УДК 005.332.4:005.921.1
Живко З.Б., д.е.н.
Львівський державний університет внутрішніх справ

ЗНАЧЕННЯ І РОЛЬ КОНТРРОЗВІДКИ В СУЧАСНИХ УМОВАХ ВЕДЕННЯ БІЗНЕСУ

В статті досліджено внутрішній та зовнішній моніторинг захищеності підприємства. Розглянуто програмні засоби, які використовуються для несанкціонованого доступу з метою організування їх локалізації та протидії витоку інформації. Визначено основні функції контррозвідки та їх роль в убезпеченні підприємства.
Ключові слова: конкурентна розвідка, контррозвідка, внутрішній моніторинг, зовнішній моніторинг, функції контррозвідки, програмні засоби, несанкціонований доступ.

Zhyvko Z.

IMPORTANCE AND ROLE OF COUNTERINTELLIGENCE MODERN BUSINESS CONDITIONS

The nature and location of counter in providing security, conducting internal and external security monitoring company are investigated in the paper. Counterintelligence – it's the protection of the confidential information from espionage. Only when companies made the transition to a market economy (industrial) counterintelligence gained legitimacy and became an integral part of the business process. The role and intentions of competitors to hide their plans in a competitive is crucial in studying.
Keywords: competitive intelligence, counterintelligence, internal monitoring, external monitoring, counterintelligence functions, software, unauthorized access.

Живко З.Б.

ЗНАЧЕНИЕ И РОЛЬ КОНТРРАЗВЕДКИ В СОВРЕМЕННЫХ УСЛОВИЯХ ВЕДЕНИЯ БИЗНЕСА

В статье исследованы внутренний и внешний мониторинг защищённости предприятия. Рассмотрены программные средства, которые используются для несанкционированного доступа с целью организации их локализации и противодействия утечки информации. Определены основные функции контрразведки и их роль в обеспечении безопасности предприятия.
Ключевые слова: конкурентная разведка, контрразведка, внутренний мониторинг, внешний мониторинг, функции контрразведки, программные средства, несанкционированный доступ.

Постановка проблеми у загальному вигляді і її зв'язок з важливими науковими та практичними завданнями. 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 функції системи економічної безпеки підприємства.

Аналіз останніх досліджень, у яких започатковано вирішення проблеми. В розвідці існують чітко сформовані принципи, які є актуальними і вартими уваги, непорушними та обов'язковими: прямопропорційна залежність між збиранням розвідувальної інформації про конкурентів, партнерів, постачальників тощо, і захистом власної бази даних, що складає комерційну таємницю.

Проблематикою економічної безпеки держави, підприємства, конкурентної розвідки, інформаційної безпеки займається низка українських та зарубіжних вчених:

Д. Бруксбенк [1], Б. Губський [2], О. Деревицький [3], А. Жуков [4], Г. Задорожний [5], Г.Козаченко [6], В. Мунтіян [7], А. Сухоруков [8], В. Ярочкін[9]. Однак, питання дослідження контррозвідки в сучасних умовах інформаційного суспільства не досліджені належним чином.

Цілі статті. Дослідити внутрішній та зовнішній моніторинг захищеності підприємства; програмні засоби, які використовуються для несанкціонованого доступу; функції контррозвідки та їх роль в убезпеченні підприємства.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. У розвідці існують чітко визначені принципи, які залишаються непорушними донині. Серед них – зв'язок між збиранням розвідувальних даних і захистом своєї власної інформації. Контррозвідка – це захист своєї конфіденційної інформації від шпигунства. 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.

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.

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).

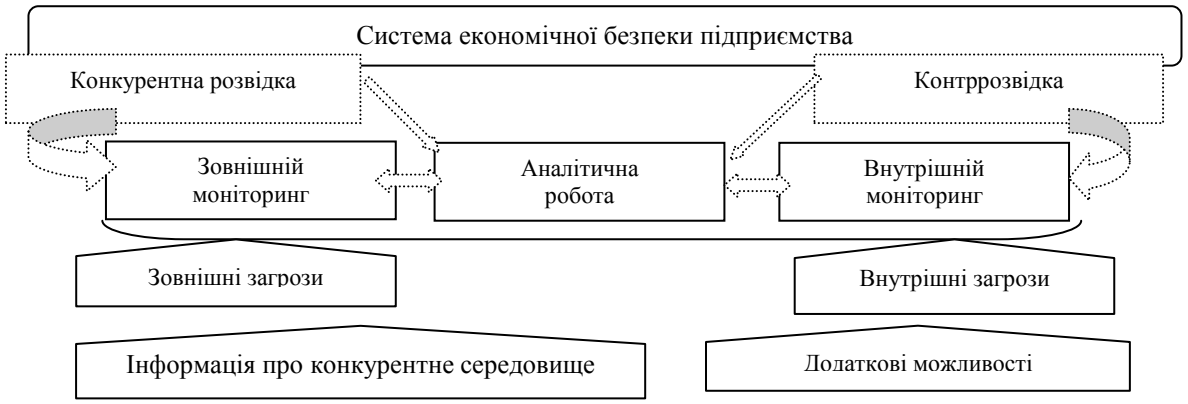

Рис. 1. Конкурентна розвідка та контррозвідка як функції системи економічної безпеки підприємства

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 [10].

Зовнішній моніторинг, і є, власне конкурентною розвідкою у найзагальнішому розумінні. Він передбачає збір повного обсягу інформації про конкурентів (технології, управління, обсяги збуту, чинники конкурентної переваги, стратегічні плани на майбутнє, стратегії завоювання ринку, можливі загрози для свого підприємства, методи оптимізації роботи, інновації та ін.).

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 розглянути способи ворожого збору та використання інформації.

Стосовно предмета дослідження можна 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.

Незаконне збирання інформації 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 послугою 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 для 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. Для цього застосовуються радіозакладки, мікрофони спрямованої дії, пристрої для зняття інформації з вікон за допомогою лазерних промінів, апаратура для виявлення й розшифровування електромагнітного випромінювання від офісної техніки, мініатюрні фото- та відеокамери. Таку техніку можуть встановлювати або використовувати як спеціально підготовлені особи, так і завербовані співробітники підприємства; проникненні в комп'ютерні мережі. Для цього злочинці застосовують спеціальні комп'ютерні програми, які дозволяють відшуковувати необхідні дані та копіювати їх [11].

Програмні засоби, які використовуються для несанкціонованого доступу, поділяються на:

експлоіти (сканери) – програми, які використовують певні недоліки в програмному забезпеченні ЕОМ чи мережі, що призводить до настання бажаних для злочинця результатів;

сніфери – дозволяють перехоплювати дані, що передаються мережами електрозв'язку;

"троянський кінь" – програми цієї групи приховано встановлюються в будь-який спосіб на комп'ютері, що цікавить злочинців, як правило, шляхом вбудовування в іншу легальну програму. При цьому програма-носій, виконуючи свої прямі функції, здійснює й додаткові, закладені в неї розробником (наприклад, збирання й передавання конфіденційної інформації);

руткіти – набір програм, який дозволяє злочинцю внести певні зміни в програмне середовище комп'ютера-жертви для здійснення контролю та отримання в подальшому легкого доступу до нього [12, с. 56-58].

Незаконним використанням комерційної чи банківської таємниці є впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу власника чи уповноваженої особи таких відомостей. Зокрема, незаконне використання може мати такі форми: (1) висування 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 [13].

Незаконне використання відомостей, що становлять комерційну або банківську таємницю, можливе і в іншому вигляді, наприклад, через умисне розголошення таких відомостей [14, с. 106]. Розголошення може здійснюватися усно, письмово, з використанням засобів зв'язку й масової інформації, комп'ютерних мереж та ін. Таке розголошення вчиняють особи, яким ця інформація стала відома внаслідок професійної або службової діяльності. Це можуть бути як працівники самого підприємства, установи, організації, так і співробітники правоохоронних чи контролюючих органів, які отримали цю інформацію, користуючись своїм службовим становищем, але не для виконання своїх функцій, а для передавання конкурентам чи використання в інших протиправних цілях, наприклад, для різних видів шантажу щодо здійснення чи нездійснення певних дій за нерозголошення комерційної або банківської таємниці.

Протидія охарактеризованим вище 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 [15-17].

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 лояльним до свого підприємства. 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" [18] 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.

Пропонуємо модель функціонування контррозвідки підприємства (рис. 2).

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

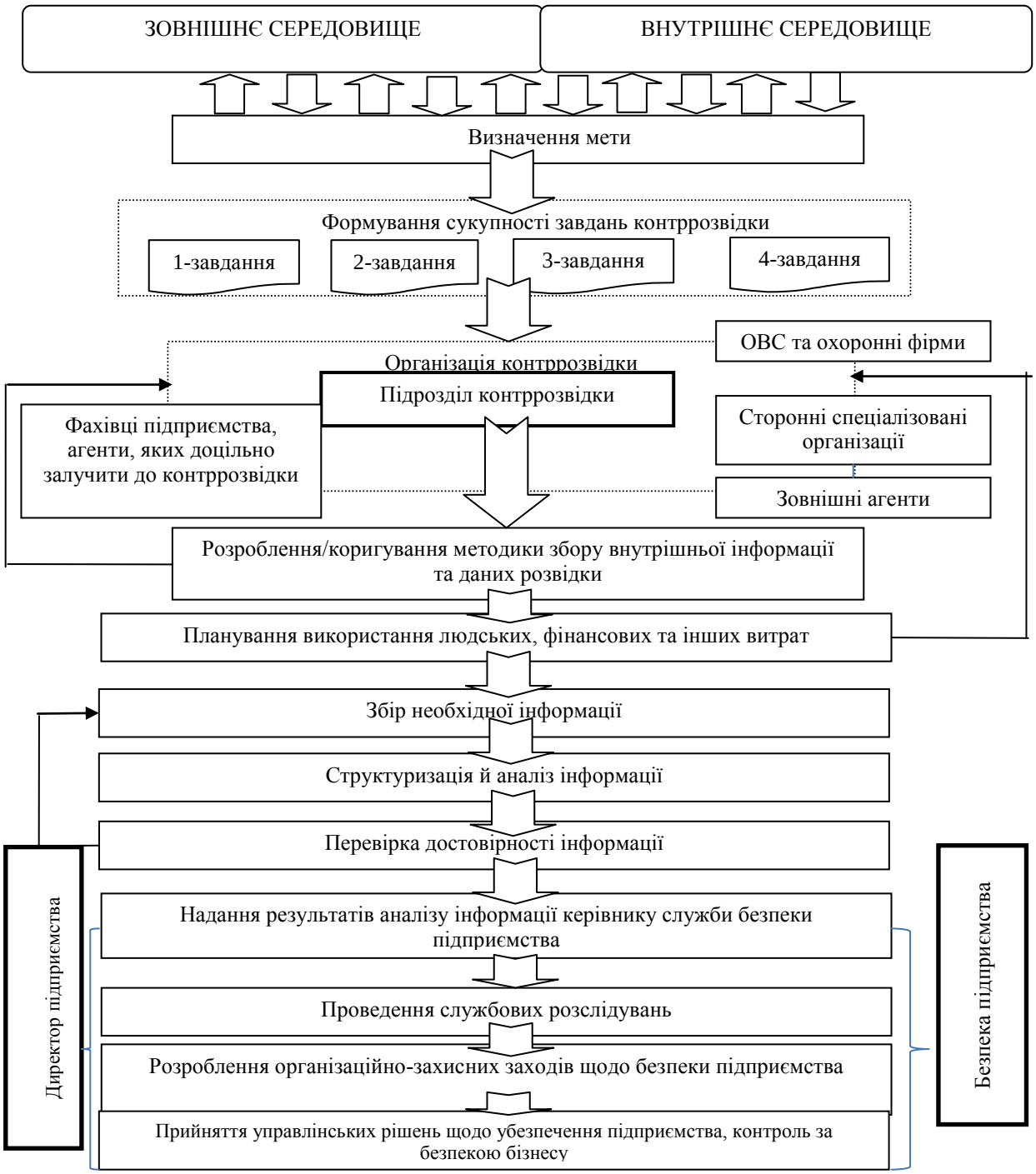

Рис. 2. Структурна модель контррозвідки підприємства

*авторська розробка

Висновок. Отже, для підрозділу контррозвідки підприємства велике значення має діяльність конкурентної розвідки підприємства, зовнішній і внутрішній моніторинг підприємства, моральний клімат колективу, визначення груп ризику, своєчасне отримання й опрацювання інформації, співпраця з правоохоронними органами та охоронними структурами. Запобігання злочину є набагато ефективнішим порівняно з ліквідацією його наслідків, тому саме системний та комплексний підхід до питання забезпечення безпеки підприємства дозволить виробити єдиний підхід і механізм убезпечення бізнесу.

Список використаних джерел:

1.Бруксбенк Д. Руководство по безопасности / Д. Брунсбенк, Дж. Уилсон / Пер с анг. – М.: ЮНИТИ-ДАНА, 2003. – 319 с.

2.Губський Б. В. Економічна безпека України: методологія виміру, стан і стратегія забезпечення / Б. В. Губський. – К., 2001. – 122 с.
3.Деревицкий А. Искусство «боевого говоруна» / А. Деревицкий. – Спб.: Питер, 2006. – 192 с.: ил.
4.Жуков А. Все о защите коммерческой информации / А. Жуков, М. Маркин. – К., 2002. – 120 с.
5.Задорожний Г. В. Економічна безпека і тіньова економіка. Монографія / Г. В. Задорожний, П. О. Іщенко, С. В. Тютюнников. – Х.: ХІБМ, 1999. – 208 с.
6.Козаченко Г. В. Економічна безпека підприємства: сутність та механізми забезпечення : [монографія] / Г. В. Козаченко, В. П. Пономарьов, О. М. Ляшенко. – К.: Лібра, 2003. – 280 с.
7.Мунтіян В. І. Економічна безпека України / В. І. Мунтіян. – К.: КВІЦ, 1999. – 463 с.
8.Сухоруков А.І. Фінансова безпека держави, Навчальний посібник / А. І. Сухоруков, О. Д. Ладюк. – К.: ЦУЛ, 2007. – 192 с.
9.Ярочкин В.И. Система безопасности фирмы/ В. И. Ярочкин. – М.: Ось-89, 1998. – 192 с.
10. IPC / [Electronic resource]. – Mode of access : http://www. tadviser.ru/index.php/.
11. Іващенко В. Основні методи незаконного збирання та розголошення комерційної таємниці [Електронний ресурс] / В. Іващенко. – Режим доступу : http://www.justinian.com.ua/article.php?id=2359.
12. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та комп'ютерних технологій / [Скалозуб Л. П., Василинчук В. І., Лебідь С. А. та ін.] ; за ред. О. М. Джужі. — К.: ДДСБЕЗ, 2009. – С. 56–58.
13. Минзов А. С. Методы сбора информации при ведении деловой (конкурентной) разведки [Электронный ресурс] / А. С. Минзов. — Режим доступа : http://www.it2b.ru/blog/arhiv/254.html.
14. Кримінальне право України: особлива частина : [підруч.] / [Баулін Ю. В., Борисов В. І., Тютюгін В. І. та ін.] ; за ред. В. В. Сташиса, В. Я. Тація. — [4-те вид., переробл. і допов.]. – Х.: Право, 2010. – 229 с.
15. 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.
16. Сайт профессионалов конкурентной разведки [Электронный ресурс]. – Режим доступа : www.scip.org.
17. Титов В. В. Конкурентная розведка в современных условиях [Электронный ресурс] / В. В. Титов. –Режим доступа : http.www.bre.ru.
18. Мак-Мак В. П. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности / В. П. Мак-Мак. – М.: Мир безопасности, 1999. — 160 с.