

УДК 338.246:005.936

DOI: <https://doi.org/10.32782/2415-8801/2020-2.3>**Березіна Л.М.**

доктор економічних наук, професор,
професор кафедри економіки
та міжнародних економічних відносин,
Полтавська державна аграрна академія

Братанов Б.В.

здобувач вищої освіти ступеня доктора філософії,
Полтавська державна аграрна академія

ХАРАКТЕРНІ ОСОБЛИВОСТІ КОНКУРЕНТНОЇ РОЗВІДКИ ТА ПРОМИСЛОВОГО ШПИГУНСТВА ПІДПРИЄМСТВ

У статті проведено порівняльний аналіз конкурентної розвідки та промислового шпигунства. Надано теоретичну інтерпретацію зазначених категорій та досліджено характерні особливості конкурентної розвідки. Розглянуто її окремі аспекти як інформаційно-аналітичної роботи сучасного підприємства для отримання конкурентних переваг та досягнення цілей підприємницької діяльності. Визначено основні результати конкурентної розвідки, означено її необхідність як інструменту ефективного управління діяльністю сучасного бізнесу. Розглянуто особливості промислового шпигунства як загрози для сфери інтелектуальної власності. Названо цілі, які переслідує промисловий шпionaж. Дано характеристику чинникам, що сприяють розвитку промислового шпигунства в Україні. Визначено основні кроки підприємства, які допоможуть запобігти промислому шпionaжу.

Ключові слова: економічна безпека, розвідка, конкурентна розвідка, шпionaж, промислове шпигунство, інформація, гіперконкуренція.

ХАРАКТЕРНЫЕ ОСОБЕННОСТИ КОНКУРЕНТНОЙ РАЗВЕДКИ И ПРОМЫШЛЕННОГО ШПИОНАЖА ПРЕДПРИЯТИЙ

Березина Л.М., Братанов Б.В.

В статье проведен сравнительный анализ конкурентной разведки и промышленного шпионажа. Представлена теоретическая интерпретация данных категорий и исследованы характерные особенности конкурентной разведки. Рассмотрены ее отдельные аспекты как информационно-аналитической работы современного предприятия для получения конкурентных преимуществ и достижения целей предпринимательской деятельности. Определены основные результаты конкурентной разведки, отмечена ее необходимость как инструмента эффективного управления деятельностью современного бизнеса. Рассмотрены особенности промышленного шпионажа как угрозы для сферы интеллектуальной собственности. Названы цели, которые преследует промышленный шпионаж. Дана характеристика факторам, способствующим развитию промышленного шпионажа в Украине. Указаны основные шаги предприятия, которые его предотвратят.

Ключевые слова: экономическая безопасность, разведка, конкурентная разведка, шпионаж, промышленный шпионаж, информация, гиперконкуренция.

CHARACTERISTIC FEATURES OF COMPETITIVE INTELLIGENCE
AND INDUSTRIAL SPYING OF ENTERPRISES

Berezina Lyudmila, Bratanov Bohdan

In today's world businesses which adept competitive intelligence in their activity are more likely to succeed. The level of competition in the world is constantly increasing and competitive intelligence, when it is used effectively, can be a determining factor that might lead the company which is in danger of complete defeat to the success. However, nowadays there is no clear and harmonized system of actions for timely detection, prevention, counteraction and controlling industrial espionage at domestic enterprises, which provides illegal methods and technologies and means primarily operational activities, including illegal penetration on the competitors' territory, blackmailing, collecting information from the communication channels, bribery, surveillance, information theft, etc. This article provides a comparative analysis of competitive intelligence and industrial espionage. The characteristic features of competitive intelligence have been studied. Some aspects of this notion are considered as information and analytical activity of a modern enterprise in order to obtain competitive advantages and achieve the goals of entrepreneurial activity. The necessity of competitive intelligence is determined as a tool for effective management of modern business activity. The author defines the concept of "competitive intelligence", which differs from the existing definitions. The author focuses out attention on the introduction of timely changes in the enterprise, taking into account the satisfaction of the potential needs of consumers and the value of their own business. The features of industrial espionage as a threat to the intellectual property are also considered. The goals which industrial espionage pursue are named in this study. Hypercompetition is a type of industrial espionage and it is considered in the work. Hypercompetition includes different types of illegal methods of competitive pressure by different subjects of economic activity in order to create unfavourable conditions or crises for their own benefit. The characteristics contributing to the development of industrial espionage in Ukraine are also described. Moreover, the company's basic steps which help to prevent industrial espionage were identified.

Keywords: economic security, intelligence, competitive intelligence, espionage, industrial espionage/spying, information, hypercompetition.

Постановка проблеми. Стрімкі зміни в сучасному ринковому середовищі змушують підприємства до боротьби за захист власних інтересів, інформації від посягань конкурентів. У цьому полягає основне завдання економічної безпеки, яка має бути комплексом заходів, спрямованих на постійний стійкий розвиток підприємства, що забезпечує механізм протидії загрозам із боку оточуючого середовища.

Серед основних чинників, які мають значний вплив на ефективність ведення господарської діяльності, виокремлюють конкурентну розвідку та промисловий шпіонаж. Їхня мета полягає у заволодінні інтелектуальною власністю конкуруючого підприємства законними або нелегальними шляхами.

Проблема захисту від нечесних конкурентів та отримання необхідної інформації для власної ефективної діяльності стали одними з актуальних аспектів господарювання у підприємствах, якими не можна нехтувати.

Аналіз останніх досліджень і публікацій. Питання, пов'язані зі зростанням значущості промислового шпигунства в сучасному світі, беруть початок у працях таких іноземних учених, як П. Райт, Раду Сьон, Т. Гловер, М. Ахмед, С. Девіс та ін. Хоча вітчизняні дослідження питань щодо захисту консолідованої інформації, понять конкурентної розвідки та промислового шпигунства відстають від закордонних, проте схожі питання підіймаються і нашими вченими, а саме: М.В. Черкашиною, В.Ю. Богдановичем, Т.П. Ткаченко, В.Л. Ортинським, А.М. Штангретом, Ф.В. Акулініною, В.Л. Диканем, М.В. Куркіним, А.О. Беседіною, Т.Е. Сухоруковою, А.М. Вергуном, В.В. Бадром, В.Д. Немцовим, Л.С. Довгань, М.Г. Саєнко, А.О. Андрейчиковим, З.Б. Живко [2], Б.М. Андрушків [4], Ю.С. Якубівською [5] та ін. Зазначені науковці зробили вагомий внесок у розкриття сутності понять «конкурентна розвідка» та «промислове шпигунство», проаналізували складники та принципи їх взаємозв'язку.

Постановка завдання. Метою статті є дослідження змісту понять конкурентної розвідки та промислового шпигунства, їх застосування на практиці та наслідків для підприємств на теренах України. Досягнення окресленої мети зумовлює вирішення комплексу завдань, а саме: розмежування понять «конкурентна розвідка» та «промислове шпигунство», виявлення їхніх складників, чинників впливу, загроз та можливих шляхів їх подолання.

Виклад основного матеріалу дослідження. Нині вітчизняним підприємствам доводиться функціонувати в умовах жорсткої конкуренції, постійно підвищуючи свою конкурентоспроможність, збільшуючи частку продукції чи послуг на ринку, перебуваючи в боротьбі за власних клієнтів. Тому процеси, пов'язані зі збором, аналізом та накопиченням інформації про стан бізнесу конкурентів, структури ринку, є життєво необхідними для будь-якого суб'єкта господарювання. Пріоритетними у забезпеченні ефективної діяльності підприємства є також його конкурентні переваги: унікальність, механізми формування, зберігання та реалізації продукції й інформації, а найголовніше – як можна забезпечити їх захист у процесі конкурентної боротьби. Такі процеси, як збір даних та розширення їх оцінка, також потребують реорганізації для зменшення затрат часу на збирання та аналіз інформації, забезпечення її достовірності, точність викладення керівникам та можливість збереження як історичної довідки для подальшого проведення ситуаційного аналізу. А тому перед топ-менеджерами будь-якого підприємства постає питання щодо збалансування та оптимізації системи економічної безпеки до стабільності стану його сталого розвитку в реаліях динамічних змін вітчизняної економіки. Вирішення даної проблематики вбачаємо в упорядкуванні збору та аналізу даних, що, своєю чергою, дасть змогу раціонально й ефективно функціонувати на ринку, враховуючи при цьому наявні

та приховані ризики та вживаючи заходів для їх попередження чи протидії.

Рушійною силою сучасного економічного прогресу вважають конкуренцію, оскільки саме вона окреслює межі дозволеного для всіх суб'єктів ринку та змушує дотримуватися законів щодо підвищення рівня ефективності виробництва. Маркетинговий складник бізнес-плану сучасного підприємства наполегливо рекомендує оцінювати конкурентів, оскільки чим більше підприємець знає про своїх суперників, тим ефективніша його комерційна політика ведення бізнесу. Тому об'єктивною є необхідність, з одного боку, у збиранні інформації про конкурента, а з іншого – у захисті інформації про його бізнес. Цю проблему вирішують за допомогою розвідувальної діяльності.

Найчастіше у спеціалізованій літературі можна зустріти такі поняття, як «економічна розвідка», «комерційна розвідка», «військова розвідка», «політична розвідка» тощо. При цьому у кожному з них виявляються свої складники, а класифікація є досить умовною та залежить від функціональних характеристик об'єкта розвідки (конкурента).

Зміст розвідки (економічної, виробничої, конкурентної) полягає в організації та проведенні заходів, спрямованих на збір інформації, необхідної для успішного розвитку компанії, в її кваліфікованій обробці та у формулюванні висновків про можливі дії конкурентів.

Деякі вчені ототожнюють поняття економічної, конкурентної та бізнес-розвідки. Однак ми погоджуємося з думкою Т.Б. Кузенко, Л.С. Мартошевої, О.В. Грачова, О.Ю. Литовченко, які вважають, що економічна розвідка більш складна за своєю структурою порівняно з іншими видами. Саме їй підпорядковуються комерційна розвідка та промислове шпигунство. Зміст розвідки зводиться до організації та проведення заходів, що спрямовані на збір необхідної для успішного розвитку діяльності підприємства інформації, її кваліфікованої обробки й формування висновків щодо можливих дій конкурентів, інших юридичних та фізичних осіб [1, с. 199–200].

На нашу думку, економічну розвідку доцільно розуміти як діяльність, яка здійснюється спеціальними засобами, методами і прийомами з метою забезпечення вищого керівництва розвідувальною інформацією щодо промисловості, транспорту, торгівлі, фінансової та грошово-кредитної системи, природних ресурсів та ін.; сприяння реалізації й захисту корпоративних інтересів та протидії зовнішнім загрозам безпеці підприємства.

Економічна розвідка включає три елементи діяльності: організацію розвідки, отримання необхідної інформації та її оброблення. Ці складники повністю взаємозалежні, ігнорування хоча б однієї з них призводить до припинення функціонування всієї системи.

Нині серед активно використовуваних методів збору розвідувальної інформації є такі:

- контрольна закупівля товарів у конкурентів для подальшого вивчення;
- відвідування підприємств-конкурентів;
- присутність власних агентів на презентаціях, виставках, конференціях конкурентів;
- переговори з конкурентами, у процесі яких свіdomo вивідується додаткова інформація;
- викрадення ноу-хау, аванпроектів та іншої технічної інформації.

У світовій практиці надання актуальної, достовірної та повної інформації вищому керівництву, орієнтованій на прийняття оптимальних управлінських рішень, можливе не лише за допомогою розвідувальних, а й завдяки контррозвідувальним технологіям у веденні бізнесу. Західна наукова література цій функції управління дала назву «бізнес-розвідка» (business intelligence), або «конкурентна розвідка» (competitive intelligence).

З.Б. Живко акцентує увагу на важливості визначення конкурентної розвідки та контррозвідки у структурі системи економічної безпеки. Зокрема, здійснення конкурентної розвідки повинне передбачати вивчення конкурентного середовища, ідентифікацію зовнішніх загроз і ризиків, прогнозування зміни зовнішнього середовища, розроблення превентивних заходів захисту, протидію недружньому злиттю та поглинанню, а контррозвідки – виявлення слабких місць у внутрішньому середовищі, перекриття каналів витоку цінної інформації, забезпечення збереження комерційної таємниці, прогнозу моменту виникнення та тенденцій розвитку кризових процесів [2, с. 212].

Конкурентною розвідкою описуються особливості правової та етичної діяльності про систематичний збір, оцінку та управління інформацією щодо конкурентів. Це включає дослідження газетних статей, публікацій компанії, вебсайтів, патентних заявок, спеціалізованих баз даних та інформації на виставках, що дає змогу визначити інформацію про підприємство. В економічній реальності «конкурентну інформацію» характеризують як «застосування принципів і практик військової та національної розвідки у сфері глобального бізнесу» [3].

Отже, конкурентну розвідку, на нашу думку, доцільно розглядати як систематичний процес, який включає збір, структуризацію, аналіз і оцінку інформації щодо внутрішнього середовища та зовнішнього оточення підприємства; доведення до вищого керівництва відомостей для прийняття ефективних та якісних стратегічних і важливих тактичних рішень у бізнесі, що дадуть змогу передбачити зміни на ринку та прийняти при цьому адекватні рішення, які дадуть змогу керувати ризиками (у разі неможливості їх попередження чи уникнення), запровадження своєчасних змін на підприємстві, беручи при цьому до уваги задоволення потенційних потреб споживачів та підвищення вартості власного бізнесу.

Сьогодні діяльність суб'єктів економічної безпеки на підприємствах базується на інформації, яка сповіщає про стан зовнішньої та внутрішньої безпеки підприємства, зокрема підрозділи конкурентної розвідки відповідають за аналіз та збір інформації із зовнішніх джерел, хоча деяка інформація фахівцями конкурентної розвідки використовується і з внутрішніх джерел.

У роботі «Целевая конкуренция», автором якої є фахівець з конкурентної розвідки П. Гордон, зазначається, що конкурентна розвідка дає компанії цілу низку істотних переваг [4, с. 52]. Зокрема, серед них:

- виявлення нових або можливих конкурентів;
- прогнозування змін на ринку;
- спрощення процесу переймання позитивного досвіду інших підприємств;
- прогноз дій конкурентів та партнерів;
- допомога в оцінці доцільності придбання чи відкриття нового бізнесу;

- вивчення нових технологій, продуктів чи процесів, які можуть вплинути на бізнес замовника;
- виявлення змін і вчасне реагування на них;
- вияв слабких місць конкурентів;
- можливість виявити потенційні джерела витоку конфіденційної інформації через співробітників компанії.

Основними результатами конкурентної розвідки є:

- оцінка наслідків дій суперників для підприємства, а також вивчення поточних тенденцій та прогноз майбутнього розвитку;
- діагностика зовнішнього конкурентного оточення й результати оцінки основних конкурентів на основі публічної та «приватної» інформації;
- оцінювання досвіду конкурентів та власного досвіду, виявлення конкурентного розриву;
- вивчення економічної стратегії, досвіду та факторів конкурентів, що визначають їх успіх;
- порівняльні дослідження, зосереджені на конкретних аспектах конкурентоспроможності підприємства.

Нині дуже часто відбувається синонімізація понять «конкурентна розвідка» та «промислове шпигунство». Хоча ці поняття мають спільні риси і багато хто їх отожднює, усе ж вони є різними. Метою і першого, і другого є одержання відомостей про діяльність наявних та потенційних конкурентів. І розвідкою, і шпигунством, як правило, займаються відповідні фахівці. Однак спільне на цьому закінчується.

Основна відмінність конкурентної розвідки від шпигунства полягає у тому, що вона здійснюється згідно з чинним законодавством, результати отримуються шляхом аналітичної обробки значних обсягів різноманітних відкритих даних. Із появою таких нових інформаційних технологій, як мережеві структури, комерційні бази даних, системи пошуку інформації тощо, та відносно дешевиною доступу до інформаційних ресурсів у аналітиків конкурентної розвідки з'явилася можливість отримувати якісні матеріали для подальшого використання керівництвом підприємства під час прийняття управлінських рішень. На протигагу цьому під час використання промислового шпигунства застосовують незаконні методи і прийоми. Це, насамперед, оперативні дослідження, які передбачають вербування інсайдерів та збір конфіденційної інформації з метою досягнення конкурентних переваг. При цьому, як правило, уточнюється, яка саме інформація буде цікавою для керівництва [3, с. 53–54].

Як уважають деякі науковці, промислове шпигунство виступає видом недобросовісної конкуренції, діяльністю з незаконного одержання інформації, яка становить комерційну цінність. Ключове слово у цьому визначенні – «незаконного» [5].

Звідси, вважаємо, що промислове шпигунство є видом недобросовісної конкуренції, за якої відбувається незаконний цілеспрямований збір інтелектуальних і конфіденційних відомостей, які становлять комерційну, службову, промислову таємницю, з метою випередження конкурентів, зміцнення власних позицій і/або захоплення більшої частки на ринку чи отримання інших переваг у бізнесі.

Серед учених, які займалися дослідженням специфіки боротьби з промисловим шпionaжем, існує думка, що іноді дуже складно відрізнити законні й нелегальні методи боротьби, зокрема якщо брати до уваги етичний бік збору інформації. Промислове шпигунство, як

правило, пов'язують із технологіями важкої промисловості, включаючи комп'ютерне програмне та апаратне забезпечення, біотехнології, аерокосмічну промисловість, телекомунікації, транспорт і технологію двигунів, виробництво автомобілів, верстатів, енергії, матеріалів і покриття.

Головною причиною використання промислового шпигунства є бажання за відносно невеликий проміжок часу та без додаткових витрат наздогнати конкурентів, які займають лідируючі позиції на ринку, чи не дати змогу суперникам, які розробляють новий товар чи перспективну технологію, зробити те ж саме [6].

Інакше кажучи, промисловий шпionaж виступає лише одним зі способів конкурентної боротьби для бізнесу. Тобто коли суб'єктом економічного шпигунства (сторонюю, що здійснює активні дії) виступає держава через спецслужби, то у разі промислового такими є окремі підприємці, фірми (фізичні чи юридичні особи). Промислове шпигунство, як правило, переслідує дві цілі:

1. одержання даних щодо роботи конкурентів, насамперед про стратегічні та тактичні плани;
2. витіснення або знищення суперників, що дасть додаткову конкурентну перевагу на ринку.

Нині у світовому економічному просторі як один із видів промислового шпигунства використовується «гіперконкуренція» – коли різні суб'єкти економічної діяльності (великі компанії, транснаціональні корпорації, держави) використовують різноманітні, часто недобросовісні або нелегальні, методи конкурентної боротьби задля створення у опонентів несприятливих умов чи криз, що дасть змогу захопити більшу частку ринку і збільшити обсяги реалізації товарів чи послуг. Також гіперконкуренція використовується для захоплення та дестабілізації ринків, що можливо зробити за допомогою наступального (агресивного) бенчмаркінгу, порушення авторських прав, переманювання професіоналів у конкурентів, кризових структур, кібератак та ін.

Базисом гіперконкуренції виступають спецструктури компаній, які використовують методи недобросовісної конкуренції у власних інтересах і убезпечують себе від подібних заходів із боку суперників. Ці структури не мають загальноприйнятої назви і позначаються різними термінами. На думку В. Гомольської, найбільш підходящим терміном є «кризові структури» – вони мають справу зі створенням криз у конкурентів, однак намагаються запобігти появі їх у власній компанії, при цьому активно приховуючи цілі своєї роботи та методи щодо їх досягнення [7, с. 50].

Не можна залишити поза увагою й те, що в поле прискіпливої уваги промислового шпигунства досить давно потрапили комп'ютерні системи. Розроблення і розповсюдження програмного забезпечення та технічних засобів, призначених для нелегального проникнення в автоматизовані системи та здатних призвести до спотворення або знищення даних чи носіїв інформації, тягне за собою покарання у вигляді позбавлення волі на строк до двох років або виправних робіт на той самий період чи штрафу у розмірі від ста до двохсот мінімальних розмірів заробітної плати. У разі якщо ці дії завдали шкоди у великих розмірах чи здійснені повторно або за попередньою змовою групою осіб, караються позбавленням волі на строк від двох до п'яти років [8].

Разом із цим промислове шпигунство в Україні здійснюється як прийнятний спосіб ведення бізнесу,

без наявності ефективного чинного законодавства для запобігання цьому. Так, була спроба використовувати кримінальні закони з метою протидії промислового шпигунства, однак останні не охоплюють поняття крадіжки або неправильного збору конфіденційної інформації зокрема. Очевидно, що у сфері бізнесу інформація є більш цінною, ніж будь-коли. Кожне підприємство є вразливим до крадіжки інформації. Близько 85% випадків промислового шпигунства здійснюються співробітниками підприємств, безпека котрих стосується, насамперед, захисту від зовнішніх загроз, незважаючи на витік інформації через внутрішні елементи. У зв'язку із цим керівництво підприємства повинне змінити спосіб формування безпеки у сфері інтелектуальної власності, визначити свої цінні інформаційні ресурси, а також потенційний перелік конкурентів, які зацікавлені в них. Окрім того, необхідним є проведення перевірок фахівців програмного забезпечення, котрі володіють конфіденційною інформацією чи комерційними таємницями. Адже, маючи безпосередній доступ до бази даних, можливим стає підкуп недобросовісних програмістів, занесення «троянів» у корпоративну комп'ютерну систему і тим самим створення можливого шляху для витіку конфіденційної інформації з підприємства. Законодавство, однак, не завжди захищає від протиправних дій, учинених промисловим шпигуном, що підлягає цивільному або кримінальному переслідуванню. Особливості конфіденційної інформації, що є вкраденою, широко оприлюднюються в ході судового процесу, який є наслідком правових норм, із метою досягнення справедливості, у результаті чого підприємство, яке постраждало від протиправного промислового шпигунства, повинне оприлюднити той самий обсяг інформації, який вона

намагається захистити, у результаті чого значення конфіденційної інформації нівелюється.

Одним із чинників, який спричиняє виникнення промислового шпигунства, є незахищеність програмного забезпечення комп'ютерів, а саме використання шкідливих програм як інструменту для шпionажу, що здійснюється з метою передачі цифрових копій комерційних таємниць, клієнтських баз даних, стратегічних планів і контактів. Нові види шкідливих програм таємно фіксують необхідну інформацію на камеру мобільного телефону чи записуючі пристрої. Для попередження таких незаконних нападів на інтелектуальну власність підприємства все частіше зберігають важливу інформацію поза мережею Інтернет, використовують спеціальні електромагнітні пристрої, щоб не допустити передачі даних через мобільний телефон.

Висновки з проведеного дослідження. Для ефективного функціонування вітчизняних підприємств усіх галузей та організаційно-правових форм в умовах випереджаючого розвитку техніки та технологій українським необхідним є процес розроблення стратегії і тактики захисту консолідованої інформації, а особливо комерційної таємниці. Стійкий розвиток підприємства неможливий без ведення успішної конкурентної діяльності, яка, своєю чергою, не відбувається без економічного, виробничого, науково-технічного шпигунства. Варто заздалегідь прорахувати всі переваги та загрози, що криють у собі конкурентна розвідка та промислове шпигунство, і, скориставшись досвідом закордонних компаній, навчитися ефективно застосовувати різноманітні їх прийоми та методи. З метою убезпечення себе від промислового шпигунства підприємствам доцільно посилювати захист своїх інформаційних ресурсів та проводити постійний моніторинг чинників уразливості даних, які підлягають захисту.

Список використаних джерел:

1. Фінансова безпека підприємства : навчальний посібник / Т.Б.Кузенко та ін. Харків : ХНЕУ, 2010. 304 с.
2. Живко З.Б. Рівні економічної безпеки підприємства та визначення інтегрального показника. *Науковий вісник Мукачівського державного університету. Серія «Економіка»*. 2015. Вип. 1. С. 84–90. URL: http://nbuv.gov.ua/UJRN/nvmdue_2015_1_17 (дата звернення: 24.03.2020).
3. Гордон Я. Целевая конкуренция / пер. с англ. С. Жильцова, И. Малковой, Е. Федоровой. Москва : Вершина, 2006. 368 с.
4. Економічна та майнова безпека підприємства та підприємництва. Антирейдерство : монографія / Б.М. Андрушків та ін. ; за заг. ред. Б.М. Андрушківа. Тернопіль : Тернограф, 2008. 424 с.
5. Якубівська Ю.С. Цільові атаки в контексті промислового шпигунства. *Проблеми розвитку внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект*. Донецк : ДонНУ, 2014. Т. 2. С. 368–372.
6. Промышленный шпионаж в конкурентной войне. URL: <http://deflab.ru/blog/komputemii-shpionag/promislennii-shpionag-konkurentnaya-voina.html> (дата звернення: 22.03.2020).
7. Гомольська В. Сучасні методи досягнення міжнародних конкурентних переваг. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення* : мат. IV Всеукраїн. наук.-практ. конф., 18-20 травня 2017 р. / упоряд. А.М. Штангрет ; редкол.: О.І. Копилок та ін. Львів : Укр. акад. друкарства, 2017. С. 48–52.
8. Кримінальний процесуальний кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 21.03.2020).

References:

1. Kuzenko T.B., Martyusheva L.S., Grachov O.V., Lytovchenko O.Yu. (2010) Finansova bezpeka pidpry'emstva [Financial security of the enterprise]. Kharkiv: KhNEU. (in Ukrainian)
2. Zhyvko Z.B. (2015) Rivni ekonomichnoyi bezpeky pidpry'emstva ta vy'znachennya integral'nogo pokazny'ka [Levels of economic security of the enterprise and determination of the integral indicator]. *Naukovy'j visny'k Mukachiv's'kogo derzhavnogo universy'tetu*. Ser.: Ekonomika, vol. 1, pp. 84–90. Available at: http://nbuv.gov.ua/UJRN/nvmdue_2015_1_17 (accessed 24 March 2020).

3. Gordon Ja. (2006) *Celevaja konkurencija* [Target competition]; transl. from engl. S. Zhilcova, I. Malkovoj, E. Fedorovoj. Moscow: Vershina. (in Russian)
4. Andrushkiv B.M., Vovk Y.Ya., Malyuta L.Ya., Palyanytsya V.A. (2008) *Ekonomichna ta majnova bezpeka pidpry'emstva ta pidpry'emny'cztva. Anty'rejderstvo* [Economic and property security of enterprise and entrepreneurship]. Ternopil: Ternograph. (in Ukrainian)
5. Yakubovskaya Yu.E. (2014) *Ciljovi ataky v konteksti promyslovogho shpyghunstva* [Targeted attacks in the context of industrial espionage]. Problems of development of foreign economic relations and attracting foreign investments: regional aspect: coll. scientific tr. Vol. 2. Donetsk: DonNU, pp. 368–372. (in Ukrainian)
6. *Promyshlennyj shpionazh v konkurentnoj vojne* [Industrial espionage in the competitive war]. Available at: <http://deflab.ru/blog/komputemii-shpionag/promislennii-shpionag-konkurentnaya-voina> (accessed 22 March 2020).
7. Gomolska V. (2017) *Suchasni metody dosjaghnennja mizhnarodnykh konkurentnykh perevagh* [Modern methods of achieving international competitive advantages]. Economic security and business entities in Ukraine: problems and ways of their development: Mat. IV All-Ukraine. Research Practice Conf. May 18-20, 2017. Lviv: Ukr.acad. printing, pp. 48–52. (in Ukrainian)
8. *Kryyminalnyj procesualnyj kodeks Ukrayiny* [Criminal Procedure Code of Ukraine] [Electronic resource]. Available at: <https://zakon.rada.gov.ua/laws/show/4651-17> (accessed 21 March 2020).

E-mail: nv220512@gmail.com