тересы российского бизнеса, и для его адаптации к российским условиям требуются значительные капиталовложения.

2. Отсутствие коммуникативной инфраструктуры между бизнесом и наукой. Нет налаженной связи и методик претворения высокорискованных проектов на практике. Инновационные проекты в связи с высокой степенью риска должны сопровождать или государство или техпарки, специальные венчурные центры. На практике подобные институты предпочитают работать с безрисковыми проектами, с низким сроком окупаемости. Более того, все процедуры получения рисковым проектам поддержки со стороны венчурных фондов чрезмерно забюрократизированы.

3. Отсутствие механизмов нефинансовой поддержки бизнеса: консалтинговой, информационной, экспортной.

Мы считаем, что в настоящее время применительно к российским предприятиям необходимо выделить еще один вид стратегии – интеграционная стратегия инновационного роста. При ней объединяющиеся предприятия (как путем слияния, так и поглощения) имеют своей целью в первую очередь развитие и модернизацию производства, так как именно это будет являться залогом стратегической стабильности компании. Мы считаем, что должен быть создан инновационно-модернизационный поток, эффективность которого невозможно обеспечить на отдельно взятом предприятии из-за недостатка ресурсов, в первую очередь финансовых. Это поток должен включать отдельные инновационные проекты с разными циклами жизни: при этом каждый последующий проект должен начинаться при достижении предыдущим максимальной точки доходности.

При помощи интеграционной стратегии инновационного роста предприятие сможет не только противостоять зарубежным производителям, создавая свои холдинговые структуры, но и создать стратегический задел успешного бизнеса путем модернизации производства, путем формирования инновационного потока проектов.

Из выбранного перечня отраслей формируются технологические платформы отраслевым методом. Это позволит сформировать устойчивые взаимосвязи государство – бизнес-наука-личность. Первоначально разрабатывается стратегическая карта по все уровням развития. На каждом этапе формирования стратегии составляется стратегическая карта отдельного уровня и сопоставляется с первоначальной. Таким образом, происходит анализ результативности и сравнение плановых показателей с фактическими и корректировка плановых показателей (стратегической карты).

Деятельность технологической платформы должна быть в той или иной степени направлена на:

- технологическую модернизацию и существенное повышение конкурентоспособности отдельных отраслей и секторов экономики;

- быстрое распространение некоторых передовых технологий в ряде отраслей и секторов экономики;

- разработку совокупности «прорывных» технологий, определяющих возможность появления новых рынков высокотехнологичной продукции (услуг).

При формировании подобной культуры на предприятии стратегическое планирование не будет рассматриваться как чужеродный механизм, а будет восприниматься как часть деятельности организации по достижению определенных целей и задач и краткосрочном и долгосрочных периодах. Таким образом, культура менеджмента предприятия должна выйти на качественно новый уровень – глобальный (стратегический) – уровень всего предприятия.

Список использованных источников

1. Авдеева Е.С. Форсайт – прогнозируемое будущее экономического развития / Е.С. Авдеева, Д.Д. Денисов // Российское предпринимательство. — 2012. — № 10 (208). — С. 4-10. — http://www.creativeconomy.ru/ articles/23858/.

2. Авдеева Е.С. Матричный инструментарий принятия управленческих решений стратегического характера / / Е.С. Авдеева, Д.Д. Денисов // Вестник Оренбургского государственного университета. – 2010. – Вып. №8 (114).

З. Б. Живко
д-р екон. наук
м. Львів

КОНТРРОЗВІДКА: СУТЬ І ЗАВДАННЯ В НЕСТАБІЛЬНИХ РИНКОВИХ УМОВАХ ГОСПОДАРЮВАННЯ

Постановка проблеми. Розвідувальна діяльність сьогодні з різним рівнем інтенсивності проводиться вітчизняними підприємствами, 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 як підсистема економічної безпеки підприємства. Контррозвідка – це захист своєї конфіденційної інформації від шпигунства.

Значення і роль контррозвідки в сучасних умовах ведення бізнесу зумовлено принаймні такими обставинами: по-перше, прагненням деяких підприємців усунути або нейтралізувати своїх конкурентів, користуючись засобами промислового шпигунства; по-друге, погіршенням кримінальної ситуації в країні, що створює поживне підґрунтя для певних верств населення вирішувати свої проблеми злочинним шляхом; по-третє, потребою здійснення захисних дій щодо представників державних органів управління, які використовують своє службове становище у злочинних цілях [2-3]. Відтак, зважаючи на складні умови ведення бізнесу в Україні, застосування контррозвідки є важливим і необхідним.

Аналіз досліджень та публікацій з проблеми. Серед авторів, що займались дослідженням даної теми можна виділити таких як В. Абрамов, Д. Ховіс, Є. Ющук, Ю. Воронова, Д. Міллер та інших. Відда-

ючи належне значимості напрацювань зазначених науковців, доцільно підкреслити, що окремі аспекти ефективності реалізації контррозвідувальних заходів залишилися без належної уваги.

Мета статті полягає в характеристиці суті та ключових завдань контррозвідувальної діяльності вітчизняних підприємств в сучасних умовах ведення бізнесу.

Виклад основного матеріалу. Перш за все зазначимо, що у розвідці існують чітко визначені принципи, які залишаються непорушними донині. Серед них – зв'язок між збиранням розвідувальних даних і захистом своєї власної інформації. Лише з переходом підприємств до ринкових відносин економічна (промислова) контррозвідка одержала легітимність і стала складовим елементом ділового процесу. В умовах конкуренції роль вивчення намірів конкурента і приховування своїх планів стає визначальною. 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. Особливо розвинена ця система в США. За довгі роки практики американські розвідники і контррозвідники розробили методики і технології захисту як збору даних про конкурентів, так і захисту власної компанії від просочування конфіденційної, стратегічно важливої інформації. Багато вітчизняних підприємств ще в 90-і рр. минулого століття на етапі становлення роботи своїх служб економічної безпеки брали приклад із західних фахівців з конкурентної розвідки, а також охоче залучали до роботи колишніх працівників спецслужб.

У найзагальніших рисах процес конкурентної розвідки і контррозвідки в системі економічної безпеки підприємства складається з трьох взаємопов'язаних складових: внутрішнього моніторингу, зовнішнього моніторингу та аналітичної роботи (рис. 1).

Внутрішній моніторинг припускає, що працівники служби безпеки всіляко захищають підприємство від проникнення «шпигунів» та «розвідників», а також відстежують дотримання співробітниками підприємства внутрішніх правил з нерозголошення конфіденційних даних.

Для цих потреб активно застосовуються 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 інформація (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 [9, с.346].

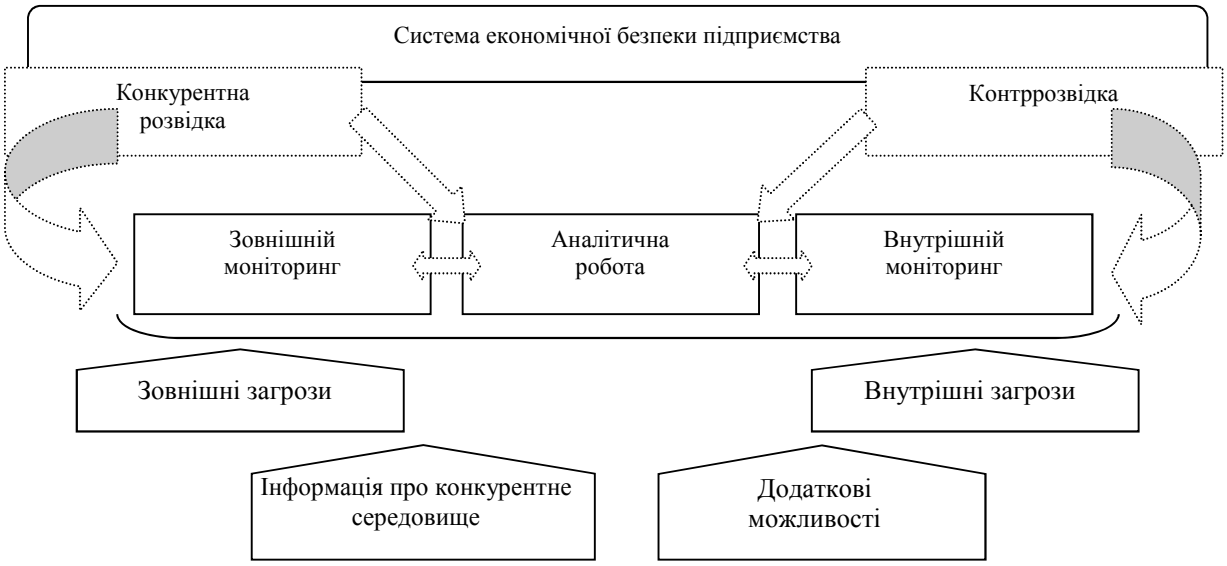

Рис. 1. Конкурентна розвідка та контррозвідка як функції системи економічної безпеки підприємства, авторська розробка

Аналітична робота передбачає проведення порівняльної характеристики, виявлення своїх сильних і слабких сторін, розробку конкретних рекомендацій для менеджменту з метою недопущення збитків, втрати частки ринку тощо.

Враховуючи, що метою контррозвідки є недопущення витоку чи оприлюднення інформації про діяльність, плани та наміри підприємства, доцільно виділити три групи типових способів злочинних посягань на інформацію, що становлять комерційну або банківську таємницю: незаконне збирання інформації, що становить комерційну або банківську таємницю; незаконне використання такої інформації; умисне розголошення такої інформації.

Протидія зазначеним способам злочинного посягання на конфіденційну інформацію є головним завданням контррозвідки. Водночас запобігання злочину є набагато ефективнішим порівняно з ліквідацією його наслідків. Проведення внутрішнього моніторингу дозволяє визначити сукупність слабких місць, завчасна ліквідація яких унеможливить реалізацію значної кількості загроз. Типовий перелік таких слабких місць для вітчизняних підприємств зводиться до такого [5-8].

Неефективна кадрова політика. Для більшості вітчизняних підприємств є традиційним найм на роботу працівників за таким критерієм як "родинні зв'язки". При цьому доволі частими є випадки, коли прийняті за таких принципом фахівці є абсолютно

некомпетентними у своїй роботі. Більше того, практика показує, що наявність родинних або дружніх зв'язків не є гарантією порядності й чесності. Багато з таких працівників уміло користуються своїм особливим положенням, будучи впевненими в повній безкарності. Але навіть там, де працівники набираються на конкурсній основі, їхнє минуле, а також деякі людські якості перевіряються досить поверхово. У результаті на підприємстві, практично, з моменту його відкриття знаходяться потенційні зловмисники, про наявність яких власники та керівники навіть не підозрюють.

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

Відсутня мотивація працівника. Низький рівень заробітної плати та незадоволення умовами роботи можуть перетворитися на реальну загрозу для економічної безпеки підприємства.

Неефективне керівництво, яке спричинено низьким рівнем менеджменту, що ускладнює процес діяльності підприємства і негативно впливає на рівень його економічної безпеки.

Атмосфера в колективі. Одним з найважливіших чинників, від якого залежить не лише безпека підприємства, є взаємини в колективі. Відомо, що дружній колектив є запорукою успіху підприємства. І дійсно, якщо працівник відчуває себе не найманцем, якого безжалісно експлуатують, а членом родини або частиною системи, то він, напевно, виявиться віддапішим своєму підприємству. Якщо підприємство намагається допомогти працівникові в його особистих утрудненнях, опікуватися про свій персонал не на словах, а на справі, то й працівник відповість тим же. Він стане сприймати проблеми підприємства як свої власні й, отже, стане активно допомагати в їхньому розв'язанні. Навпаки, ті колективи, відносини в яких прийнято називати складними, являють собою ласим шматком для зловмисника, який уміло використовуючи невдоволення й ненависть окремих співробітників, суттєво шкодить підприємству зсередини за допомогою його ж працівників.

При розробленні та/або вдосконаленні методичних засад здійсненні контррозвідувальних дій доцільно взяти до уваги науковий доробок відомого фахівця з організації служб безпеки підприємств В.П. Мак-Мака, який в останній редакції своєї відомої книги "Служба безпеки підприємства. Організаційно-управлінські і правові аспекти діяльності" [4] включив до організаційної структури служби економічної безпеки підприємства не лише відділ розвідки, але й підрозділ контррозвідки, визначив основні напрями його діяльності, функціональні обов'язки фахівців, їхні права у взаєминах з іншими підрозділами підприємства.

Як приклад зарубіжного досвіду можна привести організаційну структуру конкурентної розвідки американської корпорації Motorola, яка була першою корпорацією, що організувала таку структуру [4]. Гібридна структура складається з центрального відділу розвідки, а також одного-двох співробітників інших підрозділів, яким доручено підтримувати комунікацію з відділом розвідки. В сукупності в корпорації Motorola конкурентною розвідкою займається до 30 працівників. Правильно побудована взаємодія між підрозділами дозволяє отримати значну економію. Лише за рахунок централізації закупівлі і обробки інформації там щорічно економиться до 20 мільйонів доларів.

З урахуванням викладеного створено модель системи економічної безпеки підприємства, в якій виділено підрозділи конкурентної розвідки та контррозвідки (рис. 2).

Рис. 2. Структурна модель системи економічної безпеки підприємства , авторська розробка

Побудована модель системи економічної безпеки не враховує специфіки діяльності конкретного підприємства, але відповідає ключовим позиціям сформованої концепції забезпечення економічної безпеки підприємства та сучасним завданням, які ставляться перед системою економічної безпеки на вітчизняних підприємствах.

Виходячи з розробленої моделі системи економічної безпеки підприємства, мету діяльності контррозвідувального підрозділу можна визначити в такий спосіб: протидія розвідувальним заходам конкурентів і злочинним діям кримінальних груп чи окремих осіб, які негативно впливають на економічну безпеку та перешкоджають досягненню економічних інтересів підприємства.

Об'єктами діяльності контррозвідувального підрозділу слід вважати: фахівців підприємства, які є потенційними об'єктами розвідувальних заходів та/або злочинних дій зі сторони кримінальних структур чи окремих осіб; працівників підприємства, які мають доступ до інформації, яка є комерційною та банківською таємницею, надає підприємству суттєві конкурентні переваги; співробітників служби безпеки підприємства; працівників, які належать до групи ризику внаслідок злочинного минулого, притаманних шкідливих звичок, перебувають у родинних та інших зв'язках із конкурентами та ін.; звільнених працівників, які володіють цінною інформацією.

Визначена мета та об'єкти контррозвідувальної діяльності дозволяє визначити коло завдань підрозділу контррозвідки [1, с. 215]:

захист інформаційних ресурсів підприємства;

протидія економічному шпигунству;

захист усіх працівників підприємства від негативного впливу зі сторони злочинно орієнтованих груп чи окремих осіб;

нейтралізація внутрішніх загроз, які пов'язані із витокам конкурентно важливої інформації.

Виконання вищевказаних завдань забезпечує реалізацію сукупності функцій контррозвідки [1, с. 217]: 1) виявлення та доведення до відома вищого керівництва фактів та причин, що сприяють вчиненню правопорушень з боку персоналу підприємства; 2) спостереження за особами, які належать до групи ризику; 3) виявлення агентів промислового шпигунства з числа працівників підприємства; 4) забезпечення конфіденційності інформаційного обміну між підрозділами та посадовими особами; 5) захист комерційної та банківської таємниці; 6) з'ясування біографічних та інших характеристик претендентів на робочі місця; 7) консультування персоналу з питань забезпечення економічної безпеки підприємства.

Для об'єктивного оцінювання діяльності контррозвідувального підрозділу служби економічної безпеки підприємства необхідно розробити відповідні критерії та показники. До критеріїв діяльності контррозвідувального підрозділу можна віднести ступінь протидії розвідувальним заходам ділових конкурентів і злочинців, рівень запобігання та припинення правопорушень на підприємстві. Показниками, що доповнюють критерії, можуть бути такі: чисельність працівників, притягнутих до відповідальності за розголошення комерційної таємниці підприємства; кількість виявлених економічних (промислових) шпигунів; кількість виграних судових процесів у цивільних справах на підставі матеріалів контррозвідки; кількість службових розслідувань, проведених щодо персоналу підприємства; сума втрат, яких вдалося уникнути в наслідок виконання своїх функцій контррозвідкою.

Висновок. Узагальнюючи викладені вище результати теоретичних досліджень необхідно підкреслити, що контррозвідувальна діяльність як функція системи економічної безпеки підприємства дозволяє запобігти втратам в діяльності підприємства, зберегти його комерційну таємницю та конфіденційну інформацію і зрештою зміцнити економічну безпеку підприємства. Але для цього контррозвідувальна діяльність має бути належним чином організована, нею не можна у наш час нехтувати.

Список використаних джерел

1. Економічна безпека підприємств, організацій та установ : [підруч.] / [Ортинський В. Л., Керницький І. С., Живко З. Б. та ін.]. – К.: Алерта, 2011. – 704 с.

2. Живко З. Б. Економічна безпека підприємства: сутність, механізми забезпечення, управління : [монографія] / З. Б. Живко. – Львів: Ліга-Прес, 2012. – 256 с.

3. Живко З. Б. Інформаційна безпека бізнесу як складова економічної безпеки / З. Б. Живко, Л. Кутас, М. Живко // Актуальні проблеми забезпечення економічної безпеки України : ІІ наук.-практ. семінар з міжнар. участю, 16-18 груд. 2008 р. : тези доповід. – Тернопіль: ТНЕУ, 2008. – С. 77-78.

4. Митрофанов А. А. Экономическая безопасность коммерческих предприятий и деловая разведка [Электронный ресурс] / А. А. Митрофанов. – Режим доступа : http://www.bre.ru/security/22843.html.

5. Розслідування злочинів у сфері господарської діяльності: окремі криміналістичні методики : [монографія] / [Шепітько В. Ю., Коновалова В. О., Журавель В. А. та ін.] ; за ред. В. Ю. Шепітька. – Х.: Право, 2006. – С. 11-19.

6. Сайт профессионалов конкурентной разведки [Электронный ресурс]. – Режим доступа : <www.scip.org/>.

7. Титов В. В. Конкурентная розведка в современных условиях [Электронный ресурс] / В. В. Титов. – Режим доступа : http.www.bre.ru.

8. Хант Ч. Разведка на службе вашего предприятия: информация – основа успеха / Ч. Хант, В. Зартарьян. – К.: Укрзакордонвиза-сервис, 1992. – 159 с.

9. IPC / [Electronic resource]. – Mode of access : http://www. tadviser.ru/index.php/.