспекти діяльності систем конкурентної (економічної) розвідки наразі є іноді спірними й викликають визначені дорікання з боку громадськості. Зокрема, іноді неоднозначно оцінюється робота конкурентної розвідки з погляду її відповідності етичним і юридичним нормам. Сумніви саме такого роду, що залишилися не розв'язаними, стали каменем спотикання для ряду компаній, які так і не зважилися на створення подібних служб.

Зазначене визначає актуальність та певну наукову новизну дослідження проблеми.

**Аналіз останніх досліджень і публікацій.** Проблеми економічної безпеки підприємницьких структур в антикризовому менеджменті в свій час опрацьовували такі іноземні вчені, як: Р. Акофф, І. Ансофф, К. Боумен, Є. Брігхем, Р. Хіт, А. Штангрет; росіяни: Г. Л. Азов., А. П. Градов, А. П. Челенков та вітчизняні: А. М. Куценко, Л. О. Лігоненко, О. В. Мороз, З. Є. Шершньова тощо.

**Метою статті** є обґрунтування необхідності організації економічної розвідки у підприємстві; окреслення концепції системного підходу до забезпечення захисту комерційної таємниці й конфіденційної інформації та організації контррозвідки;

**Викладення основного матеріалу.** «Ми живемо вже не в століття інформації, – стверджує Л. Каханер, автор книги «Конкурентна розвідка». – Ми живемо в століття розвідки».

Отже, конкурентна розвідка (КР) є могутнім інструментом дослідження ринку, і в даний час являє собою дисципліну, що бурхливо розвивається, яка виникла на стику економіки, юриспруденції і спеціальних розвідувальних дисциплін. Відмінністю КР від промислового шпигунства є те, що вона здійснюється винятково в рамках існуючих державних законів, і свої результати одержує завдяки аналітичній обробці величезної кількості найрізноманітніших відкритих інформаційних матеріалів з різних джерел.

Раніше вже говорилося, що КР дає кращі результати, якщо вона організована у вигляді безперервного процесу.

*По-перше*, структура циклу розвідки вже припускає наявність процесу. При організації широкомасштабної системи розвідки у своїй компанії необхідно прагнути до розширення сфери діяльності за межі компанії і залученню до співробітництва як можна більшого числа людей.

*По-друге*, навіть якщо деякі дуже успішно працюючі компанії розглядають проведення КР як посадовий обов'язок особи з вищої адміністрації, система збору розвідувальної інформації іноді може розглядатися іншою частиною компанії як деякий вид «виконавчого шпигунського агентства». Забезпечуючи доступ до матеріалів КР тільки для менеджерів самого вищого рівня, можна іноді «втратити» співробітників, що хотіли б одержувати матеріали КР і плідно використовувати їх у своїй роботі. Більш того, не допускаючи деяких службовців компанії до матеріалів КР, можна відбити в них охоту представляти в систему КР зібрані ними самостійно інформацію.

Можна створити ефективну систему управління компанією, мати висококваліфікованих фахівців, володіти високим науково-технічним потенціалом, мати розгалужену збутову мережу, але все це виявиться не важливим, якщо керівник компанії не буде здатний виявляти зовнішні загрози й ризики, що здатні поставити компанію в складне становище [6]. Для виявлення ризиків і створюються підрозділи КР. У багатьох великих компаніях такі підрозділи розміщуються в службі стратегічного планування, що підпорядковується безпосередньо керівництву. Діяльність підрозділу КР стає найбільш ефективною, якщо її головне завдання полягає в інформаційній підтримці стратегічного планування компанії. В інших компаніях підрозділи КР можуть входити до складу кожного самостійного відділу, що знаходиться в підпорядкуванні першого віце-президента, або безпосередньо Президента компанії, який координує їхню діяльність.

Доцільно не розміщувати КР у службі маркетингу, відділі продажів, науково-дослідному відділі й інших самостійних структурних підрозділах компанії, не зв'язаних між собою. У таких випадках досить складно здійснювати взаємодію й координацію роботи КР.

Зрештою, не так важливо, де розміщується підрозділ КР. Важливо, як організована координація її роботи і як циркулюють інформаційні потоки усередині компанії. В одних компаніях інформація циркулює по замкнутому контуру й у готовому вигляді надається на нижній рівень, тобто доводиться до кожного співробітника (якому вона необхідна для виконання виробничих обов'язків), в інших – навпаки, інформація збирається на нижньому рівні, передається «наверх» (незамкнутий контур) і рідко доходить до кожного співробітника компанії. З досліджень по розробці концепції організації роботи КР, проведених фірмою *Learning Corporation*, випливає, що така організація (друга модель) доведення розвідувальних зведень до співробітників не йде на користь компанії [7].

Для максимальної ефективності роботи підрозділ КР повинен мати досить високий статус у компанії, щоб співробітники ставилися до нього із повагою й бачили в ньому свого захисника і борця за інтереси компанії. Однак цей підрозділ повинен бути доступним кожному працюючому в компанії в межах його компетенції, а не виконувати завдання в інтересах якого-небудь одного відділу.

Аналітична інформація, підготовлена підрозділом КР, повинна бути закритою для всіх сторонніх, але доступною для кожного співробітника компанії (у частині, його що стосується).

Хоча основне призначення КР – підтримка прийняття управлінських рішень, сформована певним чином система КР може допомогти компанії вирішувати й багато інших задач, а саме:

1. *Передбачення змін на ринку.* Компанії, що фокусують зусилля своєї КР на відстеженні змін на ринку, рідко потрапляють знеацька у скруту через події, що впливають на їхній бізнес. Навпаки, компанії, у яких така увага відсутня, можуть незабаром стати банкрутами.
2. *Передбачення дій конкурентів.*
3. *Виявлення нових або потенційних конкурентів.*
4. *Вивчення успіхів і невдач конкурентів*
5. *Пошук і вивчення фірм, передбачуваних до покупки (злиття).*
6. *Вивчення нових технологій, продукції і процесів.*
7. *Моніторинг змін у політичній, законодавчій і регулюючій областях, що впливають на бізнес.*
8. *Відкриття нової справи.* Конкурентна розвідка може не тільки допомогти прийняти рішення про нову діяльність або диверсифікацію, але й дозволить одержати найважливішу вихідну інформацію для його розвитку.

9. *Відкритий погляд на свою діяльність.* Багато компаній, особливо великі, мислять обмежено, не виходячи за межі власних рамок. Їхні методи роботи стають традиційними і застарілими; КР надає нові ідеї і концепції. Вона змушує сфокусувати погляд на зовнішньому світі й визначити місце своєї компанії в конкурентному середовищі.

10. *Допомога в застосуванні новітніх інструментів управління.* Деякі компанії відчувають утруднення при запровадженні в дію й підтримці таких дорогих управлінських технологій як «комплексне керування якістю», впровадження корпоративної АСУ, «перехід на нову технологію» або «система задоволення клієнта». Одна з причин — відсутність необхідної інформації.

Цілі й задачі КР багато в чому близькі цілям і завданням класичної розвідки, чий аналітичні матеріали використовуються при формуванні й здійсненні державної політики або плануванні воєнних операцій, тільки масштаби розв'язуваних задач зовсім інші. Основна область застосування КР — це ринок. Головною метою КР є систематичне відстеження відкритої інформації про конкурентів, аналіз отриманих даних і прийняття на їхній основі управлінських рішень. Створення КР конкурентної розвідки — це веління часу та єдиний спосіб вижити в гострій конкурентній боротьбі — таке думка багатьох керівників корпорацій у США. КР дозволяє передбачати зміни на ринках, проводити прогноз дій конкурентів, виявляти нових або потенційних конкурентів, проводити моніторинг появи нових «вибухових» технологій і політичних та фінансових ризиків.

Висновки з аналізу інформації КР можуть використовуватися як для прийняття тактичних рішень, так і для опрацювання стратегічних напрямків розвитку фірми або корпорації в цілому. КР широко використовує прийоми й методи стратегічного управління, що дозволяє одержувати комплексне уявлення про ситуації на ринку й уточнювати позиції, на які компанія може на ньому претендувати через співставлення свого конкурентного статусу з конкурентоспроможністю інших суб'єктів, що оперують на цьому ж ринку. Чимало конкурентна розвідка черпає й з арсеналу засобів маркетингу, чий аусилля спрямовані головним чином на виявлення й аналіз споживчого попиту в тому чи іншому сегменті ринку. Так що співробітники служби КР займаються, насамперед, збором зведень про конкурентне середовище й конкретних конкурентів (у тому числі й потенційних) та їхнім аналізом. Вони моделюють подальше поведіння суперників на ринку. КР, подібно могутньому радарові, уловлює нові віяння в бізнесі, відстежує можливості, що з'являються, й попереджає про небезпеки, що насуваються.

Втім, деякі аспекти діяльності КР іноді спірні й викликають певні дорікання з боку громадськості. Зокрема, іноді неоднозначно оцінюється робота КР з огляду її відповідності етичним і юридичним нормам. Сумніви саме такого роду, що залишилися не розв'язаними, стали каменем спотикання для ряду компаній, що так і не наважилися на створення подібних служб.

Тим часом, використовуючи різні, часом не надто коректні, методи збору інформації — від фронтального «прочісування» каналів Інтернету до копання в смітєвих кошиках своїх конкурентів, — аналітики служби накопичують дані практично зі всіх цікавих для керівництва компанії питань — від розробок суперниками нових видів продукції і рівня виробничих витрат на її виготовлення до особистісних характеристик і професійних якостей керівників та провідних фахівців компаній-конкурентів, а також мотивах прийняття ними тих або інших управлінських рішень. Адже часом навіть випадкова інформація може виявитися досить цінною [4].

При існуючій великій кількості інформації налагоджений потік її надходження являє собою аж ніяк не

саму головну підмогу у вирішенні завдань, що постають перед КР. Зрештою, з розширенням мережі Інтернет і появою комп'ютерних баз даних, інформація перетворилася в дешевий і цілком доступний покупцеві товар, і заради її одержання немає рації обтяжувати корпоративну структуру ще одним великим підрозділом. Завдання КР полягає головним чином у тому, щоб допомогти керівництву компанії витягти з цього рясного інформаційного потоку лише необхідні для прийняття рішень дані.

Концепція системного підходу до забезпечення захисту конфіденційної інформації одержала назву — «метод *OPSEC*» (*Operation Security*). Цей підхід був розроблений американськими фахівцями під час в'єтнамської війни для підвищення ефективності захисту конфіденційної інформації і зменшення вартості забезпечення її схоронності. За твердженням автора методу — відомого американського фахівця в області забезпечення безпеки А. Паттокоса, *OPSEC* є ефективним засобом приховання намірів, планів, заходів, технологій, що дозволяє постійно бути «на крок вперед супротивника». Застосування цього методу в цивільній сфері означає стійку підтримку конкурентоздатності виробленої продукції, фінансового стану підприємства. Суть методу полягає в тому, щоб припинити, запобігти або обмежити витік тієї частини інформації (найбільш конфіденційної), що може дати конкурентові можливість «довідатися» або «обчислити», що здійснює або планує Ваше підприємство, і у результаті випередити його на ринку [5].

Процес організації захисту інформації за методом *OPSEC* розбитий на сім етапів.

#### *Етап 1. Аналіз об'єкта захисту.*

На цьому етапі визначають те, що необхідно захистити. Аналіз проводиться по наступних напрямках:

- виявляється, яка інформація має потребу в захисті;

- виявляються найбільш важливі елементи (критично) інформації, що захищається;

- визначається термін життя критичної інформації (час, необхідний конкурентові для реалізації добутої інформації);

- визначаються ключові елементи інформації (індикатори), що відбивають характер охоронюваної інформації;

- класифікуються індикатори по функціональних зонах підприємства (виробничо-технологічні процеси, системи матеріально-технічного забезпечення виробництва, персонал фірми, фінанси, керування тощо).

#### *Етап 2. Виявлення загроз.*

На цьому етапі:

- визначається, кого може зацікавити інформація, що захищається;

- оцінюються методи, застосовувані конкурентами для одержання цієї інформації, а також ймовірні напрямки використання слабких місць в існуючій на підприємстві системі забезпечення безпеки в конкретному випадку;

- розробляється система заходів щодо припинення дій конкурента.

#### *Етап 3. Аналіз ефективності.*

На цьому етапі аналізується ефективність прийнятих і постійно діючих підсистем забезпечення безпеки (фізична безпека, безпека документації, надійність персоналу, безпека ліній зв'язку тощо). Потім моделюється планована операція і складається хронологічний опис подій (або їхніх функціональних зв'язків), безпека яких необхідно забезпечити. Для кожної події планованої операції визначаються індикатори, що можуть служити відправними даними для виявлення критичної інформації. Визначаються можливі специфічні джерела інформації, аналіз яких може привести до виявлення таких індикаторів (статті в пресі, прес-релізи,

телефонні розмови по незахищених каналах, недбале відношення до чернеток, передача зайвої інформації - у ході ведення переговорів, а також сталі стереотипи, шаблони в повсякденній роботі і процедурах тощо).

#### Етап 4. Визначення необхідних заходів безпеки.

У ході цього етапу на основі проведених на перших трьох етапах аналітичних досліджень визначаються необхідні додаткові заходи по забезпеченню безпеки. При цьому перелік додаткових захисних мір, що дозволяють «закрити» виявлені уразливі напрямки, супроводжується оцінкою витрат, зв'язаних із застосуванням кожної міри. Зіставлення очікуваного зниження уразливості й майбутніх витрат дозволяє оцінити економічну доцільність запропонованих мір.

#### Етап 5. Розгляд пропозицій щодо заходів безпеки і критерієві ефективність/вартість.

На цьому етапі керівниками фірми розглядаються представлені пропозиції по всіх необхідних заходах безпеки і розрахунок їхньої вартості й ефективності.

#### Етап 6. Реалізація заходів.

На цьому етапі реалізуються вжиті додаткові заходи безпеки з урахуванням установлених пріоритетів.

#### Етап 7. Контроль виконання заходів.

На заключному етапі проводиться контроль і доведення реалізованих мір безпеки. При цьому перевіряється ефективність ужитих заходів, виявляються залишені незахищеними або знову виникаючі уразливі місця. Реалізовані міри доводяться до оптимального рівня, вводиться постійний контроль за їхнім функціонуванням.

Контр-розвідувальний цикл складається з п'яти етапів:

1. Визначення вимог захисту.
2. Оцінка конкурентів.
3. Оцінка власної уразливості.
4. Розробка контрзаходів.
5. Реалізація контрзаходів.

На відміну від розвідки, об'єктом контр-розвідувальної діяльності є не зовнішнє, а внутрішнє середовище функціонування підприємства.

Це середовище містить у собі такі елементи:

- керівний склад підприємства (директор, його заступники, головбух тощо) як потенційні об'єкти розвідувальних заходів і/або злочинів з боку конкурентів;
- особи з допоміжного персоналу, що мають доступ до комерційної таємниці (друкарки, працівники канцелярії тощо);
- співробітники, з боку яких потенційно існує небезпека надання злочинним елементам таких зведень, що допоможуть їм зробити злочину (сторожачи, охоронці, водії персональних машин керівників тощо);
- співробітники самої служби безпеки;
- раніше засуджені особи з числа працівників підприємств;
- співробітники підприємства, родичі яких працюють у конкурентів;
- раніше звільнилися працівники;
- особи, що у силу своїх посадових обов'язків регулярно приймають відвідувачів підприємства.

Встановлення мети та об'єкту контр-розвідувальної діяльності дозволяє визначити коло можливих об'єктів підрозділу контррозвідки, а саме:

- боротьба з економічним шпигунством;
- припинення злочинів проти окремих співробітників (або всіх співробітників на їхніх робочих місцях);
- надання сприяння правоохоронним, судовим і контрольно-наглядовим органам у документуванні протиправних дій осіб, що роблять карні злочини й адміністративні провини.

Виконання вищевказаних задач можливо при реалізації наступної сукупності функцій контррозвідки:

- збір зведень і документів по цивільних і кримінальних справах;

- регулярне інформування керівництва підприємства про причини й умови, що сприяють здійсненню правопорушень з боку персоналу;

- документування дій осіб, затриманих за адміністративні провини;

- виявлення осіб з числа персоналу, що роблять сприяння злочинним елементам (не працюючим на підприємстві) у здійсненні ними злочинів;

- викриття економічних (промислових) шпигунів з числа персоналу;

- інформування керівників підприємства й охоронців (якщо вони мають) про плановані у відношенні них злочинах;

- пошук без звістки зниклих співробітників підприємства;

- створення умов, що виключають підслуховування розмов у службових кабінетах;

- встановлення обставин розголошення зведень, що складають комерційну таємницю;

- з'ясування біографічних і інших даних, що характеризують особистість, про співробітників підприємства (з їхньої письмової згоди) при висновку ними

- трудових контрактів;

- пошук утраченого співробітниками майна, що належить підприємству;

- консультування з питань забезпечення безпеки підприємства і його персоналу.

Щодо дотримання етики в конкурентній розвідці, то її доцільно розглядати акцентуючи увагу саме на вирішенні етичних проблем у бенчмаркінгу.

Роберт С. Кемп (*Robert C. Camp*) у своїй книзі «Бенчмаркінг — пошук найкращих промислових методів, що ведуть до вищої ефективності роботи» визначив процес бенчмаркінгу як «пошук кращих практик, що призводять до найкращого функціонування». Девід Т. Кернс (*David T. Kearns*), виконавчий директор компанії *Xerox Corporation*, визначає бенчмаркінг як «безперервний процес оцінки рівня продукції, послуг і методів роботи на основі порівняння з найсильнішими конкурентами, або тими компаніями, які визнані лідерами». Дев'яте видання Нового тлумачного словника для коледжів Вебстера (*Webster*) визначає бенчмаркінг як «точку відліку, щодо якої проводяться виміри» і як «щось, що служить стандартом (еталоном), за допомогою якого можна виміряти щось інше». Для наших цілей бенчмаркінг можна визначити як «систематизований спосіб виявлення, розуміння й розробки продуктів, послуг, дизайнів, устаткування, процесів і бізнес-практик найвищої якості для поліпшення реальної роботи організації».

Бенчмаркінг зв'язаний з низкою правових і етичних проблем. Узагалі всю конкурентну розвідку хвилюють етичні й правові колізії. Суспільство дотепер часто вважає КР непристойною справою, породженням «брудного шпигунського ремесла».

Отже, наведемо основні положення Кодексу поведіння в бенчмаркінгу.

#### 1. Принцип законності.

1.1. Якщо маютьс'я хоча б які-небудь сумніви щодо законності дії, не починайте цієї дії.

1.2. Уникайте обговорень або дій, що можуть вести до обмеження свободи торгівлі, до схем розміщення ринку і/або клієнтів, фіксуванню цін, висновковій угод, оформленню заявок або хабарам. Не обговорюйте проблеми витрат, якщо витрати є елементом визначення ціни.

1.3. Не вивідуйте торговельні секрети способами, що можуть бути розцінені як некоректні, включаючи порушення або спонукання до порушення зобов'язань по збереженню конфіденційності. Не розкривайте і не використовуйте ніяких торговельних секретів, що могли б бути отримані нелегальними способами або розкриті кимсь іншим у порушення зобов'язань по збереженню їхньої конфіденційності або по обмеженню їхнього використання.

1.4. Не поширюйте (ні як консультанта, ні як клієнта) висновки одного бенчмаркінгового дослідження на іншу компанію, не одержавши спочатку дозволу учасників першого дослідження.

#### 2. Принцип обміну.

2.1. Намагайтеся надати вашому партнерові по бенчмаркінгу інформацію такого ж виду і якості, яку запитуете від нього.

2.2. Установлюйте взаємини завчасно, щоб усвідомити чекання, усунути непорозуміння й установити взаємну зацікавленість у бенчмаркінгу.

2.3. Будьте чесного і відвертими до кінця.

#### 3. Принцип конфіденційності.

3.1. Розглядайте взаємний обмін у бенчмаркінгу як конфіденційний для залучених у нього осіб і компаній. Інформація не повинна поширюватися за межі організацій-партнерів без попередньої згоди партнера, що поділилася інформацією.

3.2. Участь якої-небудь компанії в дослідженні конфіденційно і не повинне повідомлятися без її дозволу.

#### 4. Принцип використання.

4.1. Використовуйте інформацію, отриману при бенчмаркінгу, тільки для цілей сформульованого поліпшення операцій або процесів у компаніях, що беруть участь у бенчмаркінговому дослідженні.

4.2. Використання або повідомлення імені партнера по бенчмаркінгу вимагають попереднього дозволу цього партнера.

4.3. Не використовуйте інформацію бенчмаркінгу або будь-яку інформацію, отриману в результаті бенчмаркінгового обміну, для торгівлі або реклами.

4.4. Інформація про можливі контакти, надана Міжнародною кліринговою палатою бенчмаркінгу, ні в якій формі і ніяким способом не може бути використана для маркетингу.

#### 5. Принцип контакту першої сторони.

5.1. При можливості встановлюйте контакти для бенчмаркінгу через своїх партнерів.

5.2. Поважайте корпоративну культуру партнерів і працюйте у відповідності з взаємно погодженими процедурами.

5.3. Діставайте взаємну згоду встановленого для бенчмаркінгу контакту на будь-яку передачу повідомлення або обов'язків іншим сторонам.

#### 6. Принцип контакту третьої сторони.

6.1. Одержите попередній дозвіл контактної особи, перш ніж повідомляти його ім'я у відповідь на контактний запит.

6.2. Уникайте повідомляти ім'я контактної особи на відкритих форумах без її попереднього дозволу (згоди).

#### 7. Принцип підготовки.

7.1. Продемонструйте розуміння корисності й ефективності бенчмаркінгу, заздалегідь підготувавши до першого контакту по бенчмаркінгу.

7.2. Рационально використовуйте час вашого партнера по бенчмаркінгу, ґрунтовно готуючись до кожного обміну.

7.3. Допомагайте вашим партнерам по бенчмаркінгу підготуватися, постачаючи їхніми запитальниками і повітками дня перед кожним візитом.

#### 8. Принцип завершення.

8.1. Виконуйте цілком і вчасно кожне зобов'язання, дане вашому партнерові по бенчмаркінгу.

8.2. Завершуйте кожне бенчмаркінгове дослідження як взаємно погоджене.

#### 9. Принцип розуміння дії.

9.1. Постарайтеся довідатися, якому стилю спілкування й співробітництва надає перевагу Ваш партнер по бенчмаркінгу.

9.2. Дотримуйте прийнятого стилю спілкування з вашим партнером по бенчмаркінгу.

9.3. Довідайтеся, як ваш партнер по бенчмаркінгу

хотів би, щоб ви обробляли і використовували його інформацію, і дійте саме в такий спосіб.

Комерційним структурам, наряду з організацією збору інформації з одного боку, необхідно забезпечити захист своєї інформації, тобто організацію системи доступу до зведень, що складають комерційну таємницю (КТ) підприємства (фірми) та системи їхньої безпеки.

Розглянемо найпоширеніші порушення захисту персональних даних.

Так, Державна служба України з питань захисту персональних даних за підсумком проведених нею перевірок, надала інформацію про основні положення законодавства щодо обробки та захисту персональних даних, яких зазвичай не дотримуються. Зокрема, серед них можна виділити такі:

- власник персональних даних зобов'язаний повідомляти вповноважений державний орган із питань захисту персональних даних про кожну зміну відомостей, необхідних для реєстрації відповідної бази, не пізніше ніж упродовж 10 робочих днів із дня настання такої зміни;

- на підприємстві (в установі, організації) обробку персональних даних можуть здійснювати лише ті особи, у яких посадовою інструкцією чи іншими внутрішніми документами визначений обов'язок здійснення обробки персональних даних;

- власник бази персональних даних повинен, перш ніж здійснювати обробку персональних даних, отримати згоду суб'єкта персональних даних на обробку цих даних;

- перед тим як отримувати в суб'єкта згоду на обробку персональних даних, власникові та/або розпорядникові персональних даних необхідно визначити, чи немає інших правових підстав для обробки персональних даних. Наприклад, обробка персональних даних працівників підприємства з метою забезпечення реалізації трудових відносин не вимагає згоди, проте якщо підприємством збираються персональні дані, не передбачені трудовим законодавством, необхідно отримати згоду працівників на обробку таких даних;

- забезпечення належного захисту приміщень, у яких знаходяться персональні дані, як в електронній формі, так і у формі картотек (наприклад, обладнання замками дверей у приміщеннях, шафах і сейфах) [2].

Наразі великий інтерес до методів інформаційної аналітичної розвідки проявляють, як державні, так і недержавні (комерційні) спецслужби. Це обумовлене тим, що в Інтернеті містяться великі обсяги інформації, яка може становити оперативний інтерес, як для перших, так і для других. Тому в багатьох країнах, зокрема в правоохоронних органах Росії (Управління «Р» МВС, Департамент інформаційної безпеки ФСБ), США (ФБР) і в Німеччині (ВКА), створені спеціальні підрозділи аналітичної розвідки в Інтернеті. Аналогічні підрозділи функціонують й у транснаціональних корпораціях, які все більше й більше перетворюються в «держави в державі».

Крім цього, існують самостійні дослідні центри, які спеціалізуються на «вивудженні» потрібних даних з «цифрового океану». Так, у Західній Європі й США збір інформації засобами Інтернету вже давно перетворився в досить прибутковий бізнес. За повідомленнями відкритої преси, тільки у Франції наразі працює більше десятка компаній, завданням яких є вивчення документів, у тому числі таблиць і малюнків, що існують в Інтернет-просторі. Як приклад, можна привести компанію лінгвістичної інженерії MAAG, яка орієнтована на інформаційно-аналітичне забезпечення таких ключових галузей французької економіки, як аерокосмічна промисловість, транспорт і енергетика. Для глобальних досліджень в Інтернеті використовуються спеціальні «процесори збору даних» (у деяких джерелах їх називають ще «текстово-аналітичні системи», хоча назва не зовсім вірна, оскільки аналізується не

тільки текст, але й малюнки, креслення, фотографії і графіки). У даному контексті термін «процесор» — це частина програми, яка визначає, яким чином сама програма управляє й маніпулює даними.

Процесор збору даних використовує програмне забезпечення, що одержало назву «робот», яке «витагує» потрібну інформацію, використовуючи цілий арсенал засобів і прийомів лінгвістичного, семантичного й статистичного аналізу. Діючи автономно, процесори збору даних перехоплюють будь-яку запитувану інформацію, як тільки вона з'явиться в Інтернеті.

#### Висновки.

1. В системі заходів безпеки істотне значення має оптимальний розподіл виробничих, комерційних і фінансово-кредитних зведень, що складають таємницю підприємства, між конкретними виконавцями відповідних робіт і документів.

2. При розподілі інформації, з одного боку, необхідно забезпечити надання конкретному співробітнику для якісного і своєчасного виконання доручених йому робіт повного обсягу даних, а з іншого боку, виключити можливість ознайомлення виконавця з зайвими, не потрібними йому для роботи класифікованими зведеннями.

3. Концепція системного підходу до забезпечення захисту конфіденційної інформації «OPSEC» є ефективним засобом приховання намірів, планів, заходів, технологій, що дозволяє постійно бути «на крок вперед супротивника». Застосування цього методу в цивільній сфері означає стійку підтримку конкурентоздатності виробленої продукції, фінансового стану підприємства.

4. Відмінністю конкурентної розвідки від промислового шпигунства є те, що КР здійснюється виятково в рамках існуючих державних законів, і свої

результати одержує завдяки аналітичній обробці величезної кількості найрізноманітніших відкритих інформаційних матеріалів.

**Перспективи подальших розробок у даному напрямку.** Одним із самих перспективних напрямків роботи із зазначеної проблематики вбачається подальше дослідження проблем проведення інформаційно-аналітичної розвідки засобами Інтернету. Цей комплекс заходів багато фахівців позначають і як комп'ютерну розвідку. Її сутність полягає в пошуку й передачі інформації з комп'ютерних систем і мереж «всесвітньої павутини» з наступною верифікацією й аналітичною обробкою.

#### БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Про інформацію : Закон України // Правда України. – 1992. – 2 жовтня.
2. Лист Державної служби України з питань захисту персональних даних від 05.02.2013 р. № 11/257-13.
3. Азоев Г. Л., Челенков А. П. Конкурентные преимущества фирмы. – М. : ОАО «Типография и новости», 2002.
4. Безопасность компьютерных систем. Компьютерная злочинність та її попередження / М. С. Вертузаєв, В. О. Голубєв, О. І. Котляревський, О. М. Юрченко / Під ред. О. П. Снігерьова. – Запоріжжя : ПВКФ «Павел», 2005.
5. Вертузаєв М. С., Голубєв В. О. Захист інформації в комп'ютерних системах / Під ред. О. П. Снігерьова. – Запоріжжя : ВЦ «Павел», 1998.
6. Куценко А. С. Основні проблеми і радикальні шляхи вирішення антикризового управління промисловими підприємствами : монографія / Українська академія наук. – К. : Фенікс, 2006.
7. Некоторые правовые аспекты защиты и использования сведений, накапливаемых в информационных системах // Борьба с преступностью за рубежом. – М. : ВИНТИ, 1990. – № 7. – С. 63–64; 1992. – № 6. – С. 13–14.

УДК 334.78:331.106.42

Толстая Н.В.

здобувач кафедри економічної теорії,  
Херсонський державний університет

## ФОРМУВАННЯ СТРАТЕГІЧНОГО ПОТЕНЦІАЛУ КОРПОРАТИВНИХ ПІДПРИЄМСТВ В УМОВАХ ЕКОНОМІЧНОГО РОЗВИТКУ POTENTIAL OF STRATEGIC CORPORATE ENTERPRISES IN AN ECONOMIC DEVELOPMENT

#### АНОТАЦІЯ

У статті розглянуто основні властивості, якими характеризується стратегічний потенціал корпоративного підприємства, проаналізовано механізм побудови концептуальної моделі формування стратегічного потенціалу, а також виділено підходи щодо формування стратегічного потенціалу корпоративного підприємства в умовах економічного розвитку.

**Ключові слова:** економічний розвиток, корпоративне підприємство, корпоративне управління, стратегічний потенціал, властивості економічної системи, синергія.

#### АННОТАЦІЯ

В статье рассмотрены основные свойства, которыми характеризуется стратегический потенциал корпоративного предприятия, проанализирован механизм построения концептуальной модели формирования стратегического потенциала, а также выделены подходы к формированию стратегического потенциала корпоративного предприятия в условиях экономического развития.

**Ключевые слова:** экономическое развитие, корпоративное предприятие, корпоративное управление, стратегический потенциал, свойства экономической системы, синергия.

#### ANNOTATION

The article deals with the basic properties that characterize the strategic potential of the corporate enterprise, analyzes the mechanism concep-

tual model of the strategic potential and selected approaches to forming strategic potential of corporate enterprises in economic development.

**Key words:** economic development, corporate enterprise, corporate governance, strategic potential, the properties of the economic system synergy.

**Постановка проблеми.** В умовах економічного розвитку, що характеризується високою динамічністю та нестабільністю процесів, визначальною умовою, необхідною для покращення ситуації на сучасному етапі розвитку економіки є необхідність створення більш стабільних і сприятливих умов, що забезпечать корпоративним підприємствам досягнення визначених ними довгострокових цілей свого розвитку. Керівники, проаналізувавши вплив факторів зовнішнього середовища можуть передбачити наявність потенційних загроз і можливості їх усунення. Тому особливо важливим стає вивчення нових підходів до корпоративного управління.

**Аналіз останніх досліджень і публікацій.** Дослідження питань пов'язаних із механізмом формування стратегічного потенціалу корпоративних підприємств останнім часом приділяється все більше уваги. Серед