УДК 005.332.4:005.921.1

Живко З. Б.
Львівський державний університет внутрішніх справ

ФОРМУВАННЯ СТРУКТУРНОЇ МОДЕЛІ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В КОНТЕКСТІ КОНТРРОЗВІДКИ

У статті досліджено основні аспекти формування контррозвідки, її завдання та важливість для економічної безпеки підприємства. Запропоновано структурну модель системи економічної безпеки підприємства з чітким зазначенням місця та ролі в ній контррозвідки, інформаційного забезпечення та моніторингу.
Ключові слова: система економічної безпеки підприємства (СЕБП), економічна розвідка, розвідувальна діяльність, контррозвідка, інформаційне забезпечення, моніторинг, персонал, служба безпеки підприємства (СБП)

Постановка проблеми. Розвідувальна діяльність сьогодні проводиться більшістю вітчизняних підприємств, а відтак, поруч із потребою отримання достовірної інформації про конкурентне середовище, не менш актуальною і важливою є проблема захисту власних таємниць, тобто виникає проблема ефективного функціонування контррозвідки. Саме тому дослідження цієї проблематики є актуальним та важливим для забезпечення економічної безпеки будь-якого бізнесу.

Аналіз останніх досліджень. З давніх-давен і до нині в розвідці існують чітко сформовані принципи, які і сьогодні є актуальними та вартими уваги, непорушними та обов'язковими. А саме: прямопропорційна залежність між збиранням розвідувальної інформації про конкурентів, партнерів, постачальників тощо, і захистом власної бази даних, що складає комерційну таємницю. За визначенням О. Івченка «контррозвідка – це захист своєї конфіденційної інформації від шпигунства» [1]. Економічна контррозвідка статус легітимності отримала лише після розвитку ринкових відносин. Саме ринок змушує підприємців не лише вивчати ділові стосунки з партнерами, особливості підписання угод, наміри та контакти конкурентів, але й приховувати власні плани, програми розвитку, забезпечення персоналу.

Слід погодитися з автором, що як і в традиційній контррозвідці, запобігання розкриттю своїх джерел інформації (нехай навіть і відкритих), а також методів збору інформації для конкурентної контррозвідки є пріоритетним завданням [1].

Особливо розвинена ця система в США, де американські спеціалісти з даного профілю розробили цілу низку методик і технологій захисту як розвідувальних даних про конкурентів, так і захисту комерційно важливої інформації від викрадення і просочування. Вітчизняні бізнесмени на початкових етапах створення служб безпеки запозичали досвід західних фахівців з конкурентної розвідки, та охоче залучали до роботи колишніх працівників МВС, прокуратури та СБУ.

Питаннями економічної розвідки займалися як вітчизняні, так і зарубіжні науковці, зокрема: Г. Андрощук [3], А. Вайс [4, 5], Д. Геррінг [6], М. Живко[7, 8], П. Крайнєв [3], А. Митрофанов [9], А. Неласа [7], В. Ярочкін [10] та багато інших, однак питання саме контррозвідки є мало вивченими і дослідженими.

Виділення невирішених раніше частин загальної проблеми. Для того, щоб інформація, яка належить підприємству, набула підстав для правового захисту, її слід подати як відомості, що містять комерційну таємницю та конфіденційну інформацію, які є власністю суб'єкта господарської діяльності. Цей аспект як полегшує роботу контррозвідки, так і ускладнює, адже вимагає виконання певної процедури щодо визначення інформації в якості комерційної таємниці.

Необхідно зауважити, що чіткого нормативного регламентування процесу організації та реалізації режиму комерційної таємниці немає. Підрозділу контррозвідки потрібно не лише в межах чинного законодавства визначити конфіденційну та таємну інформацію, але й захистити її та персонал, який дотичний до неї. Тому спробуємо сформувати дієву модель контррозвідки в СЕБП.

Виклад основного матеріалу. У найзагальніших рисах процес конкурентної розвідки і контррозвідки в системі економічної безпеки підприємства складається з трьох етапів: (1) внутрішній моніторинг; (2) зовнішній моніторинг; (3) аналітична робота.

Внутрішній моніторинг припускає, що працівники служби безпеки всіляко захищають підприємство від проникнення «шпигунів» і розвідників, а також відстежувати дотримання співробітниками підприємства внутрішніх правил щодо нерозголошення конфіденційних даних [11, с. 201]. Для цих потреб активно застосовуються як загальні інформаційно-комунікаційні системи, так і спеціальні інформаційні системи. Однією із найбільш поширених є IPC (Information Protection and Control), яка захищає інформацію методом шифровки носіїв, а також повним контролем всіх можливих носіїв і каналів, через які, з технічної точки зору, може відбуватися витік важливої інформації (e-mail, icq, Skype, соціальні мережі, принтери, зовнішні носії, накопичувачі, USB, WiFi, Bluetooth і так далі). Особливої цінності така система набуває, враховуючи той факт, що до 75% конфіденційної корпоративної інформації розголошується мимоволі, помилково або з необачності персоналу.

Зовнішній моніторинг, відповідно до вище викладених положень, – це і є конкурентна розвідка в найбільш загальному розумінні. Він припускає збір повного об'єму інформації про конкурентів: технології, управління, об'єми збуту, чинники конкурентної переваги, стратегічні плани на майбутнє, стратегії завоювання ринку, можливі загрози для власного підприємства, методи оптимізації роботи, інновації і так далі.

Аналітична робота припускає проведення порівняльної характеристики, виявлення своїх сильних і слабких сторін, розробку конкретних рекомендацій для менеджменту з метою недопущення збитків, втрати частки ринку тощо [11, с. 202].

Відповідно до положень чинного законодавства інформація є комерційною таємницею за наявності таких ознак: 1) має дійсну або потенційну комерційну цінність унаслідок необізнаності з нею

третіх осіб; 2) до неї не існує вільного доступу на законних підставах; 3) власник або уповноважена ним особа вживає заходів щодо збереження її конфіденційності. Інформація, що становить комерційну таємницю, повинна бути зафіксована на матеріальному носії та забезпечена реквізитами, що дозволяють ідентифікувати її. Це можуть бути: результати дослідів і їх протоколи, дані про якість матеріалів, документація з виготовлення продукції, креслення, формули та рецепти, статистичні розрахунки, звіти про виготовлену продукцію або надані послуги, картотеки й електронні бази даних клієнтів, відомості про організацію виробництва, методи реклами, інформація про джерела фінансування тощо. У деяких ситуаціях інформація, що становить комерційну таємницю, може втілюватися в предметах – виробах, блоках, агрегатах, приборах і речовинах. Однак і в цьому разі для визнання відомостей, втілених у предметах, комерційною таємницею необхідно, щоб інформація була попередньо задокументована в установленому порядку.

Документальне забезпечення правового статусу комерційної таємниці та конфіденційної інформації на підприємстві сприятиме надійному її захисту як у випадку розголошення відповідних відомостей працівниками підприємства, так і цілеспрямованими діями конкурентів щодо її викрадення.

Можна виділити три групи типових способів злочинних посягань на відомості, що становлять комерційну або банківську таємницю: 1) незаконне збирання відомостей, що становлять комерційну або банківську таємницю; 2) незаконне використання таких відомостей; 3) умисне розголошення такої інформації [11, с. 207].

Незаконне збирання відомостей може виявлятися у: 1) викраденні відповідної інформації чи об'єктів, що її містять, з приміщень, де вони зберігалися. Така крадіжка може бути як відкритою, так і завуальованою, коли справжні предмети посягання (документи, вироби, що містять комерційну таємницю) викрадаються разом із іншими і в такий спосіб створюється хибне уявлення про дійсні цілі злочинців; 2) таємному проникненні злочинця до приміщення й копіювання інформації паперовим чи електронним способом. Для фіксації інформації та її пересилання можуть застосовуватися мобільні телефони з вбудованими фотокамерами й послуга MMS; 3) підкупі співробітника підприємства, який мав чи має законний доступ до інформації. Працівник за певні матеріальні чи інші блага копіює інформацію та передає її замовникові. Якщо людина вже звільнилася або на сьогодні не має законного доступу, але інформація, якою вона володіла раніше, ще не втратила комерційної привабливості, то вона її просто повідомляє; 4) підкупі посередників у переговорах, які володіють певною інформацією; 5) незаконному отриманні інформації у співробітників правоохоронних або контролюючих органів, яким вона стала відома внаслідок виконання ними службових обов'язків; 6) погрозах фізичним насильством над особою чи її близькими родичами, якій інформація була довірена в результаті виконання її трудових обов'язків; 7) шантажі працівника, який знаходиться на «гачку» внаслідок певних життєвих обставин; 8) впровадженні свого агента в штат підприємства під виглядом звичайного співробітника; 9) вербуванні діючого працівника або спонуканні до розголошення звільненого із застосуванням мотивів етнічної, расової, релігійної близькості, бажанням помститися керівникові за незаконне звільнення, переведення на іншу роботу, зняття з посади; 10) використанні різних технічних пристроїв, що фіксують і передають інформацію. За допомогою спеціальної техніки здійснюється прослуховування приміщень або зняття інформації з каналів зв'язку; 11) проникненні в комп'ютерні мережі. Для цього злочинці застосовують спеціальні комп'ютерні програми, які дозволяють відшуковувати необхідні дані та копіювати їх.

Незаконним використанням комерційної таємниці є впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу власника чи уповноваженої на те особи таких відомостей. Зокрема, незаконне використання може мати такі форми:

1) пред'явлення майнових або інших вимог до власника комерційної чи банківської таємниці за повернення або нерозголошення відповідних відомостей. Такі вимоги можуть стосуватися повернення на роботу, призначення на вищу посаду, звільнення іншого працівника, надання послуг тощо;

2) продаж інформації третім особам (електронних баз даних операторів телефонного зв'язку, ДАІ, БТІ та ін.);

3) обмін інформації, що становить комерційну чи банківську таємницю, на іншу або матеріальні цінності;

4) корегування своїх дій при укладанні договорів з власником такої таємниці.

Більшість співробітників підприємства не має уявлення, що одержувана ними в ході роботи інформація є конфіденційною й не підлягає розголошенню. Звідси особливо важливим є проведення роз'яснення при прийомі на роботу щодо необхідності збереження комерційної інформації, визначення безпосередніх об'єктів, які підпадають під цю категорію, здійснення періодичних перевірок щодо дотримання даних вимог.

Отримання достовірної, повної та своєчасної інформації про дії конкурентів, її моніторинг є метою не лише розвідки, але й контррозвідки, адже слід пам'ятати, що не лише ваша фірма прагне отримати конфіденційну інформацію щодо бізнесу партнерів і конкурентів, але й конкуренти намагаються добратися до таємниць, гарантію збереження яких покладено на контррозвідку. Тому особа, що відповідає за моніторинг системи економічної безпеки підприємства, повинна дотримуватись таких правил:

- чітко визначати корисну і цінну інформацію, необхідну для розробки стратегії забезпечення економічної безпеки підприємства та здійснення тактичного управління й оперативної реалізації;

- зайва й помилкова інформація повинна вилучатися для оптимізації величини інформаційного потоку;

- відсутня інформація для ухвалення рішення повинна оперативно поповнюватися.

Зазначені проблемні питання вагомо впливають на об'єктивність оцінок і точність аналітичних розрахунків, підготовку й прийняття управлінських рішень щодо визначення складу заходів для забезпечення необхідного для розвитку рівня економічної безпеки вітчизняних підприємств. Тому і виникає невідкладна потреба як у створенні сучасних інформаційних систем та цільового програмного забезпечення (які дозволять здійснити моніторинг і прогностичну оцінку, підготувати результуючу інформацію з урахуванням особли-

востей сучасних процесів вироблення і нагромадження потенціалу виробничих економічних систем для досягнення високого рівня економічної безпеки), так і визначення об'єктів моніторингу, що є пріоритетним на даному історичному етапі розвитку української економіки.

Звернувшись до іноземного досвіду, як приклад можна привести організаційну структуру конкурентної розвідки американської корпорації Motorola, яка була першою корпорацією, що організувала таку структуру. Гібридна структура складається з центрального відділу розвідки, а також по одному-двох співробітниках інших підрозділів, яким доручено підтримувати комунікацію з відділом розвідки. В сукупності в корпорації Motorola конкурентною розвідкою займається до 30 осіб. Правильно побудована взаємодія між підрозділами дозволяє отримати значну економію. Зважаючи вище викладені аргументи, нами створено модель функціонування системи економічної безпеки підприємства, в якій виокремлено діяльність щодо конкурентної розвідки та контррозвідки (рис. 1).

Важливість інформаційного забезпечення процесу гарантування економічної безпеки вимагає при формуванні системи моніторингу враховувати наступні ключові моменти:

- по-перше, побудова алгоритму здійснення моніторингу системи економічної безпеки повинна базуватися на загальнонаукових інформаційних принципах;

- по-друге, наукові дослідження щодо активізації процесів з економічної безпеки слід провадити на основі попередньо визначених економічних закономірностей із урахуванням різноспрямованих факторів впливу на забезпечення адаптивності управління функціонуванням підприємства за умови високого рівня невизначеності. Лише тоді в них є чітка логіка, що виключає непослідовність вирішення проблем та кількісне обґрунтування позицій стосовно формування конкурентної позиції та вибору пріоритетів в управлінні внутрішнім середовищем;

- по-третє, саме оцінювання за результатами проведення моніторингу є найбільш поширеним показником, який характеризує динаміку процесів і відображає певний рівень використання усіх видів ресурсів як матеріальних, так і трудових й інтелектуальних не лише для економічної безпеки.

Висновки. Підводячи підсумки в проведеному дослідженні, доцільно взяти до уваги науковий доробок відомого фахівця з організації служб безпеки підприємств В. Мак-Мака [12], який у відомій книзі «Служба безпеки підприємства. Організаційно-управлінські і правові аспекти діяльності» не лише включив в організаційну діаграму служби безпеки підприємства відділ розвідки, але і приклав до загального опису діяльності розроблене ним положення про підрозділ розвідки, корпоративний нормативний документ, що визначає основні напрями її діяльності, функціональні обов'язки співробітників, їх права у взаєминах з іншими підрозділами компанії. Останнє важливо у зв'язку з тим, що до сил конкурентної розвідки корпорації належать і співробітники інших підрозділів компанії, що займаються збором і дослідженням інформації, підтримують комунікацію із співробітниками підрозділами розвідки.

Побудована модель не враховує специфіки діяльності певного підприємства, але відповідає ключовим позиціям сформованої у першому розділі роботи концепції забезпечення економічної безпеки підприємства та сучасним завданням, які ставляться перед системою економічної безпеки на вітчизняних суб'єктах господарської діяльності.

Доведено, що важливість інформаційного забезпечення процесу гарантування економічної безпеки вимагає при формуванні системи моніторингу дотримання трьох основних аспектів: (1) побудови алгоритму здійснення моніторингу; (2) необхідно враховувати різноспрямовані фактори впливу на забезпечення адаптивності управління функціонуванням підприємства за умови високого рівня невизначеності та (3) оцінювання за результатами проведення моніторингу є найбільш поширеним показником, який характеризує динаміку процесів, відображає певний рівень використання усіх видів ресурсів.

Рис. 1. Структурна модель системи економічної безпеки підприємства [11, с. 212]

Список літератури:
1. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка / Олег Івченко // Юридичний журнал «Юстініан». – №7, – 2003. – [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua
2. Економічна розвідка – це Ваша рука на пульсі конкурента // Матеріали сайту Рента Груп. – [Електронний ресурс]. – Режим доступу : http://arenta-group.com/ua/showarticle/172.html
3. Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны : Монография. /Издательский дом „ИнЮре". – Киев. – 2000 г.
4. Вайс А. Сбор конкурентной информации [Электронный ресурс] / А. Вайс. – Режим доступа : http://it2b.ru/blog/arhiv/769.html.
5. Вайс А. Краткое руководство по конкурентной разведке: как собирать и использовать информацию о конкурентах : Часть 2 [Электронный ресурс] / А. Вайс. – Режим доступа : http://it2b.ru/blog/arhiv/767.html.
6. Herring J.P. A Process to Identify and Define Intelligence Needs [Електронний ресурс] / Jan P. Herring. – Режим доступу : http://www.cipher-sys.com/
7. Живко З. Б. Управління інформаційною безпекою підприємства / З. Б. Живко, М. О. Живко, Г. В. Неласа // Сучасні проблеми і досягнення у галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей VI Міжнародної науково-практиичної конференції (19-21 вересня 2012р.), м. Запоріжжя : ЗНТУ, 2012. – С. 301–302
8. Живко З. Б. Конкурентна розвідка як спосіб отримання інформації в системі безпеки бізнесу / З. Б. Живко, М. О. Живко // Сучасні проблеми науки та освіти. Матеріали 12-ї Міжнародної міждисциплінарної науково-практичної конференції 27 квітня – 09 травня 2012 р. / Харків : Українська Асоціація «Жінки в науці та освіті», Харківський національний університет імені В. Н. Каразіна, 2012. – С. 143–145.
9. Митрофанов А. А. Экономическая безопасность коммерческих предприятий и деловая разведка [Электронный ресурс] / А. А. Митрофанов. – Режим доступа : http://www.bre.ru/security/22843.html.
10. Ярочкін В. І. «Система безопасности фирмы»/Ось-89 – Москва – 2003 р. – С. 5-36.
11. Живко З. Б. Економічна безпека підприємства: сутність, механізми забезпечення, управління. Монографія / З. Б. Живко. – Львів : Ліга-Прес, 2012. – 256 с.
12. Мак-Мак В. П. Служба безопасности предприятия (организационно–управленческие и правовые аспекты деятельности). – М : Мир безопасности, 1999. – 466 с.

Живко З. Б.
Львовский государственный университет внутренних дел

ФОРМИРОВАНИЕ СТРУКТУРНОЙ МОДЕЛИ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В КОНТЕКСТЕ КОНТРРАЗВЕДКИ

Резюме
В статье исследованы основные аспекты формирования контрразведки, задачи и важность её для экономической безопасности предприятия. Предложена структурная модель системы безопасности предприятия с чётким указанием места и роли контрразведки, информационного обеспечения и мониторинга.
Ключевые слова: система экономической безопасности предприятия (СЭБП), экономическая разведка, разведка, контрразведка, информационное обеспечение, мониторинг, персонал, служба безопасности предприятия (СБП)

Zhyvko Z. B.
Lviv State University of Internal Affairs

FORMATION OF STRUCTURAL MODEL OF ECONOMIC SECURITY COMPANIES IN THE CONTEXT COUNTERINTELLIGENCE

Summary
In this paper the basic aspects of the formation of counter-intelligence, tasks, and its importance for economic security. The structural model of enterprise security with a clear indication of the place and the role of counter-intelligence, information and monitoring.
Key words: economic security (ES), economic intelligence, intelligence, counter-intelligence, information support, monitoring, personnel, security service companies (SSC)