МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Кафедра фінансово-економічної безпеки та інтелектуальної власності

Кучер Віталій Сергійович

Промислове шпигунство як загроза економічній безпеці підприємства / Industrial espionage as a threat to economic security of the enterprise

спеціальність: 8.18010014 – Управління фінансово-економічною безпекою
магістерська програма – Управління фінансово-економічною безпекою

Магістерська програма

Виконав студент групи ФЕБм-21
В.С. Кучер
_____

Науковий керівник:
к.е.н., доцент, Ю.Є. Якубівська
_____

Магістерську роботу допущено
до захисту:
«____» _____20___р.
Завідувач кафедри
_____ Н.Б. Москалюк

ТЕРНОПІЛЬ – 2017

ЗМІСТ

«Сучасна наукова, промислова та економічна
інформація більшою частиною легко доступна.
95% даних можна отримати із спеціальних журналів,
звітів компаній, внутрішніх видань підприємства,
брошур і проектів, які роздають на ярмарках і виставках.
Мета шпигуна - роздобути 5% інформації, яка залишилась,
в якій і криється фірмовий «секрет», «таємниця майстерності»
(Французький дослідник промислового шпигунства М. Денюзьєр).

ВСТУП

Актуальність теми дослідження. Причиноюнепорозуміння між визначеннями понять «промислове шпигунство» і «бізнес-розвідка» або «економічна розвідка» є неправильне тлумачення власне терміну «промислове шпигунство». Вважається, що такого роду діяльність завжди повинна бути пов'язана з промисловістю або ж виробництвом. А так як більшість сучасних видів бізнес-діяльності включають перепродаж товарів та надання послуг, то на перший погляд здається, що проблемиз шпигунством у таких підприємств немає. Даний аспект визначає актуальність теми дослідження. Забезпечення успішного підприємництва, розвиток вільної конкуренції, створення безпечного середовища для розвиткубізнесу сприяють активному залученнюрозвідувальної активності, апромислове шпигунство розглядається як діяльність, спрямована на тактичне або стратегічне отримання переваги над конкурентом, ідентифікація та управління ризиками.

Актуальність теми дослідження полягає у відсутності чіткої та злагодженої системи заходів для вчасного виявлення, запобігання протидії та боротьби з промисловим шпигунством на підприємствах України. Промислове шпигунство передбачає нелегальні методи й технології і полягає передусім в оперативній діяльності, зокрема в незаконному проникненні на простір конкурента, шантажі, знятті інформації з каналів зв'язку, підкупі, стеженні, викраденні інформації тощо.

Таким чином, проведення дослідження щодо основних схем та засобів протидії промисловому шпигунству на сьогодні є актуальним та необхідним.

Основною метою написання магістерської роботи є загальнотеоретичний аналіз тенденцій розвитку та удосконалення системи протидії промисловому шпигунству на підприємствах України, а також дослідження системи права у сфері адміністративно-правового забезпечення безпеки суб'єктів господарювання в контексті запобігання промисловому шпигунству.

Для досягнення цієї мети запропоновано розглянути наступні **завдання:**

– охарактеризувати термінологічні аспекти категорії «промислове шпигунство» в контексті його відмінності від економічної розвідки;

–здійснити аналіз правопорушень та,відповідно, методи протидії та боротьби з проявами промислового шпигунства в на міжнародному та національному рівнях;

- дослідити класифікацію видів промислового шпигунства;

- проаналізувати нормативно-правові відносини у сфері протидії промисловому шпигунству на міжнародному та національному рівнях;

- визначити перспективи розвитку системи протидії та боротьби з промисловим шпигунством в Україні;

- запропонувати рекомендації щодо українського законодавства та його правозастосування в сфері протидії та боротьби проти проявів промислового шпигунства на підприємствах України;

- сформувати систему організаційних заходів протидії промисловому шпигунству на підприємстві.

Об'єктом дослідження є феномен промислового шпигунства як загроза економічній безпеці підприємства.

Предметом дослідження є система запобігання і боротьби з промисловим шпигунством на підприємствах України.

Методи дослідження. Методи дослідження, що були використані при написанні магістерської роботи:

- абстрагування (при дослідження категорій «промислове шпигунство» та «комерційна таємниця» в контексті національних та закордонних термінологічних аспектів);

- припущення (в процесі формування удосконаленої системи боротьби з промисловим шпигунством в Україні);

- системний підхід (для відображення характерних рис та протиріч існуючих нормативно-правових норм у сфері боротьби та протидії промисловому шпигунству в Україні);

- аналізу і синтезу (при здійсненні аналізу правопорушень та дослідження нормативно-правових відносин у сфері протидії промисловому шпигунству).

Теоретична й методологічна основа дослідження. В основу написання цієї магістерської роботи покладено результати дослідницької роботи таких вітчизняних і зарубіжних учених, як Аширлієва Ш. [1], Жаліло Я. [14], Мошак Г. [26], Ткачук Т. [46-48], Тимчук Д. [45], Чечерскі М. [70], Франчук В. [55], Якубівська Ю. [59-63] та інших.

Як і решта держав, Україна, без урахування зарубіжного досвіду, практики діяльності суб'єктів недержавної правоохорони не в змозі вирішити власні економічні проблеми щодо впливу глобальних факторів, викликів і загроз безпеці діяльності суб'єктів господарювання.

У [1; 14; 70; 59-63] систематизовано міжнародний і вітчизняний досвід забезпечення безпеки та захисту бізнесу. Описано використані на практиці методи і способи ведення розвідки і контррозвідки, приділено увагу шпигунству, технічним засобам отримання та збереження конфіденційної інформації.

У [46-48] узагальнено міжнародний та вітчизняний досвід використання спецслужб у сучасних умовах. Описана їх структура на рівні держави та підприємства, а також робота по припиненню розвідувальної діяльності та промислового шпигунства недобросовісних конкурентів, шахраїв, кримінальних елементів.

У [45; 55] описуються, як використовувати конкурентну розвідку під час ведення бізнесу підприємству, просування продукту та відслідковування змін в конкурентному середовищі. Вказано, які існують методи збору інформації, як і де їх використовувати.

У наведених наукових працях та інших публікаціях підіймається питання конкурентної розвідки та промислового шпигунства. Проте, науковцями, які працювали в сфері конкурентної розвідки та промислового шпигунства, так і не було виділено чіткої межі між конкурентною розвідкою та промисловим шпигунством.

Концепція промислового шпигунства в контексті корпоративної безпеки є складною і багаторівневою системою загроз, містить взаємопов'язані і взаємозалежні характеристики кожного індивіда. Це характеризується в першу чергу недотримання законів і правил, у той час як для економічної розвідки не є характерним порушенням чинного законодавства.

Інформаційною базою дослідження є національне та іноземне законодавство, матеріали звітів Європейського центрального банку, Єврокомісії, дані сайту Контррозвідувального бюро («AGG»), світової бізнес організації «BASCAP «, організацій та установ, публікації провідних науковців у сфері економічної безпеки, розвідувальної діяльності.

Основні результати дослідження, що характеризують його новизну, розкривають зміст магістерської роботи, полягають в тому, що: запропоновано шляхи удосконалення системи боротьби з промисловим шпигунством на підприємствах України.

Практичне значення одержаних результатів. Сформульовані в роботі теоретичні положення та практичні рекомендації можуть бути використані в процесі здійснення активної боротьби та протидії економічному та промисловому шпигунствуна підприємствах України, при прийнятті і реалізації відповідних організаційно-управлінських рішень у контексті забезпечення економічної безпеки підприємства.

Апробація та публікація результатів дослідження. Основні положення та висновки дослідження висвітлювалися у доповіді на тему: «Виробництво контрафактної продукції як результат промислового шпигунства» та були опубліковані у збірнику «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави».

Зв'язок роботи з науковими програмами, планами, темами. Магістерська робота виконана у відповідності до тематики магістерських робіт кафедри фінансово-економічної безпеки та інтелектуальної власності Юридичного факультету Тернопільського національного економічного університету.

Структура та обсяг магістерської роботи. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел зі 93 найменувань на 10 сторінках, 1 додатку. Основний текст викладений на 108 сторінках.

РОЗДІЛ І
ПРОМИСЛОВЕ ШПИГУНСТВО ЯК РІЗНОВИД ЕКОНОМІЧНОЇ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ

1.1. Поняття промислового шпигунства в контексті розвідувальної діяльності

Розвідувальна діяльність (шпигунство) - явище настільки ж давнє, як і сама наша цивілізація. Розвідка виникла у доісторичні часи, розвинулася із зародженням торгівлі та ремесел. Як тільки нововведення розпочинали приносити вигоду їх власникам, вони тут же старалися їх засекретити. Ті ж, хто втрачав на незнанні, намагалися опанувати цими таємницями за будь-яку ціну. Потужний поштовх розвитку економічної розвідки дав поділ праці і виникнення торгівлі і грошей.

Батьківщиною перших теоретиків розвідки вважається Китай, там вже в IV ст. до н.е. появилася перша фундаментальна праця про це ремесло. Це була книга «Мистецтво війни» китайського філософа Сунь Цзи: «Якщо освічений государ або розважливий генерал здобувають перемогу над противниками кожен раз, коли ті переходять до дій, то це досягається завдяки попередній інформації. Так звана попередня інформація не може бути отримана ні від духів, ні від божеств, ні за аналогією з минулими подіями, ні шляхом розрахунків. Її необхідно отримати від людини, яка знайома з ситуацією противника» [85, с. 14].

Зародком конкурентної розвідки, що набирала силу з розвитком ремесел і торгівлі, було приватне шпигунство. Ще на початку розвитку цивілізації афінські, єгипетські торговці і родоські купці виконували збір таємної інформації, наявність якої могла б сприяти комерційному успіху. Проте така розвідка носила епізодичний характер і чинилася самими торговцями або їх посередниками. Купці намагалися довідатися, який товар, якої якості, в якій кількості привезли на даний ринок конкуренти, за якою ціною будуть

продавати. Зрозуміло, по можливості, вони не упускали випадку зіпсувати товар конкурентів, пустити слух про його неохайність, про його уявні і дійсні вади, оббрехати, а також відзначити непомірно високі ціни при неприпустимій якості товарів. Пізніше всі ці прийоми отримали наукоподібні назви - імідж, дифамація, кон'юнктурний аналіз, реклама тощо.

Перша справжня приватна розвідслужба була створена флорентійськими купцями-банкірами в XIV ст. Потім таку розвід службу створили Фуггери з Аусбурга, які в XV і XVI ст. входили до числа найбільших промисловців.

Високою ефективністю своєї розвідслужби прославилися Ротшильди. Наприкінці XVIII ст. п'ять братів заснували банки в п'яти європейських столицях (Відні, Парижі, Лондоні, Франкфурті та Неаполі). Під час війни з Наполеоном, вони навербували більше 200 агентів і надали всі свої розвіддані, а також здібності і можливості з міждержавним переведенням капіталів у розпорядження Англії. Усі витрати вони з лишком покрили за допомогою спритної біржової афери. Завдяки своїм інформаторам Натан Ротшильд першим дізнався про поразку Наполеона. Він негайно приступив до масового продажу своїх акцій. Всі інші біржовики відразу ж наслідували його приклад, так як вирішили, що бій програли англійці. Коли ціни впали до гранично низького рівня, Ротшильд все скупив[85, с.15].

Англійці першими розширили діяльність своїх секретних служб на область економіки. Головною ставкою у грі послужила текстильна промисловість. Завдяки технічній перевазі Великобританія забезпечувала собі в області текстилю практично монопольне становище. Однак наприкінці XVIII ст. представники південних штатів Америки не пошкодували фінансових коштів на організацію промислового шпигунства на англійських фабриках в Ланкаширі, в результаті чого їм вдалося отримати креслення прядильної машини.

Засновник «Apple» Стівен Джобс був здивований, коли дізнався, що його комп'ютери вже випускають на Тайвані. У 1980 р. в світі промислового шпигунства запалилися «нові зірки» - фірми з Тайваню, Гонконгу і Південної

Кореї крали все, що тільки можна було вкрасти. Зокрема, компанія «Apple» була змушена постійно судитися з тайванськими фірмами, які буквально копіювали їх комп'ютери[87].

Фірма «Multitec», наприклад, випускала оновлені версії свого комп'ютера після кожної нової версії комп'ютера «Apple». При цьому вироби тайванських майстрів в деталях копіювали вироби американців. Ще далі пішла тайбейська фірма «GuanHaurIndustrial», яка скопіювала не тільки сам комп'ютер, але навіть керівництво користувача, написане засновником «Apple» Стівеном Возняком. Нарешті, компанія «SunriseComputerService», що базувалася в тому ж Тайбеї, не посоромилася запозичити у «Apple» навіть назву. Свій комп'ютер «Sunrise» назвала «Apolo», що в китайській транскрипції звучить точно так само, як «Apple». При цьому тайванські копії коштували близько 500 дол. США. У той час як персональні комп'ютери від «Apple» коштували трохи менше 1,5 тис. дол.. США. [81] Тому споживачі, як завжди, тільки вигравали від діяльності економічних розвідників. Методи роботи далекосхідних шпигунів у той же час залишалися цілком традиційними: вивчення готової продукції конкурента, збір відкритої інформації, підкуп його співробітників та інше.

На сучасному етапі розвитку конкурентних відносин все більшого поширення набуває саме промислове шпигунство, як метод недобросовісної конкуренції - це служба, що забезпечує керівництво підприємства (під підприємством тут розуміється будь-яка організація, від підприємницької структури до держави або міжнаціональної корпорації включно) інформацією, необхідною для превентивного прийняття рішень. Це не тільки збір інформації, але й її класифікація (по значущості, ступеню достовірності і т.д.), аналіз, прогнозування розвитку ситуації, підготовка рекомендацій керівництву.

Служба конкурентної розвідки (яка керує водночас і промисловим шпигунством на підприємстві) може складатися з одного штатного співробітника (а то і менше, коли ці обов'язки покладено на кого-небудь з керівництва за сумісництвом), а може і бути великим і розгалуженим підрозділом, все залежить від масштабу підприємства. При цьому реально в

процес промислового шпигунства втягується безліч співробітників підприємства, що не мають прямого адміністративної зв'язку з цим підрозділом.

Розрізняють два види роботи розвідувальної служби: стратегічна розвідувальна служба і оперативна розвідувальна служба. Завдання стратегічної розвідувальної служби за змістом близькі завданням стратегічного планування та маркетингу і зводяться до прояснення структури і динаміки того поля господарсько-економічної діяльності, на якому працює (або збирається працювати) підприємство, з виявленням і аналізом усіх конкурентів і контрагентів на цьому полі.

Оперативна розвідувальна служба вирішує гострі завдання негативного взаємодії з конкретним конкурентом і частенько діє на межі етично і юридично неприйнятних норм і засобів (на відміну від конкурентної розвідки, яка працює в межах легітимних методів).

Предметом інтересу стратегічної розвідувальної служби найчастіше є:
1. Нормативно-правова база (та її частина, що регламентує процеси та обставини, пов'язані з діяльністю підприємства);
2. Конкуренти (потенційні і справжні);
3. Ринки (потенційно можливі та існуючі);
4. Нові технології та права на об’єкти інтелектуальної власності;
5. Ресурси (при намірі підприємства розширити збутові або виробничі можливості);
6. Тренди зміни всіх перерахованих вище об'єктів.

Предмети інтересу оперативної розвідувальної служби - істотно інші:
1. Історія фірми-конкурента;
2. Інформація про її керівні кадри;
3. Організаційна структура фірми-конкурента, особливості організації її виробництва;
4. Маркетинговий стиль, стратегія конкурента;
5. Дослідно-конструкторські роботи фірми-конкурента, її перспективні плани;
6. Лобіювання, зв'язки з владними структурами;

7. Кадрова політика фірми-конкурента.

При цьому, оскільки мова йде про цільові функції формування ускладнень або перешкод конкуренту, то всі ці завдання ставляться з явним акцентом на пошук слабких місць. Промислове шпигунство - це здобуттянезаконним методом конфіденційних даних про діяльність конкурентів, розкрадання даних, наприклад, про складову ноу-хау, провадження недобросовісної конкуренції, отримання персональних даних дляподальшого їх застосування в злочинних цілях.

Новітнє промислове шпигунство - це водночас й умисне приведення в непридатність інформаційних систем, виробничого устаткування, здійснення психологічного тиску на працівників підприємства з метою дестабілізації роботи конкурента.

Є три основні фактори: споживачі, конкуренти і зміни ринкових умов. Таким чином, промислове шпигунство, а також конкурентна розвідка, є формою бізнес-аналітики, яка означає не тільки створення баз даних конкурентів, їх переваги і недоліки, але також і прогнозування конкурентоспроможності їх продукції та продуктів і послуг конкурентів; очікування можливих економічних криз на фінансових ринках; визначення шляхів їх усунення; рекомендації щодо вирішення проблеми конкретного сегменту ринку; захист стабільності та економічної безпеки підприємства; розробка стратегічних планів для прийняття управлінських рішень. Основні параметри кожногопідприємства є наступними:

– ідея бізнес-моделі - те, що потрібно зробити, щоб отримати прибуток;

– процес - пряме виробництво чи інший вид діяльності для отримання прибутку через правильну організацію бізнес-процесів;

– ефективне управління ризиками - визначення шляхів і методів для забезпечення рентабельності бізнес-процесів або зменшення їх до мінімального рівня.

Суть концепції «ідеї» в контексті промислового шпигунства полягає у тому, щоб максимізувати фінансові доходи від існуючих засобів.Бізнес-ідея може

самостійно формуватися за умови, що вона має під собою достатні ресурси і час для власноїреалізації в бізнесі, і може створюватися шляхом копіювання, крадіжки і т.д., заощаджуючи час і гроші. Ідея, яку можна купити, зібрати її складові частини, скопіювати або банально викрасти.

«Процес» - це бізнес-модель, яка дозволяє функціонувати на рівних з бізнес-партнерами, які отримують набагато більш прибуток. Західні компанії давно використовуються поняття, такі як «бенчмаркінг», який визначається як вивчення досвіду, стратегії, рішення, кращої бізнес-практики в галузі, щоб використовувати форми, адаптовані для поліпшення якості своєї компанії.Дане поняття включає в себе збір інформації про стандарти і інші ключові бізнес-показники (критерії) та їх відтворення в їхніх компаніях. При перекладі з англійської мови, дане поняття означає опорну точку геодезичної висоти - постійний орієнтир, еталон, який призначений для визначення висоту і ширину. Бенчмаркінг - порівняння ефективності встановлених критеріїв, прийнята система цінностей. На Заході, термін «бенчмаркінг» почав використовуватися в кінці 1970-х років. У Сполучених Штатах, Японії та інших країнах бенчмаркінг розвиває в контексті державної підтримки; в цьому напрямку також маломісце і промислове шпигунство, мета якого полягає в пошуку партнерів для порівняльного аналізу[83, с. 272].

Таким чином, бенчмаркінг - система методів і способів вивчення позитивного досвіду партнерів і конкурентів, розробка взаємопов'язаних шляхів забезпечення ефективності та рентабельності системи показників, дослідження досягнення кожного з них окремо і всіх разом, індивідуальний прибуток від показників, основні цілі поширення і впровадження в власний бізнес складних бізнес-рішень. Сьогодні бізнес-аналітики є частиною корпоративної культури сучасного бізнесу.Для виживання бізнесу в умовах конкуренції відіграють першорядну роль розвідки намірів конкурентів, розвиток бізнес-напрямків, аналіз можливості ризику. Захід досліджує ці аспекти бізнесу, а промислове шпигунство і конкурентна розвідка настільки широко поширені, що ці процеси стають само собою зрозумілими. На жаль, в Україні концепція бізнес-аналітики

та промислового шпигунства, вважаються недобросовісними практиками, і термін «розвідувальна діяльність» застосовується з обережністю, через відсутність розуміння процесів пошуку інформації, то він інтерпретується як промислове шпигунство.

Промислове шпигунство виникає, коли присутня слабкість розвідувальної діяльності. На практиці, бувають ситуації, коли правові межі не співпадають з етичними. Так, виникає питання, чи маємо ми справу з некомпетентною розвідувальною діяльністюабо з проявами промислового шпигунства. Шпигунство включає передачу, викрадення або збирання інформації, що містять дані державних і військових секретів, відтак, щоб мати справу з промисловим шпигунством,протидією повиннізайматися органи, уповноважені державою.

Оцінка ефективності процедур забезпечення безпеки в контексті запобігання створенню шпигунської діяльності складається з наступних кроків:

1. Визначення внутрішніх і зовнішніх загроз.
2. Визначення слабких сторінпідприємства.
3. Перевірка точності класифікації загроз на об'єкті.
4. Показання заходів щодо нейтралізації загроз.
5. Перевірка ефективності заходів щодо нейтралізації загроз [6, с. 79].

Проте, нерідко матеріали справи, торгові секрети якимось чином потрапляють на перші сторінки газет, брошур. Якщо для деяких компаній, ця інформація не важлива, то для когось стає цінною знахідкою. Є ситуації, в яких підприємство прагне отримати необхідні дані шляхом корумпованих комп'ютерних систем, ігноруючи етичні норми, щоб вкрасти або купити цінну інформацію.

Таким чином, визначити межі промислового шпигунства, об’єктом якого є секрети та результати нового дослідження, технології, ноу-хау конкурентів, використання дешевих матеріалів і фінансових ресурсів, дуже складно. Концепція промислового шпигунства схематично показано на рис. 1.1. в якості моделі взаємопов'язаних заходів:

Рис. 1.1. Процес використання конфіденційної інформації в контекстіпромислового шпигунства
Джерело: Складено автором

Якщо яка-небудь частина комбінованого ланцюга зникає чи нівелюється, промислове шпигунство не досягне своєї мети. Сучаснепромислове шпигунство - це умисне пошкодження промислового обладнання, інформаційних систем, психологічний тиск, що призводить до впливу на працівників у контексті дестабілізації конкурентів. У сучасній економіці, це спроба деяких підприємств стати абсолютним монополістом у місті чи регіоні. Там застосовуютьсяхабарництво, погрози, шантаж співробітників, коучинг кваліфікованих фахівців з конкурентів, крадіжки баз даних і опису процесу. Вивчення гострих проблем вітчизняної економіки показують, що причиною більшості з них є: халатність керівників компанії і державних чиновників в контексті створення та захисту конкурентного середовища, та активна діяльність конкурентних розвідувальних організацій, що може призвести не тільки до значних фінансових витрат, але йдо банкрутства або втрати бізнесу.

Тим не менш, незважаючи на минулий досвід конкурентної політики в контексті розвинених країн, Україна, наприклад, не вчиться на помилках інших,

і допускає серйозні помилки в галузі безпеки. Прикладом цього є той факт, що існує змова між виробниками нафти, чиї позиції на ринку ґрунтуються на власності 90% внутрішнього ринку для російської кампанії, що призвело до монополізації цього стратегічно важливого ринку.

Таким чином, розвідувальна діяльність - це об'єктивний процес. Відносини в комплексі розвідувальної діяльностіпогано визначені в будь-якому способі отримання інформації про конкурента, а відтак, вона безпосередньо пов'язана зі зброєю, яка може бути використана проти конкретної компанії. Розвідувальна діяльність є соціально корисним явищем, оскільки вона допомагає компаніям розвиватися, як внутрішньо, так і на зарубіжних ринках, удосконалюватися, диверсифікуватися. Тим не менш, в найближчому майбутньому, коли компанія стає більш професійною, конкурентоспроможною і цивілізованою, розвідувальна діяльність розглядається як необхідна умова для забезпечення стратегічної стабільності, конкурентоспроможності та економічного захисту підприємства. На макрорівні, всі країни проводять економічну розвідку: це питання національної безпеки і міжнародного права. У той же час державні розвідувальні структури все частіше працюють в інтересах приватних корпорацій. Що стосується макрорівня, в цьому питанні ми маємо справу з правим конкурентним захистом економічної конкуренції, захистом та охороною авторського права і суміжних законів, обмеженням монополізму, порушенням комерційної таємниці тощо.

На практиці, промислове шпигунство вже давно використовується у конкуренції, не призводячи до контактів з об'єктами. Використовуючи наночіпи, які встановлені в аудіо або відео пристрої, можна отримати найбільш повну інформацію. Деякі з цих пристроїв можуть передавати інформацію на відстані 1000 км і більше. Нещодавно розширено технікурозвідувальної діяльності та промислового шпигунства з використання лазерного випромінювання. У ході слухань у Конгресі США в травні 2002 року представники органів, уповноважених на боротьбу з промисловим шпигунством оголосили список з 23 країн, де ця діяльність здійснюється

спецслужбами. У цьому списку були Ізраїль, Англія, Німеччина, Франція, Росія та інші. Американське товариство промислової безпеки щороку показує все більше число великих американських корпорацій, для яких були здійснені акти промислового шпигунства. Найбільш привабливими є секрети «IBM» (комп'ютери), «Honeywell» (обладнання літаків), «Istman–Kodak» (фотоапаратура, в тому числі в контексті авіації), «АТТ» (з'єднання), «GeneralElectri»с (електротехнічне обладнання)[86].

На теперішньому етапі розвитку суспільства об'єми економічного шпигунства різко ростуть. Інформація про результати чужих фундаментальних і прикладних досліджень дозволяє зекономити власні кошти й сили і зосередити усю увагу на маркетингу та виробництві. Дальший розвиток науково-технічного прогресу, зростання потоку патентів і жорсткість конкуренції як «війни всіх проти всіх» роблять викрадення чужих секретіввинятково прибутковою, а відтак, дуже перспективною справою. На жаль, більшість підприємств не надто розважливо ставиться до загрози з боку конкурентів і спецслужб «дружніх»держав. Керівництво цих підприємств найчастіше ігнорує перспективупромислового шпигунства й не цікавиться методами негласного збору інформації. Безпека сприймається суб'єктом витрат і не розглядається як об'єкт вкладень. Коли ж проблема таки постає, її стараються вирішити з мінімальними втратами.

Термін «промислове шпигунство»уперше був сформульований на початку 60-х років на семінарі з методики збору інформації для керівного складу підприємства «ManadgementInvestigationServices»[80, с.129]. Успішно здійснені акти промислового шпигунства дають істотні переваги над конкурентами, котримподекуди доводиться затрачувати великі кошти на подолання результатів таких дій. Промислове шпигунство відносно бізнесу — це різновидність економічного шпигунства, котрому властиве звуження масштабів завдань з отримання інформації, що інтересує, від державного масштабу до масштабу однієї або декількох підприємств-конкурентів.

Промислові шпигуни, зазвичай використовують старі методи збору інформації. Клієнт у звичному шпигунстві – це держава, а в промисловому – конкурент. Клієнт формулює потреби в інформації, установлюєстроки вирішення завдань і підрозділяє фінансові ресурси. Така тенденція розвитку промислового шпигунства дуже впливає на маркетингове середовище підприємства, що пов’язано із помітними збитками для підприємства, яке понесло фінансові утрати на маркетингове дослідження,котре проводила фірма. За оцінкою незалежних західних експертів, у більше ніж 80% випадків результати розвідувальної діяльності застосовуються для економічного (промислового) шпигунства, тому відділ маркетингу самий уразливий на підприємствах, його потрібно захищати різноманітними методами захисту, котрі існують на теперішній день.

Об'єктами агентурногоопрацювання можуть бути не лише «другі» або «треті особи» фірми-конкурента, але й будь-які службовці, навіть нижчої ланки. Вони цілком здатнівиконати приховане встановлення відповідної апаратури (так званих «комарів», «жучків» тощо). Для цього треба від декількох секунд до двох-пяти хвилин. Так, зокрема Німецькі підприємства втрачають близько 20 млрд. євро щороку через промислове шпигунство. Щорічні втрати німецьких підприємств від промислового шпигунства, складають, щонайменше, 20 мільярдів євро, повідомляє «Deutschlandradio» з посиланням на голову Комітету з економічної безпеки Б.Штоппелькампа (BertholdStoppelkamp)[88].

Найчастіше об'єктом промислового шпигунства є дослідження у галузі екологічно чистих технологій, особливо розроблювання високоємких акумуляторів і електроприводів. Задіяні в даних дослідженнях вчені, менеджери й інженери змушені приділяти підвищену увагу боротьбі з інсайдерськими витоками інформації. Точна кількість шпигунських атак, котрим піддаються німецькі підприємства, залишається невідомим. За даними статистики, зі ста випадків промислового шпигунства стає загальновідомо лише про шість. Лі Чанг вважає, що в більшості випадків важливі дані пропадають абсолютно непомітно [82, с.2-3]. Крім того, за його словами, більшість

підприємств не повідомляє про ті інцидентипромислового шпигунства, що стали відомими, щоб не підніматидодаткового галасу. У багатьох німецьких підприємств не вистачає спеціально навченого персоналу і ресурсів для протидії промисловому шпигунству. Найбільше це торкаєтьсясередніх і малих підприємств. Більше половини німецьких підприємств припускають, що однією з головних небезпек для своїх «ноу-хау»є соціальні мережі.

Провідні німецькі підприємства почали масово блокувати своїм службовцям доступ до «Facebook» та інших соціальних мереж, щоб завадити витоку закритої інформації. Зподібними проблемами зіштовхуються й британські компанії. Відповідно до заяви, розміщеної на сайті британської контррозвідки «MI5», промислове шпигунство є однією з трьох першочергових сучасних загроз британської безпеки. «Тепер набагато більше, ніж у минулому, розвідслужби направляють зусилля на комерційні підприємства, — говориться в офіційній заяві «MI5». — Принаймні 20 іноземних розвід служб у якоюсь мірою діють проти інтересів Великобританії» [83, с.290]. На прикладі даних європейських країн ми можемо сказати лише одне: розвитку промислового шпигунства ніщо не заважає, навіть високий розвиток країни. Тому підприємства всіх держав борються з шпигунством як на державному, так і на підприємницькому рівні.

Отож, можна зробити висновок, що наведені приклади промислового шпигунства не можуть не викликати тривоги. Його основоположною причиною служить великий вплив, який промислове шпигунство може реалізувати на економічну міць держави у модерному світі. Як уряди, так і окремі підприємства прагнуть не відстати від інших, або заволодіти їх таємницями виробництва. У наші дні промислове шпигунство є складовою боротьби за вплив, тому шпигунство в широких масштабах — невідворотне, тому як підприємствам, так і країнам треба посилювати захист своїх даних від шпигунів.Якщо звернутись до американського досвіду, то в 1990 р. президент США Дж. Буш у своїй доповіді «Стратегія США в галузі національної безпеки» проголосив пріоритетним напрямком у роботі американських спецслужб

економічну розвідку. У 1993 р. Б. Клінтон дав настанову керівництву розвідувального співтовариства США про поглиблення досліджувань у галузі економічної розвідки. Було акцентованона трьох пріоритетних напрямках[84, с.220]:

- макроекономічна розвідка – збирання стратегічної інформації про глобальні процеси в економіках інших держав;

- мікроекономічна розвідка – збирання оперативної й тактичної інформації про роботу окремих підприємств;

- економічна контррозвідка – протидія спробам іноземних державних спецслужб і комерційних підприємств завоюватитехнологічні й торгово-економічні секрети.

Довідники окреслюють промислове шпигунство як вид недобросовісної конкуренції, практика із незаконного добування відомостей, що становлять комерційну цінність. Потрібно одразу відділити поняття розвідки і промислового шпигунства. Метою обох є одержання інформації, яка б дала здатність здобути конкурентну перевагу на ринку.

Головною відмінністю між промисловим шпигунством та конкурентною розвідкою є способи й методи отримання інформації. Все, що використовується розвідником, є законним (тобто дотримуються етичні норми). Характерні ознаки промислового шпигунства наведено Додатку А. Промислове шпигунство, навпаки, передбачає нелегальні технології й методи. Служба конкурентної розвідки використовує тільки відкриті джерела, оскільки робота розвідника — інформаційно-аналітична, тобто збір й обробка різних даних, що впливають на розвитокбізнесу.

Промислове шпигунство полягає в першу чергу в оперативній роботі, зокрема в незаконному проникненні на територію конкурента, знятті інформації з каналів зв'язку, шантажі, підкупі, стеженні, викраденні інформації тощо.

1.2. Методи промислового шпигунства та його відмінність від економічної розвідки

Існує широкий спектр термінів, що визначають такі поняття, як: конкурентна розвідка, промислове шпигунство, маркетингова розвідка, українськими економістами використовується також англійське слово «бенчмаркінг».

Шпигунство передбачає передачу, викрадення або збирання з метою передачі конкурентам, відомостей, що становлять державну, комерційну або військову таємницю, тому промисловим шпигунством повинні займатися відповідні органи, уповноважені на це державою.

Промислове шпигунство або іншими словами розвідка – це професіональна діяльність з метою отримання інформації, яка надає одержувачеві суттєві переваги в економіці, політиці та інших сферах функціонування. Розглянемо детальніше зазначені категорії[1].

Конкурентна розвідка — це сталий процес збирання, структурування, накопичення, аналізу даних про зовнішнє й внутрішнє середовище підприємства та надання вищому менеджменту інформації, котра дозволяє йому окреслювати зміни в ситуації і приймати вчасні оптимальні рішення щодо керівництва ризиками, запровадження змін на підприємстві, а також відповідні заходи, скеровані на збільшення вартості підприємства та задоволення майбутніх запитів споживачів[27, с.17].

Маркетингова розвідка - поняття дуже широке, слово «маркетинг» має на увазі не тільки вивчення конкурентів, але і просування продукту, ціноутворення, рекламу, починаючи з початкової стадії існування продукту до його продажу[27, с.18].

«Бенчмаркінг» (benchmarking) в перекладі з англійської мови має на увазі порівняння ефективності системи, числа, з якимось встановленим, прийнятим значенням. Конкурентна розвідка - це вузьке спрямування, яке повинно відповідати основній меті - побудові системи боротьби з конкурентами, тобто

створення комплексу заходів щодо отримання і обробки даних про конкурента: майнових, фінансових та управлінських ресурсів, можливостей і уразливості, а також інформації про тактичні і стратегічні плани[1].

Вважається, що, коли конкурентна розвідка є реальним і повним розвідуванням інформації, збір даних про науково-дослідну діяльність здійснюється для того, щоб забезпечити плавний розвиток і процвітання підприємства, промислове шпигунство, яке також застосовуються щодо підприємницького сектору безпеки, є концепцією набагато ширшою. Воно спрямоване на розвиток нових технологій, нових знань, управлінських рішень, досягнення значних переваг, а також вирішення проблем поліпшення фінансових показників, максимізації прибутку з мінімальними витратами і розробки стратегічних планів розвитку підприємства.

Жаліло Д. [14, с. 266] підкреслює, що конкурентна розвідка - це вузька лінія промислового шпигунства, яка відповідає основній меті, а саме: побудові системи взаємовідносин з конкурентами, які розробляють систему стратегії для прийому та обробки інформації на конкурента: нерухомість, фінансові ресурси та управління, можливості і слабкі сторони, а також стратегічні та оперативні плани.

Конкурентна розвідка - це аналітичний процес, який обробляє розрізнені бізнес-дані (виробництво, маркетинг, торгівля та послуги) в чітку і корисну інформацію про фінансову та інші сторони розвитку підприємства: бізнес конкурентів;міжнародні корпорації; партнерів підприємства; іноземних корпорацій; використання можливостей і стратегічні плани.

У даному підрозділі ми детальніше розглянемо методи конкурентної розвідки та промислового шпигунства, що дозволить дослідити ключові їхні відмінності. На рис. 1.2. зображено методи конкурентної розвідки:

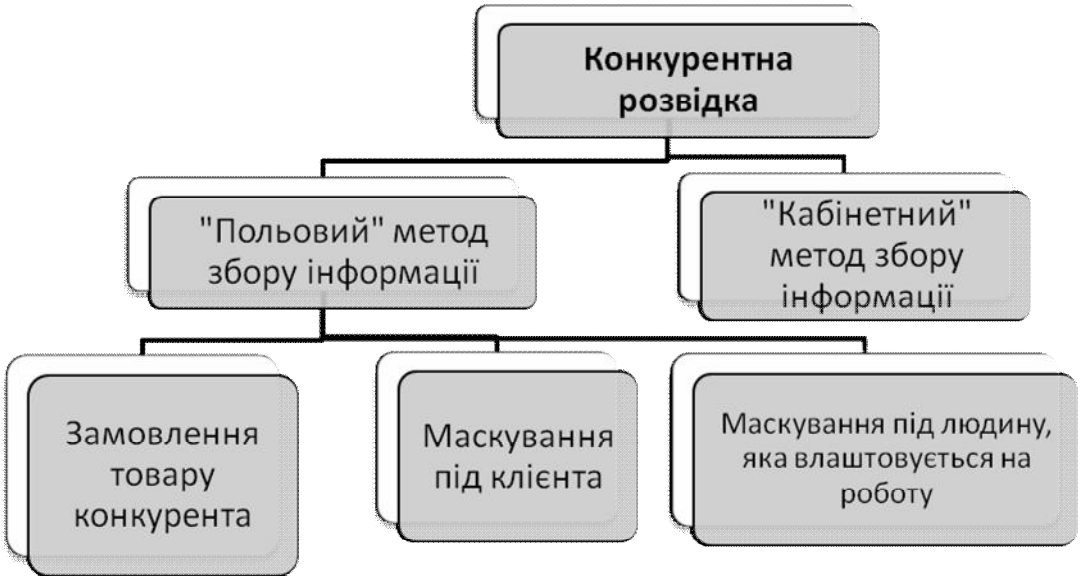

Рис. 1.2. Методи конкурентної розвідки
Джерело: Складено автором на основі [50]

Сьогодні успішне проведення розвідувальної дільності в дуже високій мірі залежить саме від конкурентної розвідки, оскільки своєчасне отримання достовірної інформації про конкурента і його діяльність є ключем до успіху в бізнесі. Тим не менш, межа між маркетингом та аналізом даних за методикою промислового шпигунства така непомітна, що це проблематично визначити. Промислове шпигунство - це незаконна діяльність з метою придбання конфіденційних даних про діяльність конкурентів, крадіжки інформації, ноу-хау, недобросовісної конкуренції, отримання персональних даних для їх використання в контексті злочинної діяльності.

Завдання конкурентної розвідки зводяться до того, щоб визначити, як йдуть справи у конкурентів: як проходять продажі, які досягнення в просуванні на ринок, за рахунок чого удається оптимізувати виробничий процес, збільшити дохід. Що ж до методів конкурентної розвідки (рис.1.2.), то тут всі законні способи ефективні. Але можна розділити на найбільш загальні: «польовий» (з виходом на конкурентну територію) і «кабінетний» (не виходячи з офісу).

1. «Кабінетний» метод збору інформації. Аналітики використовують дані з офіційних джерел (аналітичних звітів, державної статистики, ЗМІ, прогнозів і коментарів спеціалістів, річних звітів конкурентів, їх офіційних сайтів тощо).

2. «Польовий» метод збору інформації:

- замовлення товару конкурента. Цей метод дає максимально інформації про рівень обслуговування, якість самого конкуруючого товару, можливості і вартість доставки. Дізнавшись слабкі і сильні сторони конкурента, підприємству легко підтягти свої показники або переманити клієнтів, наприклад, запропонувавши безоплатну доставку.

- маскування під клієнта. Найчастіше використовується підприємствами, які працюють у галузі роздрібних продажів або послуг. Представник компанії приходить до прямого конкурента під виглядом клієнта з вулиці, ретельно оглядає, оцінює рівень цін і якість обслуговування. Якщо потрібно більше інформації, наприклад, про менеджмент, можна зобразити сварливого клієнта, котрий прийшов скаржитися на якість, і, неодмінно, повинен потрапити до вищого керівництва.

- маскування під особу, котра прийшла на співбесіду або хоче влаштуватись на роботу. Під виглядом кандидата можна дізнатися про систему роботи на підприємстві, рівні зарплат службовців, можливих кадрових проблемах, методах мотивації персоналу тощо. Ці дані будуть особливо необхідні, якщо в на підприємстві є кадрові проблеми або існує загроза переманювання цінних кадрів конкуруючою фірмою.

Перед конкурентною розвідкою стоять два завдання:

- знати про всі можливості або загрози в навколишньому світі і вчасно подати сигнал. Причому цей сигнал повинен бути поданий якомога раніше, доки ситуація не стала очевидною для всіх, що дозволить керівникові мати достатній запас часу для оцінки становища та використання шансу для захисту від небезпеки;

- забезпечити, щоб керівник, котрий визначає політику компанії, в будь-який момент часу знав правдиве становище свого підприємства в навколишньому світі. І неважливо, наскільки воно сприятливе. Головне - що інформація повинна бути об’єктивною [3, с. 112].

Сукупність методів, притаманних промисловому шпигунству, можна інтегрувати у дві групи, рис. 1.3.:

1. Агентурні методи.
2. Технічні методи.

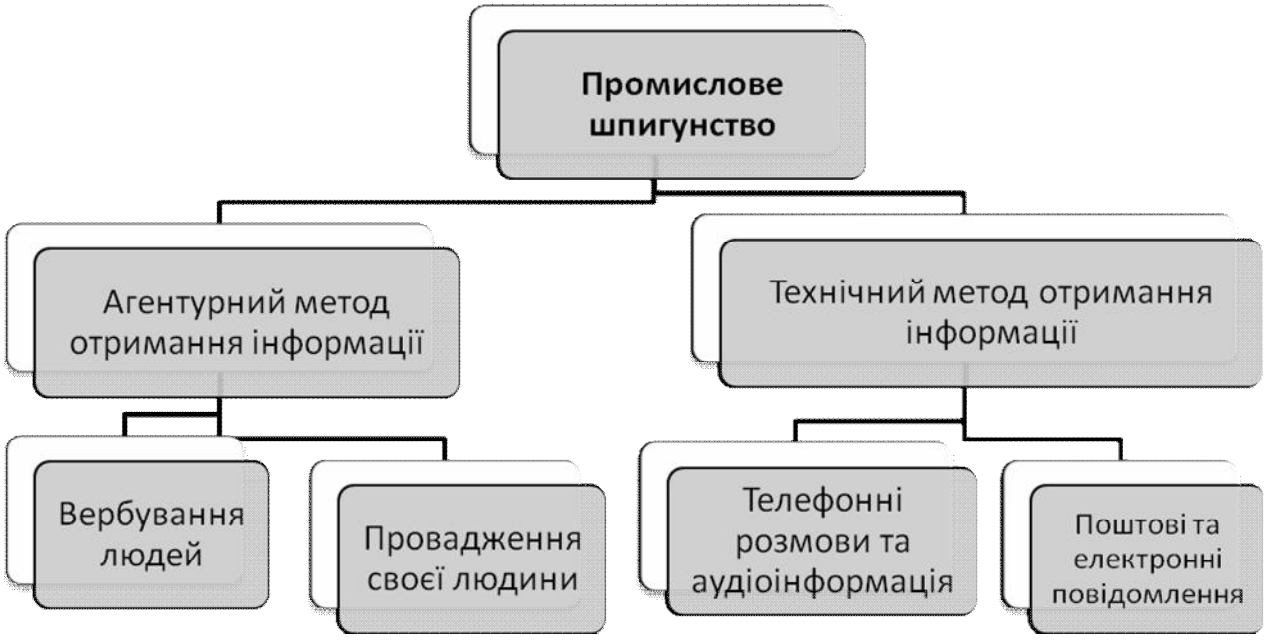

Рис.1.3. Методи промислового шпигунства
Джерело: Складено автором на основі [50]

Агентурний метод отримання інформації —основа будь-якого виду шпигунства. Тут можливі два напрями діяльності: або впровадження своєї людини, або вербування. Обидва способи мають свої переваги. У будь-якій комерційній структурі є «другі» або «треті» особи, котрі за своїми знаннями й досвідом наближаються до рівня вищої ланки і які спроможні самостійно вести власну гру. Наслідком вербування може бути те, що прибуткові замовлення підуть тим особистостям, які й влаштували бізнес-шпигунство на свою користь. Якщо завершальною метою промислового шпигунства є ліквідація фірми-конкурента, або отримання комерційної таємниці, то варіант із запровадженням має істотні переваги, тому що довіра до близької людини, звичайно ж, більша.

Об'єктами агентурної розробки можуть бути не тільки, скажімо, «другі» або «треті особи» фірми-конкурента, а й будь-які службовці, навіть, нижчої ланки. Вони цілковитоздатнівиконатинепомітне встановлення відповідної

апаратури («комарів» , «жучків» тощо). Для цього потрібно від декількох секунд до двох-пяти хвилин. Для того, щоб поставити обладнання для перехоплення телефонних повідомлень, узагалі не потрібно проникати в офіс, доцільно лише знайти телефоніста, котрий погодиться знайти необхідний телефонний кабель. Такі «закладки» можуть бути інстальовані по лінії телефонного кабелю на відстані до 3-х кілометрів від офісу, що значно ускладнює їх виявлення [42].

Технічні методи промислового шпигунства використовують техніку, збут й виробництво якої врегульовано законодавчо. Для реєстрації і перехоплення акустичної інформації існує великий арсенал різноманітних засобів: електронні стетоскопи, мікрофони, лазерні мікрофони, радіо-мікрофони («радіозакладки»), апарати магнітного запису.

Непомітне підкидання радіопередавальних (частіше закамуфльованих) пристроїв — доволі поширений спосіб добування інформації. Такі предмети протягом кількох годин або кількох днів, доки не «сяде» елемент живлення, «усмоктують» усю озвучену в приміщенні інформацію. А якщо в зловмисників є бажання якомога більше «попрацювати» на «ворожій» території, то вони підключають «вухо» до електромережі стаціонарно; тоді підслуховувальнийприлад працюватиме доти, доки його не знайдуть. Вибір «жучків» великий, коштують вони від 10–20 до 100–200 дол. США, також є і саморобні — примітивні[47, с.244]. До речі, недорогі «жучки» можна використовувати для підслуховування розмов на вулиці, розкидаючи «шкідливих комах» у листі й траві, покриваючи подібною «мережею» великі території. Їх можна придбати на будь-якому радіо ринку, однак, за рекомендації авторитетної особи.

За даними спеціалістів, в Україні найпоширенішим з усіх технічних засобів зняття інформації є приховане підключення до телефонних ліній. Прослуховування телефонів поширене через дешевизну й простоту. Випадки негласного відео спостереження поодинокі.

Сьогодні відомо багато методів «сканування» телефонних переговорів — від простих, наприклад, перехоплення сигналу радіотелефонів, до таких технічно складних і дорогих, як високочастотне нав'язування (коли телефонна лінія може використовуватися не тільки як безпосередняоснову інформації, а й як канал передачі інформації, отриманої з іншого джерела, зокрема, за допомогою акустичного «жучка», а також як джерело живлення для професійнихпідслуховувальних пристроїв, що передають інформацію по радіоканалах).

Пристрої прослуховування, які найчастіше встановлюють у офісах, залежно від джерел електроживлення можуть бути автономними або стаціонарними. Наприклад, автономні «жучки» отримують енергію від акумуляторів або невеликих батарейок, до яких приєднують мініатюрні передавачі й мікрофони. Цих «комах» непомітно «залишають» у приміщенні, де вони й працюють, доки вистачає заряду батареї (зазвичай 7–10 діб).

Рік від року росте популярність «мобільного» шпигунства й захисту від нього. За словами продавців захисного устаткування, за останній час значно піднявся попит на блокатори стільникових телефонів.

Існують зовнішні пристрої, при використанні котрих навіть відключений мобільний телефон (якщо з нього не виймуть акумулятор) можуть активувати і «призвести» його передавати діалог власника та й усі розмови в приміщенні, де перебуває даний телефон. Для протидії «мобільному» прослуховуванню спеціалісти розробили різноманітні шумогенератори для мобільних телефонів (найпростіші з них коштують 250–300 дол.США). Причому, якщо такий іноземний пристрій елементарноробить шумові перешкоди в радіодіапазоні роботи мобільного телефону, то вітчизняні прилади працюють більш широко: вони блокують таким чином, що «убивають» тільки синхроімпульс зв'язку з базою і ніяк себе не демаскують. Такі пристрої і коштують дорожче — 1,2 тис. дол. США [47, с.245].

Інший напрям промислового шпигунства, що набуває популярності в усьому світі, а також і в Україні, — це отримання конфіденційної інформації за

допомогою Інтернету.В Україні понад 20 підприємств мають ліцензію на виготовлення й розробку підслуховувальних закладних пристроїв. Діяльність бізнес-аналітики в контексті економічного шпигунства поділяється на такі складові:

1. Секторальна розбивка економіки країни.

2. Промислове шпигунство, яке, у свою чергу поділяється на: комерційне, технологічне та науково-технічне (рис. 1.4.).

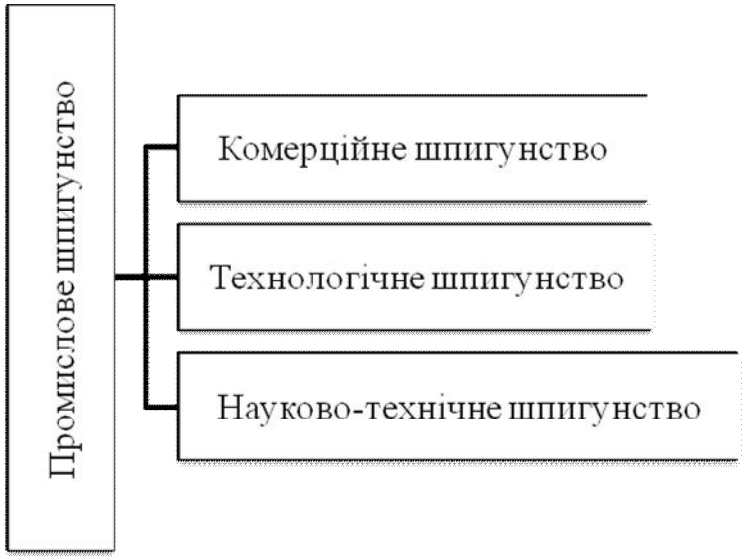

Рис.1.4.Основні види промислового шпигунства
Джерело: Складено автором

Це основні методи промислового шпигунства, які, у свою чергу, поділяються ще на низку способів добування конфіденційної інформації (дезінформування конкурентів, шантаж і підкуп, використання можливостей правоохоронних та контрольних органів тощо).

Елементом ринку корпоративних безпеки є механізм захисту від конкуруючого підприємства власних секретів виробництва, прав на об’єкти інтелектуальної власності тощо. Безпека визначається як відсутність неприпустимого ризику заподіяння шкоди [48, с. 23]. Цей компонент відображає рівень відповідності національного виробничого потенціалу підприємства по відношенню до зовнішнього, утвореного в ринковому середовищі, в такому обсязі, наскільки виробництво, наукові дослідження, маркетингові заходи можуть задовольнити потреби ринку і конкретні потреби

споживачів. Важливість цього елементу економічної безпеки полягає в тому, що він несе відповідальність за ефективність доставки продукції до конкретних споживачів, зважаючи на неузгодженість заходів маркетингу, дизайнерів, інженерів, економістів, фінансистів, низьку якість продукції, затримку відгуку на зміну ринкових умов, неефективної мережі продажу, низької корпоративної культури–це список можливих внутрішніх факторів навколишнього середовища, які загрожують безпеці на корпоративному ринку. Зовнішнє середовище знаходиться поза контролем компанії, це система відносин покупців, продавців, агентів, партнерів, конкурентів, фінансових установ, рекламних агентств, митні та податкових організацій. На рівень безпеки впливають на ринку: недобросовісні дії конкурентів, платоспроможність клієнта, часті зміни в податках і обмінних курсів, політична ситуація в країні і в світі тощо.

1.3. Активні чинники та інструменти промислового шпигунства у якості засобів негласного збору інформації

Із зростанням інфляції, зростанням конкуренції і соціальної напруженості в світі промислове шпигунствоактивізовується. Беруть участь у підтримці даної активності і представники неурядових організацій, і приватніособи. Практика показує, що неурядові організації, що займаються промисловим шпигунством, найбільш зацікавлені в таких питаннях конкуруючих фірм, організацій та банків:

– фінансова звітність та прогнози;

– маркетингова стратегія і цінова політика;

– технічні характеристики поточних і майбутніх продуктів;

– умови контрактів;

– майбутнє виробничі плани;

– фінансове становище об'єкта;

– умови продажу або злиття об'єктів;

– організаційна структура об'єкта;

– найбільш важливі елементи системи безпеки, доступу до мережі умовно-дострокового звільнення та інформаційних центрів.

Щоб витягти необхідну інформацію організації використовують спеціальні форми і методи, такі як:

– завуальовані запитання до фахівців конкурента;

– підступні пропозиції для фахівців, що працюють в конкурента з пропозицією заповнити текст зі спеціально відібраних питань;

– очевидні переговори з конкурентом в питаннях, що стосуються товарів або ліцензії, і після отримання необхідної інформації, відмова від ходу переговорів;

– безпосереднє спостереження за об'єктом, яким може бути відділ або фахівець;

– використання професіоналів в цілях отримання інформації;

– напад на майно конкурента;

– підкуп співробітників конкурента;

– залучення фахівців, агентів, експертів конкурента;

– розмова-допит з конкурентом;

– крадіжки креслень, проектів, документів;

– шантаж і тиск в різних способів;

– незаконне придбання інформації корумпованими елементами в уряді.

Типові активні чинники промислового шпигунства:

– отримання ринків збуту;

–виробництво контрафактних товарів;

– усунення конкурентів або їх дискредитування;

– перепродажі секретів підприємства;

– перерви в переговорах, що стосуються угод;

– шантаж;

– створення умов для проведення терористичних і диверсійних операцій.

Найбільш активну участь в промисловому шпигунстві беруть транснаціональнікорпорації (ТНК). Експерти вважають, що в сучасному світі працює не менше, ніж 55 тис. транснаціональних корпорацій з близько 170 тисяч. філіями. Триста основних транснаціональних корпорацій контролюють близько 25 % усіх активів[7, с.177]. У розвідувальній діяльності транснаціональних корпорацій присутні всі види шпигунства:від науково-технічного до політичного. Особливе місце в цій області належить іноземним юридичним особам, які мають розвідувальну мережу, що складається з «інформаторів», і котра поширена по всій країні з величезними фінансовими можливостями.

Спеціальним методом реалізації промислового шпигунства є шантаж. Для конкретної людини це сімейний стан, звички, уподобання, схильності його та членів його сім'ї, і, якщо це можливо, компроміс між збереженням інформаціїта можливістюотримання кимось хабара. Спеціальне обслуговування ASIS - американського співробітництва в галузі промислової безпеки - який об'єднує керівників служб безпеки найбільших транснаціональних корпорацій, американських за походженням, було створене для боротьби з повторною маршрутизацією науково-технічної інформації поміж філіями американських корпорацій за кордоном. Є й інші асоціації. Наприклад, відомий французький бренд«PierreCardin», «ChristianDior», «Chanel», «NinaRicci» і «Gucci» об'єднали свої сили проти промислового шпигунства, і прийшли до висновку, що це буде простіше для них, щоб боротися з приватними конкурентами[67, с.130].

Польський законодавець, наприклад, виділяє також поняття «шахрайських наслідувань», які, відповідно до ст. 13 Закону «Про боротьбу з недобросовісною конкуренцією» [90] заборонені і полягають в тому, що за допомогою технічних засобів відтворення, що копіюються на зовнішні форми продукту, можуть ввести в оману споживачів щодо ідентичності виробника або продукту. Загалом, це результат промислового шпигунства. Адемчак А. і ДюВаль М.зазначають, що порушення принципів чесної конкуренції, насамперед, призводять до наслідків на ринку, позбавляючи потерпілого

підприємця можливості провадження бізнесу [64, 334]. Є два типи відповідальності за здійснені недобросовісної конкуренції за польським законодавством: цивільна і кримінальна. Відповідальність цивільна регулюється ст. 18 Закону «Про боротьбу з недобросовісною конкуренцією», а кримінальна відповідальність - ст. 23-24 даного нормативно-правового акту.

На додаток до інформації про діяльність компаній, банків та інших організацій, сили безпеки транснаціональних корпорацій збирають дані про відомих політиків у країні розташування виробничих потужностей, так і в країнах, в яких вона здійснює свою діяльність, для того, щоб мати можливість лобіювати власні інтереси або ж змусити їх пристати до своїх інтересів. Для цього проводяться заходи, орієнтовані на складання списків провідних фахівців і менеджерів компаній-конкурентів, атакож спецслужб великих корпорацій і спеціальних служб, науково-дослідних талановитих учених з різних країн.

Згідно з визначення НД ТЗІ 2.7-011-2012, закладний пристрій – потай встановлений технічний засіб, який створює загрозу для інформації [28, с.50]. Залежно від виду інформації, що перехоплюється, закладні пристрої поділяються на акустичні, телефонні, апаратні та закладні відеосистеми. Інформація, що перехоплюється акустичними закладними пристроями, може записуватися з використанням портативних пристроїв звукозапису або передаватися по радіоканалу, оптичним каналом, по електромережі змінного струму, по лініях допоміжних технічних засобів, металоконструкціях будинків, трубах систем опалення і водопостачання, а також спеціально прокладених кабелях та лініях. Широко використовуються акустичні закладні пристрої, що передають інформацію через радіоканал. Закладні пристрої можуть бути виконаніу вигляді окремого модуля, зазвичай у формі паралелепіпеда, або закамуфльовані під предмети повсякденного побуту: електронний калькулятор, авторучку, електролампочку, запальничку, наручний годинник, вазу, поясний ремінь та ін. Для перехоплення акустичної інформації зловмисник може скористатися безліччю портативних засобів, що дають змогу перехоплювати акустичну інформацію по прямому акустичному, віброакустичному,

електроакустичному й оптико-електронному (акустооптичному) каналах. Сюди відносять [26, с. 230]: телефонні закладні пристрої, радіожучки, радіомікрофони, стетоскопи, мікрофони спрямованої дії. Промислове шпигунство здійснюється за допомогою різних засобів:

– спеціальний пристрій запису;

–пристрій для захоплення телефонних ліній ;

–аудіо та відео міні камери;

– обладнання для отримання інформації з вікон, з використанням лазерних випромінювачів;

– навідні мікрофони;

–спеціальна система спостереження і передачі відео;

–спеціальна фотоапаратура;

–прилади спостереження;

–прилади нічного бачення;

– пристрій для виявлення випромінювання і т.д.

На сьогоднішній день виокремлюють такі види направлених мікрофонів (мікрофонів направленої дії):

- мікрофон направленої дії «Супер Вухо 30» - персональний звуковий підсилювач. Високочутливий мульти-елемент спрямованого мікрофона збирає звуки для посилення на відстані до 30 метрів і має можливість обертатися на 90 градусів. Новий динамік «Супер Вухо 30» підсилює звуки до 40 децибел.Направлений мікрофон «Супер Вухо 30» компактний пристрій, важить 65.0 грам і має розміри: 9.0 x 5.0 x 2.0 см. І легко розміщується в кишені або гаманці (Вартість - 1682.70 грн) [15];

- направлений мікрофон «Супер Вухо 50» посилює звук до 50 децибел. Високочутливий мультиелемент мікрофона збирає звуки для посилення на відстані до 50 метрів. Направлений мікрофон «Супер Вухо 50» допомагає чути звуки навколо вас на відкритому повітрі, у закритому приміщенні, скрізь, де це необхідно. Направлений мікрофон досить компактний, легко може бути

розміщений в кишені одягу або в сумочці. Направлений мікрофон захищений поролоновою оболонкою і може обертатися на 180 градусів. Зручні стерео навушники поставляють ясний, свіжий звук, особливо в діапазоні людського голосу. (Приблизна вартість - 2000 грн.) [15];

- «Супер Вухо 100». Потужна система реєстрації звуку посилює звук до 70 децибел і дозволяє чути навіть найслабше спів птахів, або неголосний розмова, або шуми на відстані до 50-100 м. Для збільшення спрямованості і купчастості збору звуків в мікрофоні спрямованої дії використовується пластикова параболічна тарілка. Користувач надягає стерео навушники, включає мікрофон направленої дії «Супер Вухо 100», і регулює (пристосовує) за допомогою регулятора гучність звучання до своїх індивідуальних потреб. Наявність в мікрофоні спрямованої дії вбудованого диктофона дозволить Вам зберегти найважливіші моменти і не упустити нічого важливого. Ціна становить близько 1170 грн.[15].

- «Супер вухо плюс». Однією з особливостей «Супер вуха плюс» є те що, на відміну від інших спрямованих мікрофонів, вам не потрібно одягати навушники і направляти постійно мікрофон у бік об'єкта, прилад фіксується у вушній раковині за допомогою спеціального вушного держателя, як лівостороннього, так і правостороннього. Так само «Супер вухо плюс» стилізований під звичайну бездротову гарнітуру для мобільних телефонів і з боку він не відрізнити від неї. (Вартість - 795.00 грн) [15].

- мікрофон направленої дії «Супер Вухо SD» призначений для прослуховування та запису віддалених звуків, розташованих в зоні прямої видимості. Параболічна антена для концентрації звуків має посилення до 70 дБ - це означає, що можна почути неголосні звуки на відстані до 50-100 метрів.Мікрофон оснащений вбудованим моноклем з 8-кратним збільшенням зображення, щоб було легше вибрати об'єкт спостереження і розгледіти всі його деталі.Відмінною особливістю даного мікрофона є вбудований диктофон із записом на SD карту пам'яті. Таким чином, можливо записати всі уловлювані звуки в цифровому форматі на карту пам'яті. (Вартість - 1710.00 грн.) [15].

Для ознайомлення із принципом роботи закладних пристроїв, було сконструйовано два пристрої, схеми яких є у відкритому доступі в мережі Інтернет. За допомогою виготовлених пристроїв проводили експериментальні дослідження для визначення технічних характеристик пристроїв за різних умов. Перший виготовлений пристрій (ЗП-1) – найпростіший за схемою побудови (рис. 1.5.) [24].

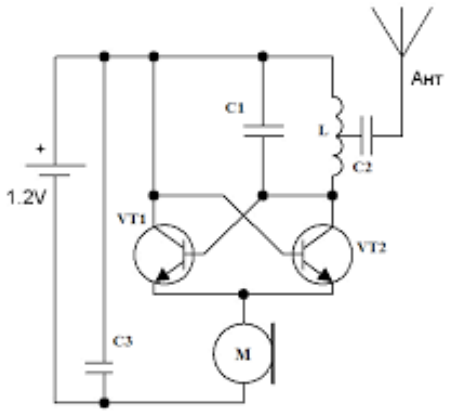

Рис. 1.5. Схема закладного пристрою №1
Джерело: Мандрона М. М. Порівняльний аналіз закладних пристроїв для несанкціонованого отримання акустичної інформації / М. Мандрона, Р. Сало/ Науковий вісник НЛТУ України. – 2014. – Випуск 24.2. – С. 344.

Його особливість – використання мінімальної кількості радіоелементів і простота в реалізації. У ЗП-1 використовуємо лише два транзистори типу КТ368, які модулюють частоту. Мікрофон стандартний від гарнітури мобільного телефону. Антена виготовлена з мідного дроту довжиною 30 см, намотаного на гелеву ручку, для зменшення розміру. Зважаючи, що струм споживання всього 0,2 мА вимикача живлення не потрібно. Струм споживання є такий низький, що цей пристрій може працювати місяць на одній батарейці. Не зважаючи на всі переваги, він має недоліки, а саме – радіус прослуховування лише 10 м. Проте цього достатньо, щоб прослуховувати все, що відбувається у сусідній кімнаті. На рис. 1.6. наведено схему побудови другого пристрою (ЗП-2) [24]. Його особливість – значно менші розміри, порівняно із ЗП-1. Це відбулось завдяки використанню мініатюрних гальванічних елементів.

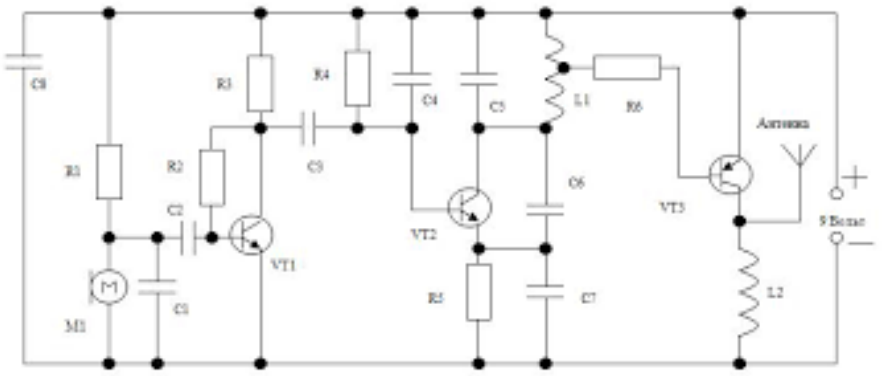

Рис. 1.6. Схема закладного пристрою №2

Джерело: Мандрона М. М. Порівняльний аналіз закладних пристроїв для несанкціонованого отримання акустичної інформації / М. Мандрона, Р. Сало/ Науковий вісник НЛТУ України. – 2014. – Випуск 24.2. – С. 345.

Схема ЗП-2 характеризується великою чутливістю. Її зібрано з двох частин: мікрофонного підсилювача і передавача. Можна використовувати будь який електронний мікрофон, у роботі застосовуємо цифровий мікрофон від мобільного телефону. Чутливість мікрофона не є велика, тому в схемі використовуємо каскад підсилення мікрофона на одному транзисторі (S9014), але можна використати й інші транзистори малої потужності, такі як: КТ315, КТ368, КТ3102, С9014/9018. У табл. 1.1 подано результати експериментальних випробувань закладних пристроїв за найбільш важливими характеристиками.

Таблиця 1.1

Характеристики сконструйованих закладних пристроїв

(складено автором на основі [24])

	Відстань прослухову-вання, м		Час-тота, Гц	Струм споживан-ня, мА	Живлен-ня, В	Час робо-ти, год	Чутли-вістьмікр о-фонна, м	Габа-рити	Ва-га, г
	без шуму	з шумом							
ЗП-1	2	5	99,6	0,2	1,5	360	1	6*3,5*2	40
ЗП-2	50	60	103,4	30	9	6	5	4*2*1	14

Для того, щоб обрати ефективний закладний пристрій, потрібно провести порівняльний аналіз характеристик розроблених закладних пристроїв. Після тестування ЗП-2 продемонстрував хороші результати, відстань

прослуховування становить близько 50 м без шуму і більше 60 м з незначним шумом.ЗП-1 значно відстає у цій характеристиці – не більше 5 м, проте дальність йогоє достатньою для прослуховування сусідніх кімнат. Також цей пристрій дуже важко виявити індикаторами поля, оскільки він випромінює слабкий сигнал. Частота передавання закладного пристрою не відіграє значної ролі в прослуховуванні. У цьому випадку головне, щоб частота потрапила в діапазон FM приймача і не збігалася з частотою радіостанцій. Для ускладнення відстеження закладному пристрою підбирають частоту, наближену до частоти, на якій працюють інші пристрої, наприклад Wi-Fi, мобільний телефон тощо. Для того, щоб обрати ефективний закладний пристрій, потрібно провести порівняльний аналіз характеристик розроблених закладних пристроїв. Після тестування ЗП-2 продемонстрував хороші результати, відстань прослуховування становить близько 50 м без шуму і більше 60 м з незначним шумом. ЗП-1 значно відстає у цій характеристиці – не більше 5 м, проте дальність його є достатньою для прослуховування сусідніх кімнат [24, с.350]. Також цей пристрій дуже важко виявити індикаторами поля, оскільки він випромінює слабкий сигнал. Частота передавання закладного пристрою не відіграє значної ролі в прослуховуванні. У цьому випадку головне, щоб частота потрапила в діапазон FM приймача і не збігалася з частотою радіостанцій. Для ускладнення відстеження закладному пристрою підбирають частоту, наближену до частоти, на якій працюють інші пристрої, наприклад Wi-Fi, мобільний телефон тощо. Від струму споживання закладного пристрою залежить час його роботи. Споживання струму в ЗП-1 нижчий, тому і час його роботи значно більший. ЗП-2 споживає струму значно більше, відповідно і час роботи в нього набагато менший; це спричинено тим, що у схемі побудови більше радіоелементів, які потребують електроенергії. Живлення закладних пристроїв впливає на їх розмір та час роботи. ЗП-1 потребує малого струму, тому можна використати і менші батарейки. Найдовше на одному автономному джерелі живлення може працювати ЗП-1. Його час роботи сягає близько місяця на одному гальванічному елементі типу ААА. У ЗП-2 встановлено значно

менший час роботи, близько 6 год без заміни джерела живлення. Це пов'язано з величиною струму, який він споживає. Чутливість мікрофона – одна з найважливіших характеристик будь-якого закладного пристрою, тому що чим вища чутливість, тим чіткіше можна почути розмову. Чутливість ЗП-1 всього один метр. Це дуже мала відстань і тому потрібно, щоб пристрій знаходився поблизу промови розмовника, наприклад на робочому столі, замаскований під звичайний предмет. Чутливість ЗП-2 достатня для підслуховування усієї кімнати. У наступній табл. 1.2 описано переваги і недоліки досліджуваних закладних пристроїв.

Таблиця1.2

Переваги та недоліки досліджуваних закладних пристроїв

(складено автором)

Пристрій	Переваги	Недоліки
ЗП-1	Малий струм споживання і напруга живлення, довгий час роботи, не попадає в частоту радіостанцій, найменша собівартість.	Мала чутливість мікрофона і відстань прослуховування, великий розмір.
ЗП-2	Велика дальність прослуховування, маленький розмір, вага і вартість.	Частота дуже близька до радіостанцій, великий струм споживання і напруга живлення, відносно малий час роботи і мала чутливість мікрофона.

На сучасному етапі, коли багато традиційних ресурсів людського прогресу втрачають своє першочергове значення, інформація як була, так і залишається одним із головних ресурсів науково-технічного і соціально-економічного розвитку світового співтовариства. Однак багато фахівців відзначають слабкістьюриспруденції розвинених країн щодо захисту підприємств від промислового (комерційного) шпигунства [10; 20]. Викрадення промислових секретів важко довести, а неадекватність законів обмежують суди і дають мало шансів потерпілим у переслідуванні злочинців, які займаються промисловим шпигунством. Таким чином, проблема захисту інформації та забезпечення її конфіденційності набуває актуальності для багатьох комерційних підприємств, чия діяльність перебуває поза сферою, де ці питання

вирішують державні органи. І, звичайно, кожному хочеться для зміцнення своєї безпеки використовувати самі надійні сучасні методи і засоби, що враховують усі особливості прийомів несанкціонованого добування інформації. Метою статті є класифікація засобів негласного збору інформації для вибору оптимальних способів здійснення інформаційної безпеки власників конфіденційної інформації. Аналіз публікацій. Один з ефективних шляхів негласного збору інформації засновано на застосуванні так званих закладних пристроїв (ЗП), що таємно встановлюються в місцях можливого перебування об'єктів спостереження або підключаються до використовуваних ними каналів зв'язку, причому для опису таких пристроїв використовуються також терміни «радіомікрофони», «закладки», «жучки», «спецзасоби» [18, с.241]. На сьогодні створено величезну кількість типів таких пристроїв, що відрізняються принципом функціонування, способом передачі інформації, дальністю дії, а також розміром і зовнішнім оформленням. Зазвичай ЗП таємно встановлюються на елементи конструкції будівель та інтер'єру, кріпляться під одягом або камуфлюються під особисті речі.

Для того, щоб систематизувати уявлення про закладні пристрої, доцільно ввести п'ять ознак їх класифікації. Залежно від каналу передачі інформаціїрозрізняють такі типи ЗП: радіозакладки; інфрачервоні закладки; закладки з передачею інформації струмопровідними лініями; закладки з записом на магнітофон. У радіозакладних пристроях (РЗП) для передачі інформації використовується енергія електромагнітних хвиль, які не впливають на органи чуття людини і здатні поширюватися на значні відстані, долаючи природні та штучніперешкоди. Завдяки цим двом властивостям РЗПдозволяють за допомогою спеціальної приймальноїапаратури вести таємне спостереження за цим об'єктом із досить віддаленої від нього точки. В інфрачервоних закладках для передачі інформації використовується енергія електромагнітних хвиль, але не радіодіапазону, а невидимої частини оптичної сфери спектру – інфрачервоного діапазону. Завдяки малій довжині такі хвилі розповсюджуються вузьким пучком у заданому напрямі, їх важко виявити

навіть за допомогою спеціальної апаратури, однак висока прихованість таких пристроїв і незастосовність на мобільних об’єктах істотно ускладнює їх застосування. Закладки з передачею інформації струмопровідними лініями використовують властивістьелектричних сигналів розповсюджуватися назначні відстані по провідниках і володіють такимисуттєвими перевагами: висока прихованістьпередачі інформації, велика дальність дії, відсутність необхідності в додаткових джерелахживлення, унаслідок чого вони часто застосовуються недобросовісними конкурентами дляотримання відомостей конфіденційного характеру. У випадках, коли відсутня необхідністьотримання оперативної інформації в реальномумасштабі часу, а також є можливість прихованоговилучення та заміни касети або магнітної стрічки, закладка може оснащуватися магнітофономзамість пристрою передачі по одному зрозглянутих каналів. Такий спосіб, як правило, застосовується тільки в тих випадках, коли єпотенційна загроза виявлення об’єктом спостереження каналу передачі інформації (наприклад, задопомогою спеціальної апаратури контролю). Залежно від способу сприймання інформаціїрозрізняють три типи ЗП: мікрофонного типу; вібраційного типу; із підключенням до комунікаційних ліній. Принцип дії ЗП мікрофонного типу заснований на перетворенні акустичних атмосфернихколивань в електричні сигнали і передачі їхспоживачу одним із вищеперелічених способів. ЗПвібраційного типу (стетоскопи) перехоплюютьакустичні коливання твердих середовищ (вібрації), що виникають унаслідок тиску на них атмосфернихакустичних хвиль. ЗП із підключенням до комунікаційних ліній призначені для негласногоперехоплення інформації, що циркулює втелефонних або волоконно-оптичних лініях.За наявністю пристрою управління ЗПумовно можна розділити на три групи: ізбезперервним випромінюванням; із дистанційнимуправлінням; із автоматичним включенням припояві сигналу. ЗП із безперервним випромінюванням найбільш прості у виготовленні, дешеві і призначенідля отримання інформації протягом обмеженогопроміжку часу, проте недоліком таких пристроїв єможливість їх виявлення за випромінюванням. Суттєво

збільшити час безперервної роботи ЗПз автономним живленням і підвищити прихованістьдозволяє застосування дистанційного управління ЗП. Воно дозволяє переводити пристрій у режимвипромінювання тільки в тих випадках, колиоб'єкт спостереження веде переговори або передаєінформацію по каналах зв'язку. Іншим способом збільшення часу роботи ЗП євикористання пристроїв автоматичного включення електричного в лінії). Пристрої включення від голосу називають акустоматами, а також системами VAS або VOX [4, с. 121]. При появі сигналу з початком розмови об'єкта спостереження з ким-небудь подається напруга на передавач, і той переходить у режим випромінювання. Застосування акустомата дозволяє в кілька разів збільшити час роботи ЗП, але призводить до його подорожчання і втрати перших слів при кожному включенні. За використовуваним джерелом живленняЗП поділяються на два види: із власним (автономним) джерелом; із живленням від зовнішнього джерела. Причому, до другого виду відносяться ЗП із передачею інформації струмоведучими лініями і з безпосереднім підключенням до комунікаційних ліній. За зовнішнім виглядом ЗП можуть бути у звичайному виконанні (у металевому корпусі і мають форму паралелепіпеда) або в закамуфльованому вигляді (вбудовані в предмети інтер'єру або особисті речі). Класифікація, принципи дії та основніхарактеристики радіозакладних пристроїв(РЗП). Найбільш широке застосування в практиці промислового шпигунства знаходять пристрої з радіоканалом передачі перехопленої інформації, які називаються радіозакладками (РЗП) або радіомікрофонами (РМ). Підвищений інтерес до використання РЗП пов'язаний з їх винятковими можливостями віддаленого спостереження за об'єктами, у тому числі мобільними, незалежно від часу доби і погодних умов. Для класифікації РЗП може бути використано такі ознаки: принцип формування сигналу; спосібзакриття переданої інформації і дальність дії. Відповідно до принципу формування сигналуРЗП можуть бути активні, пасивні та напівактивні. У пасивних і напівактивнихРЗП використовується підсвічування (випромінювання) додаткового джерела сигналу. Однак, володіючи високою прихованістю (вони не випромінюють, якщо їх не

опромінює потужне джерело сигналу), пасивні та напівактивні РЗП досить громіздкі, дорогі, а тому не знайшли широкого практичного застосування. Найпростіші РМ містять кілька основних елементів, що визначають їх технічні характеристики та можливості застосування: мікрофон із низькочастотним підсилювачем; радіопередавач (РП); джерело живлення, від якого залежить тривалість роботи РМ; антена; блок накопичення і стиснення інформації; пристрій управління, у ролі якого може використовуватися приймач дистанційного управління, що дозволяє переводити РМ у режим випромінювання тільки за кодованими радіосигналами «ініціації»; та приймальна апаратура. За способом закриття інформації РЗП бувають: без закриття інформації; із використанням складних видів модуляції; із кодуванням інформації. Залежно від потужності передавача РЗП діляться на три види – малої, середньої і великої дальності дії. Деякі дані за характеристиками РЗП, які серійно випускаються, наведено в таблиці 1.3.

Таблиця 1.3

Залежність діяльності дії радіозакладок від потужності передавача та експлуатаційних норм

(складено автором на основі [24])

Ринт. мВт (потужність РП)	Дальність передачі інформації, м		
	У залізобетонному приміщенні	Із приміщенням на вулицю	Пряма видимість
1	20-30	50-100	100-200
10	30-60	150-200	200-500
100	50-100	300-400	800-1000
500	100-200	400-600	1000-2000

Мережеві закладні пристрої (МЗП) та їххарактеристики. МЗП, які призначено для негласного збору акустичної (мовної) інформації з передачею її електромережею, володіють рядом переваг, порівняно з іншими типами ЗП: необмежений час безперервної роботи, так як живлення ЗП здійснюється від тієї ж електромережі; підвищенаприхованість роботи, зумовлена видом модуляції і середовищем поширення інформаційних сигналі ЗП; складність точного виявлення місця установки приймального обладнання, на відміну,

наприклад, від провідних мікрофонів, які використовують власні провідники для передачі сигналів; відсутність візуальних демаскуючих ознак, так як мережеві ЗП установлюються у звичайних побутових електроприладах. Ці переваги, поряд із відносно низькою вартістю, зумовлюють високу ймовірність застосування мережевих ЗП у системах тривалого контролю акустичних сигналів у виділених приміщеннях. Основні характеристики деяких мережевих ЗП, які серійно випускаються, наведено в таблиці 1.4.

Таблиця 1.4

Основні характеристики мережевих закладних пристроїв (МЗП)

(складено автором на основі [24])

Тип МЗП	Робочий діапазон частот, кГц	Вид модуляції	Потужність, мВт	Дальність дії, м	Ціна (орієнтовна у 2015 р.), у.о.
Електромережа-КС	60-300	WFM	7-10	100	200
Електромережа-КМ	60-450	WFM	100-250	300	300
Подовжувач	600-650	WFM	100	250	250
HKG-2221	100-150	FM	10-25	150	220
PK-1295-S	60-200	NFM	10	100	200
SEL-M220-01	200-500	FM	25	200	180
Мережевий модуль	200-800	WFM	150-350	500	320

Заходи щодо захисту інформації від впливупромислового шпигунства. У разі витоку інформації, яка складає комерційну таємницю, особи, які незаконними методами отримали її, а також особи, що розголосили комерційну таємницю, зобов’язані відшкодувати власникові комерційної таємниці заподіяні цими діями збитки. Це означає, що якщо власник не вживав заходів для захисту інформації або інформація не становить комерційної цінності для нього, то в разі її розголошення або використання третіми особами такий володар не має права в судовому порядку вимагати відшкодування завданих йому збитків. Вважається, що основною метою віднесення інформації до комерційної таємниці є необхідність захисту її від несанкціонованого використання третіми особами, промислового шпигунства, незаконної передачі та поширення, або, інакше кажучи, від недобросовісної конкуренції. Однією з основних ознак відомостей, що становлять комерційну таємницю, є те, що

стосовно цих відомостей вжито заходів щодо забезпечення конфіденційності. Тільки за дотримання цих умов може наступити передбачена законодавством дисциплінарна, матеріальна, адміністративна та кримінальна відповідальність.

Висновки до розділу 1

Отож, для підприємництва промислове шпигунство — це лише засіб конкурентної боротьби. І якщо суб'єктом економічного шпигунства (стороною, котра реалізовує активні дії) є держава в особі власних спецслужб, то щодо промислового — ним є окремий підприємець, підприємство, тобто фізична або юридична особа.

Промислове шпигунство, зазвичай, має такі цілі:

- одержання інформації щодо конкурентів, передусім конфіденційної, про тактичні й стратегічні наміри їхнього бізнесу;
- здобуття конкурентної переваги на ринку, шляхом знищення або витіснення конкурента.

Найбільш розповсюджені форми промислового шпигунства:

- підкуп особи, що володіє даними;
- впровадження шпигуна, котрий мав би можливість доступу до конфіденційної інформації;
- крадіжка інформаційного носія з даними, які представляють службову або комерційну таємницю;
- перегляд кореспонденції, прослуховування телефонів, електронних листів.

Сукупність методів, притаманних промисловому шпигунству, можна інтегрувати у дві групи:

- агентурні методи;
- технічні методи.

Промислове шпигунство здійснюється за допомогою різних засобів:

– навідні мікрофони;

– прилади нічного бачення;

– спеціальні пристрої запису;

– пристрій для захоплення телефонних ліній;

– аудіо та відео міні камери;

– прилади спостереження;

– спеціальна система спостереження і передачі відео;

– обладнання для отримання інформації з вікон, з використанням лазерних випромінювачів;

– спеціальна фотоапаратура;

– пристрій для виявлення випромінювання і т.д.

Типові активні чинники промислового шпигунства:

– виготовлення контрафактних товарів;

– перепродажі таємниць підприємства;

– отримання ринків збуту;

– знищення або дискредитування конкурентів;

– шантаж та саботаж;

– перерви в переговорах, що стосуються угод;

– створення умов для проведення терористичних і диверсійних операцій.

РОЗДІЛ ІІ

АНАЛІЗ ПРАВОПОРУШЕНЬ ТА ДОСЛІДЖЕННЯ НОРМАТИВНО-ПРАВОВИХ ВІДНОСИНУ СФЕРІ ПРОТИДІЇ ПРОМИСЛОВОМУ ШПИГУНСТВУ

2.1. Міжнародне інституційне забезпечення та правове регулювання протидії промисловому шпигунству

Розглянемо американську теорію та практику у сфері боротьби з промисловим шпигунством. Основну увагу, на нашу думку, варто зосередити на аспектах кримінально-правової охорони комерційної таємниці,яка є першочерговим об'єктом посягань в контексті активних шпигунських правочинів. Американське право традиційно визнає комерційну таємницю однією з ключових форм інтелектуальної власності, головною запорукою розвитку інновацій у США, об'єктом промислового шпигунства. Більше того, комерційна таємниця часто є результатом багаторічних досліджень і тестувань, а також вимагає тисяч (а іноді й мільйонів) доларів інвестицій у науково-дослідницьку діяльність. Суспільна небезпека зловживання з комерційною таємницею інтерпретуєтьсяамериканською наукою кримінального права в декількох вимірах.

По-перше, розкриття комерційної таємниці чи викрадення ноу-хау може суттєво знизитиконкурентоздатність компанії чи взагалі зруйнувати її бізнес. Наприклад, неважко уявити, що всі конкурентні переваги компанії «Coca-Cola» зникнутьу разі розкриття засекреченої формули її всесвітньо відомого напою.

По-друге, небезпека промислового шпигунства проявляється ще й у тому, що в кінцевомупідсумку злочином завдається шкода не лише власникові секрету, ай третім особам - законослухняним працівникам компанії та їх родичам уразі звільнення; місцевим мешканцям, які опосередковано залежать віддіяльності містоутворюючої компанії; іншим компаніям - як контрагентам, так і конкурентам; чи навіть цілим галузям національної економіки.

По-третє, розкриття окремих видів комерційної таємниці може створитибезпосередню загрозу національній безпеці країни. Федеральне законодавствоduже жорстко охороняє це благо від будь-яких проявів промислового шпигунства. Так, матеріали опублікованої судової практики красномовно свідчать про непоодинокі спроби заволодіти чутливою секретною інформацією військового характеру. Узагалі, ураховуючи домінантні позиції США у світовій економіці, передусім у сфері високих технологій, потреби в забезпеченні економічного добробуту та національної безпеки й оборони, надійний захист від промислового шпигунства цілком природно залишається одним із пріоритетних напрямів протидії федеральним економічним злочинам. У 1996 р. було прийнято федеральний «Акт про економічне шпигунство»(англ. –«EconomicespionageAct»), що не в останню чергу стало результатом активного лобіювання з боку ФБР [66, с.40]. На той час федеральні агенти систематично стикались із проблемою, коли чинне законодавство не могло охопити випадки зловживання з інформацією, що має комерційне значення. Більше того, чимало компаній стикнулись із проблемами виконання рішень суду у цивільних справах про відшкодування збитків, пов'язаних із розголошенням комерційної таємниці в контексті промислового шпигунства. Таким чином, за задумом авторів, Акт про економічний шпіонаж повинен був заповнити правозастосовні прогалини в чинному на той момент федеральному та місцевому законодавстві. На сьогодні Акт про економічне шпигунство покликаний забезпечувати реалізацію двох основних завдань, а саме - забезпечення загальнонаціональної та економічної безпеки.

Глава 90 Розділу 18 Зібрання законів США (федеральний КК) має офіційнуназву «Захист комерційної таємниці» та структурно складається здев'яти норм (§§ 1831-1839), що безпосередньо закріплюють відповідні складизлочинів, а також визначають процесуальні та термінологічні аспектикримінальноївідповідальності за порушення режиму захисту від промислового шпигунства. Так, § 1831 має назву «Економічне шпигунство» і

спрямована на протидіюнезаконному заволодінню торговими секретами на користь іноземних (не США) держав [80, с.130].

Повернемося до порівняльного дослідження ознак злочинів, що посягають на засади добросовісної конкуренції в частині захисту від промислового шпигунства інформації, що є комерційною таємницею. У Сполучених Штатах для встановлення факту злочину, передбаченого § 1831 КК, необхіднообов'язково встановити наявність його чотирьох обов'язкових елементів [76, с.294]:

1) особа викрала чи без авторизації власника отримала, знищила чи передалаіншим інформацію;

2) особа знала, що ця інформація є чужою власністю;

3) інформація дійсно утворювала комерційну таємницю;

4) особабула обізнана про те, що злочин учинено на користь іноземного уряду, іноземного органу сприяння чи іноземного агента. Відповідно завданнямпрокуратури як органу державного обвинувачення США є доведеннявсіх чотирьох елементів промислового шпигунства під час розгляду кримінальноїсправи.

Зупинимося дещо детальніше на кожній із цих ознак. Федеральній судово-слідчій практиці наразі відомі три основні способинезаконного заволодіння інформацією в контексті промислового шпигунства, що становить комерційнутаємницю. Перший полягає в тому, що злочинці переманюють на свій бікпрацівників (інсайдерів) американських компаній та науково-дослідних установ, причому нерідко однакової національної приналежності. По-друге, вони використовують цілий арсенал протиправних дій - підкуп, кібератаки, крадіжки, підслуховування, вимагання тощо. Нарешті злочинціможуть фіктивно створити ззовні нормальні ділові відносини міжіноземними та американськими компаніями з метою збирання засекреченоїкомерційної інформації. Наведені способи незаконного заволодіння конфіденційною інформацією комерційного характеру найчастішефігурують у матеріалах кримінальних розслідувань ФБР. Поняття

«отримала», «знищила», «передала»тлумачаться американськимисудами досить широко й охоплюють як традиційні форми викрадення, де об'єкт фізично вилучається з володіння законного власника, такі менш поширені з них - копіювання, дублювання, малювання, фотографування, скачування, завантаження, фотокопіювання тощо. У таких нетрадиційнихвипадках зловживання з комерційною таємницею оригіналносія засекреченої інформації ніколи не вилучається з володіння власника. Водночас цінність і вартість інформації знижується чи взагалі перестаєіснувати через утрату ознак ексклюзивного джерела. Важливим моментом, що потребує належного юридичного закріплення, тут є ознака «безавторизації власника».

Законодавча історія розглядуваної заборонидемонструє, що така авторизація - це дозвіл, погодження, згода чи санкціонуванняна отримання, знищення чи передачу інформації третім особам.Авторизація повинна охоплювати всі дії з комерційною інформацією або чітко вказувати на конкретні дії захисту від промислового шпигунства. А тому, якщо роботодавець надав працівникові компанії доступ до комерційної таємниці в процесі виконання останнім своїх професійних функцій, працівник усе одно буде підлягати кримінальній відповідальності в контексті промислового шпигунства, якщо він, скажімо, власноруч передасть цю інформацію іншим особам.

Далі, § 1831 КК США передбачає дві відмінні вимоги щодо встановленнявнутрішнього психічного ставлення винного до свого діяння. Згідноз першою вимогою заволодіння інформацією відбувається із наміром, усвідомлено. Тобто винна особа повинна усвідомлювати, що заволодіваєв контексті промислового шпигунства інформацією, яка є чужою власністю, і водночас не має права обертати їїна свою користь. Друга вимога стосується обізнаності винного про те, щовін заволодіває саме комерційною таємницею. Таким чином, у разі, якщоособа привласнює комерційну таємницю внаслідок незнання, помилкичи випадку, вона не підлягатиме кримінальній відповідальності за аналізованоюзабороною. Повертаючись до законодавчої

історії параграфу, необхідно зазначити, що американський Конгрес не побачив проблем ізустановленням факту обізнаності винного про сутність захисту від промислового шпигунства комерційної таємниці. Адже в переважній більшості випадків самі компанії зацікавлені впоширенні режиму секретності на відповідні об'єкти - шляхом уведенняпроцедур захисту документообігу, затвердження заходів безпеки, укладанняконфіденційних угод із працівниками. Ці та подібні кроки слугують своєрідним захисним бар'єромна шляху потенційних зловмисників та водночас виступатимуть доказомпорушення режиму секретності в разі незаконного заволодіння комерційноютаємницею в контексті промислового шпигунства.

У контексті аналізу особливостей застосування § 1831 КК США у судовійпрактиці доречно звернутися до фактів резонансної кримінальноїсправи, пов'язаної зі спробою передати конкурентам конфіденційнукомерційну інформацію про діяльність усесвітньо відомої компанії«Coca-Cola». Як слідує з обставин справи, один із працівників цієї компаніївикрав засекречені документи, а також декілька зразків її продукції йпередав їх своєму другові з метою подальшої реалізації злочинної схеми зпродажу цих матеріалів. Зловмисники надіслали лист з пропозицієюпридбати секретну інформацію віце-президентові конкуруючої компанії«Pepsi». У «Pepsi» запідозрили протиправну поведінку й переслали листкерівництву компанії «Coca-Cola», яке, у свою чергу, передало його ФБР. Агенти ФБР провели спеціальну операцію, у якій один із агентів видавсебе за представника компанії «Pepsi». Федеральне розслідування показало, що в цій протиправній схемі були задіяні три особи, причому одна зних була інсайдером компанії «Coca-Cola». Зловмисники затребували 1,5млн. дол. США за передачу 20 конфіденційних матеріалів, у тому числі зразок продукту - безалкогольного напою. Компанія «Coca-Cola» офіційно підтвердила, що ці матеріали утворюють захищену комерційну таємницю. Успішне кримінальне розслідування діяльності злочинної групи сприяловинесенню обвинувального

вироку: усіх трьох співучасників було засудженодо позбавлення волі на строк від 2 до 8 років [10].

Наведена кримінальна справа може слугувати вдалим прикладомрозслідування протиправної діяльності в контексті промислового шпигунства, яке проводитьсяза принципом «на випередження» стосовно настання потенційнихсуспільно-небезпечних наслідків. Розслідування, здійснюване безпосередньо«у процесі» поступової реалізації порушником свого злочинногоумислу, у подальшому сприяєоб'єктивному судовому розгляду кримінальноїсправи й винесенню обґрунтованого вироку.

Проаналізувавши норми чинного законодавства, які передбачають правомірність окремих випадків отримання (збирання, ознайомлення) з метою використання, а так само використання відомостей, що становлять комерційну таємницю (зокрема з боку працівників міліції, адвокатів, аудиторів, податкових інспекторів), Е.О. Радутний робить слушне застереженняпро те, що такі випадки потрібно відрізняти від злочинного посягання на відносини з охорони комерційної таємниці, адже тут ідеться про легітимні основи отримання й використання відповідних відомостей. Отже, саме незаконний характер промислового шпигунстванадає збиранню або використанню те соціальне забарвлення, яке є необхіднім для визнання вчиненого діяння правопорушенням. Водночас кримінальне переслідування може мати місце тільки при незаконному збиранні й незаконному використанні відомостей, що становлять комерційну таємницю.

Ознайомлення з офіційним текстом § 1831 КК США наводить до думкипро те, що для безпосереднього опису форм і способів скоєння цьогопротиправного діяння американський законодавець використовує арсеналпонять, чимало з яких є занадто близькими за змістом до промислового шпигунства. Їх перелік указуєна казуїстичну, часом навіть заплутану природу описання способівзловживань із комерційною таємницею.

Цілком справедливо припустити, що вітчизняним криміналістам такий занадто деталізований підхід наврядчи стане в нагоді.І.А. Клепицький

справедливо вказує на те, що закони, які визначаютьрежим різних захисту від промислового шпигунстваємниць, зазвичай деталізують коло адресатів заборони. Якщо особа отримала доступ до секретних відомостей при інших обставинахі в іншій якості, ніж прямо зазначено в цих законах, - вона зобов'язана зберігати таємницю через дію загального припису ч. 2 ст. 183КК РФ, якщо таємниця була йому «довірена або стала відома по службіабо роботі». При цьому формулювання «по службі або роботі» слід розумітив найширшому сенсі. Це формулювання, на думку автора, повинноохоплювати не тільки учасників трудових і службових відносин, а й працюпідприємців, адвокатів і т.д. [69].

Видається, що й у складі розголошення комерційної таємниці (ст. 232 КК України) формулювання «таємниця відома у зв'язку з професійноюабо службовою діяльністю»повинна отримувати поширювальну інтерпретаціюз боку правозастосовувача й має охоплювати, зокрема, випадкичасткового заволодіння чутливою комерційною таємницею в контексті промислового шпигунства та випадковеотримання доступу до неї з боку осіб, які лише опосередковано чи тимчасовомали професійні відносини з юридичною особою - власником комерційноїтаємниці.

Звертає на себе увагу й та обставина, що в США дія заборони пропромислове шпигунство поширюється як безпосередньо на громадянСША, так і на іноземних осіб - нерезидентів. Більше того, цей параграфпо суті сконструйований під злочини іноземців, що в американському нормативному полі трапляється рідко. Санкції за скоєння промислового шпигунства будь-якій з перелічених його форм є досить суворими й передбачають кримінальний штраф у розмірі до 5 млн. дол. та (або) позбавлення волі на строк до 15 років. Для організацій передбачене покарання у вигляді штрафу до 10 млн. дол. Чи в розмірі потрійної вартості викраденої комерційної таємниці (уключаючи витрати на дослідницьку, дизайнерську діяльність та інші витрати навідтворення засекреченого об'єкта, яких винна організація уникла) [69].

Тепер із позицій теорії та практики розглянемо іншу федеральну заборону, покликану охороняти режим захисту від промислового шпигунства комерційної таємниці в американському діловому середовищі. § 1832 Глави 90 КК США із офіційною назвою«Викрадення торгових секретів» містить підстави кримінальної відповідальностіза незаконне використання засекреченої комерційної інформації- у цьому випадку вже на території США. Дія параграфу поширюєтьсяна будь-яку особу, яка, діючи з наміром незаконно привласнити комерційну таємницю, що стосується товару чи послуги в міжнародномучи національному обігу, на користь будь-якої іншої особи окрімвласника, знаючи чи бажаючи заподіяти шкоду власникові комерційноїтаємниці, свідомо:

1) викрадає, або без дозволу привласнює, приймає, забирає або приховує чи шляхом шахрайства, хитрощів або обмануотримує таку інформацію;

2) без дозволу копіює, дублює, робить начерк, малюнок, фотографію, скачує, завантажує, змінює, знищує, робить фотокопію, повторює, передає, доставляє, відправляє, надсилає поштою, уснопередає чи повідомляє таку інформацію;

3) отримує, придбаває або володієтакою інформацією, знаючи, що вона викрадена або привласнена, отримана або обернена на свою користь без дозволу;

4) намагається вчинитибудь-яке правопорушення, зазначене в пунктах із 1 по 3; або

5) вступає в змовуз однією чи більше особами з метою вчинити будь-який злочин, описанийу ч. 1-3, і такі особи вчиняють будь-яку дію із метою досягнення мети змови.

Спостерігаємо подібний до передбаченого в попередньому параграфі детальнийперелік способів та форм протиправної поведінки. Покарання за злочин, передбачений § 1832, є меншим порівняно із санкціямив складі § 1831 – «лише» до 10 років позбавлення волі для фізичнихосіб та до 5 млн. дол. для організацій. Слід додати, що для фізичних осіб - порушників також передбачено кримінальний штраф, однак із незрозумілихпричин його розмір у цьому параграфі не розкривається. При всьому цьомужорсткість санкцій,

передбачених обома федеральними заборонами, значновища за покарання у вигляді штрафу, наразі запропоновані вітчизнянимзаконодавством у ст.ст. 231 та 232 КК України.§ 1832 є змістовно ширшимпорівняно з нормою про промислове шпигунство, оскільки тут відсутня законодавча вказівка на скоєння протиправнихдій на користь іноземного одержувача інформації. Водночастут вимагається, щоб комерційна таємниця стосувалася саме продукту чипослуги, що використовуються (або які планується використати) урядомштату чи іноземним урядом [69].

Як бачимо, вартісний підхід до розуміння інформації, що містить комерційну таємницю в контексті промислового шпигунства, притаманний як правозастосовній практиці України, так і США. С.О. Харламова слушно додає, що суб'єктивна сторона незаконного збирання відомостей, що становлять комерційну або банківську таємницю, характеризується прямим умислом зі спеціальною метою – розголошення чи іншого використання. При цьому винна особа усвідомлює: вона незаконно використовує відомості, що становлять комерційну або банківську таємницю, тобто використовує їх з порушенням законодавства, що регламентує використання конфіденційної інформації, чи використовує відомості, здобуті незаконним шляхом. Що ж до наслідків незаконних дій з відомостями, що становлять комерційну або банківську таємницю, у вигляді заподіяння істотної шкоди суб'єктові господарської діяльностіяк результат промислового шпигунства,то умисел може бути як прямим, так і непрямим. Розголошеннякомерційної або банківської таємниці з суб'єктивної сторони характеризується прямим умислом, корисливим мотивом та іншою особистою зацікавленістю [69].

На думку Є.В. Тітомера, указана в ст. 231 КК України мета діяння не в усіх випадках передбачає бажання винної особи настання наслідку саме у вигляді істотної шкоди, заподіяної суб'єкту господарської діяльності. Автор підтримує позицію О.С. Харламовоїпро те, що вчинення зазначеного злочину можливо як із прямим, так і непрямим умислом. Указується на дві можливі

моделі суб'єктивної сторони вказаного діянняв контексті промислового шпигунства:

1) винна особа незаконно збирає відомості, що становлять таємницю, маючи намір їх розголосити або використати іншим чином, і бажає завдання істотної шкоди суб'єкту господарської діяльності;

2) винна особа незаконно збирає відомості, що становлять таємницю, бажаючи їх розголосити або використати іншим чином, і при цьому свідомо припускає або байдуже ставиться до можливого спричинення істотної шкоди суб'єкту господарської діяльності [26, с. 354-355].

Доречне звернення до положень американського кримінального законодавства свідчить про відсутність в американського Конгресу прагнення закріпити вимогу про усвідомлення винним правового змісту терміна «комерційна таємниця», закріпленого в ч. 3 § 1839 КК США. У такому разі межі застосування заборони істотно б звузилися, що явно б йшло у розріз з метою федерального законодавця. Більше того, обвинувачення не повинно встановлювати, що винний знав про незаконність своїх дій. Головне довести, що з урахуванням професійних відносин між компанією-роботодавцем та її найманим працівником останньому був закритий (чи обмежений) доступ до інформації, що становить комерційну таємницю. При цьому необхідно визначити, що працівник знав або повинен був знати про існування такої заборони (обмеження). Тут маємо можливість спостерігати за властивим американському кримінальному праву прагматичним підходом у частині притягнення до кримінальної відповідальності: рівень (стандарт) установлення вини за допомогою офіційного тлумачення положень кримінального закону спеціально понижується зрівня обізнаності про однозначну протиправність своєї поведінки до рівня розуміння неправильності (некоректності) професійної поведінки в корпоративному середовищі. Спрацьовує класичне правило: незнання закону не звільняє від відповідальності. Як бачимо, тут простежуються принципово схожі, хоча й дещо відмінні змістовно, підходи в

Україні та США до встановлення інтелектуальної ознаки винив контексті захисту комерційної таємниці від проявів промислового шпигунства.

Розглянемо правове регулювання протидії та боротьби з проявами промислового шпигунства в країнах Європи (на прикладі Республіки Польща). Промислове шпигунство загрожує такимоб'єктам права інтелектуальної власності, як винаходи, товарні знаки, корисні моделі та промислові зразки. Чечерскі М. зазначає, що право на захист на товарного знаку і промислового зразку, що надано Патентнимвідомством, забезпечує захист на території Польщі. Тим не менш, реєстрації торгової марки чи промислового зразку в ОНІМ (Бюро з гармонізації внутрішнього ринку) є ефективним на всій території Європейського Союзу [70]. Отримання патентного захисту винаходів, виданих патентним відомством забезпечує захист на території Польщі. Тим не менш, реєстрації за кордоном в ЄПВ (Європейська патентна організація), якої Польща є членом з 1 березня 2004 р., є ефективною для всієї території Європейського Союзу [70].

У контексті захисту інтелектуальної власності проти промислового шпигунства виступають угоди «ноу-хау». Польське законодавство не дає визначення поняття «ноу-хау». За податковим законодавством, «ноу-хау»– це еквівалентне значення вартості інформації, пов'язаної зі знаннями в технічній, технічно-організаційній або організаційнійгалузі [64, с.210].

Торгівельні таємниці, а власне їх захист, окремо регулюються в кожній з 27 держав-членів ЄС: національні органи влади і закони регулюють їх надання, обсяг, виконання і дію на території країни.Торгівельні таємниці, порушені третіми особами, розглядається в якості елементів цивільного правопорушення. У цьому випадку, коли торгівельні таємниці захищені правами інтелектуальної власності на національному рівні, вони повинні підпадати під дію Директиви ЄС [74], що регулює захист прав інтелектуальної власності. Директива охоплює будь-яке порушення прав інтелектуальної власності, не містить визначення прав інтелектуальної власності. Дія Директиви не обмежується тими правами, які узгоджені на рівні ЄС, оскільки також включає в себе права, що

захищаються як права інтелектуальної власності відповідно до національного законодавства. Таким чином, Директива передбачає тільки мінімальну гармонізації примусових заходів.

Розглянемо правову основу міжнародного характеру та інституційного аспекту захисту від промислового шпигунства. Міжнародний захист промислової власності. Паризька конвенція [31] встановлює заборону чинів недобросовісної комерційної практики (конкуренції) між їїкраїнами-членами; це означає, що будь який прояв конкуренції, що відбувається в конфлікті з добросовісними правилами провадження бізнесу і торгівлі є неприйнятним. Угода TRIPS[52] є однією з найважливіших угод Світової організації торгівлі (СОТ). Необхідною умовою для вступу України до СОТ е обов'язкове виконання угоди TRIPS. Ця угода визнана світовим співтовариством як правовий документ, що охоплює питання, пов'язані з охороною прав на ОІВ, які розглядаються як товар.

Відповідно до вимог частини III Угоди TRIPS «Захист прав інтелектуальної власності» країни-учасниці зобов'язуються забезпечити на своїй території дію таких процедур, які дозволяють здійснювати заходи, що запобігають порушенню законодавства у сфері охорони прав інтелектуальної власності та їх недопущення. Стаття 41 Угоди TRIPS зазначає, що законодавство кожної країни повинно мати норми, що дозволяли б удатися до ефективних дій, спрямованих проти будь-якого порушення прав інтелектуальної власності, включаючи термінові заходи для запобігання порушень і правові санкції на випадок подальших порушень. Угода TRIPS передбачає захист прав інтелектуальної власності за допомогою адміністративних процедур, цивільно-правові способи захисту прав, а також карні процедури і штрафи, що можуть бути застосовані до порушників прав.

Угода з торговельних аспектів прав інтелектуальної власності (ТРІПС) [52] ґрунтується в рамках відповідних положень Паризької конвенції з охорони промислової власності і Бернської конвенції з охорони літературних і художніх творів. Відповідність захисту від промислового шпигунства містить, що містить

положення ТРІПС, передбачає розділ 7 під назвою: захист секретної інформації. Стаття 39 (2) передбачає, що [52]: фізичні та юридичні особи повинні мати можливість перешкоджати тому, щоб інформація, яка законно знаходиться під їх контролем, розголошувалась, збиралась або використовувалась іншими особами без їхньої згоди у такий спосіб, який суперечить чесній комерційній практиці, якщо така інформація:

- є секретною у тому розумінні, що вона як єдине ціле або у точній сукупності та поєднанні її компонентів не є загально відомою або доступною для осіб у колах, що звичайно мають справу з інформацією, про яку йдеться;
- має комерційну цінність через те, що вона є секретною;
- зберігається у секреті внаслідок вжиття за відповідних обставин певних заходів особою, яка законно здійснює контроль за цією інформацією.

Європейська система захисту комерційної таємниці. ЄС не має конкретних правових положень щодо захисту комерційної таємниці та секретної інформації, хоча законодавство в різних країнах Європи вже давно використовує аспекти традиційної системи захисту комерційної таємниці. Деякі держави-члени ЄС, такі як Італія, Німеччина та Болгарія забезпечили надійний захист для комерційної таємниці. Загалом, виплата компенсацій та цивільна відповідальність доступні у Франції, Німеччині, Великобританії тощо.Загалом, більшість держав-членів ЄС не мають окремої системи правового захисту комерційної таємниці. Залежно від правової системи, захист комерційної таємниці здійснюється на основі конкретних положень про захист секретної інформації, захист від недобросовісної конкуренції, а також на основі інших положень договірного права і кримінального права. Наприклад:

- право договору, якщо договір між сторонами спрямований на захист комерційної таємниці за допомогою пункту про конфіденційність, або класифікації безпеки;

- закон про боротьбу з недобросовісною конкуренцією, коли привласнення відбудеться конкурентами, які не мають будь-яких договірних відносин або як результат промислового шпигунства;

- кримінальне право, коли співробітник крадеторгівельні таємниці на підприємстві або бере участь у заходах, які могли б бути розглянуті яевторгнення в приватне життя, електронне шпигунстві тощо.

Стан і форма захисту комерційних (бізнес) таємниці, у тому числі ноу-хау, та законодавства про недопущення корупції та боротьбу з недобросовісною конкуренцією та захист від промислового шпигунства дуже відрізняються в різних державах-членах ЄС. На європейському рівні підприємство може використати посилання на європейську директиву щодо захисту прав інтелектуальної власності (Директива 2004/48 Європейського парламенту / ЕС від 29 квітня 2004 року про захист прав інтелектуальної власності [74], тільки у випадку, коли торгові секрети охороняються у якості прав інтелектуальної власності на національному рівні. Директива щодо захисту прав інтелектуальної власності регламентує правила процедури, що стосується будь-якого порушення прав інтелектуальної власності, відповідно до законодавства Співтовариства та / або за національним законодавством країни ЄС. Ця Директива містить важливі положення і включає в себе джерела, які доступні в цивільних судах.

До інших законодавчих актів у сфері європейського захисту прав інтелектуальної власності в контексті промислового шпигунства є:

1. Розпорядження Комісії (ЕС) № 772/2004 від 27 квітня 2004 року про застосування статті 081 (3) Договору (ст. 101 (3) ДФЕС) до категорій угод про передачу технології (TTBER) [72].

2. Положення Комісії - Рекомендації щодо застосування статті 81 Договору про ЄС (стаття 101 TFUE) до угод про передачу технології [73].

3. Гаазька конвенція про договори по вибору умов суду [79].

4. Директива 2005/29 / ЕС Європейського парламенту та Ради від 11 травня 2005 року про прояви недобросовісної комерційної діяльності підприємства

щодо споживачів та про про недобросовісну комерційну практикуна внутрішнього ринку та про внесення змін інших директив. Управління. ЄС від 2005 № 149, стор. 22. [75].

Більшість нормативно-правових актів регламентуються через органи Всесвітньої організації інтелектуальної власності (ВОІВ).
До нормативно-правових актів у сфері боротьби з проявами недобросовісної конкуренції та захисту інтелектуальної власності в контексті промислового шпигунства на території Польщі належать також:

1. Закон від 16 квітня 1993 року про боротьбу з недобросовісною конкуренцією, «Journal» з 2003 року № 153, пункт. 1503 з поправками. [90].
2. Закон від 30 червня 2000 року Про промислову власність, т. У. з 2003 року № 119, пункт. 1117, з поправками. [91].
3. Закон від 23 серпня 2007 року Про боротьбу з недобросовісною комерційною практикою на ринку, «Dz». У. з 2007 року № 171, пункт. 1206, з поправками. [92].

Відповідно до ст. 11 Закону про боротьбу з недобросовісною конкуренцією Польщі чином недобросовісної конкуренції в контексті промислового шпигунства є передача, розголошення або використання чужої секретної інформації або придбання її від несанкціонованого особи, якщо це загрожує або порушує інтереси підприємця. Це положення застосовується також до службовця, який працював на основі трудового чи іншого договору протягом трьох років з моменту його припинення, якщо інше не передбачено договором [90]. П.4 ст.3 зазначеного Закону визначає поняття комерційної таємниці як нерозкритої для суспільного загалу технічної, технологічної, організаційної або іншої інформації підприємства, що має комерційну цінність, по відношенню до котрої підприємець вжив необхідних заходів для підтримки її конфіденційності.

Захист прав інтелектуальної власності щодо боротьби проти промислового шпигунства, пов'язаних з ноу-хау та іншими результатами діяльності у сфері інтелектуальної власності в Польщі,охороняються вище

переліченими нормативно-правовими актами, а також інші в галузі права інтелектуальної власності та захисту від промислового шпигунства. Патентне відомство діє в якості центрального державного органу, відповідального за реалізацію широкого кола завдань, пов'язаних із захистом промислової власності в контексті промислового шпигунства на території Польщі.

2.2. Промислове шпигунство в ЄС: тенденції розвитку та методи його подолання

Історія промислового шпигунства, під яким розуміється таємний, зазвичай незаконний вид діяльності, не тільки нараховує багато століть впродовж існування людства, але й продовжує поповнювати свої сторінки у нашому непростому сучасному світі. Потужна конкурентна боротьба обумовлює активізацію промислового шпигунства в різних формах його прояву, тому що головним його мотивом є прибуток конкуруючих фірм. При цьому слід зазначити, що до промислового шпигунства може бути залучений хто завгодно. Навіть відомий усьому світу автомобільний магнат Генрі Форд, який тривалий час не міг винайти більш простий і дешевий спосіб збирання автомобілів, запозичив принцип побудови конвеєрної лінії для збирання своїх автомобілів у м’ясообробному цеху, коли брав участь у відкритті м’ясопереробного комбінату.

Промислові шпигуни займаються шантажем службовців, які контролюють конфіденційну інформацію або мають доступ до неї. Вони можуть проникати в корпорацію таємним шляхом з метою викрадення, перезнімання (фотографування) певних даних або встановлення пристроїв для підслуховування.

Агенти шпигунства в корпораціях або в масштабах країни, насамперед, намагаються скомпрометувати потрібних осіб, використовуючи звичайні людські слабкості такі, наприклад, як жадібність та інтимний зв'язок. При цьому останній уважається найбільш швидким способом компрометації

службовця. Компрометуючий матеріал може мати форму відеозапису або знімків. Показуючи такі записи та знімки службовцю, його залякують юридичними і соціальними наслідками та труднощами на роботі у випадку розголошення цих матеріалів. Якщо службовець одружений, його залякують викриттям перед дружиною.

Послуги зрадництва службовців можуть оплачуватися грошима, улаштуванням канікул і іншими матеріальними благами. У разі, коли така тактика не спрацьовує, застосовується впровадження таємних агентів або нелегальне проникнення в потрібне приміщення (офіс).

Як показує дійсність, промислове шпигунствотриває й у наші дні. Озброєння й фармацевтика, транспорт, зв'язок і сільське господарство, харчова промисловість і вища освіта. Практично всі сфери економіки страждають від шпигунства. Від нього неможливо заховатися. Навіть стратегічні компанії, діяльність яких має змішаний (подвійний), воєнно-цивільний характер, недостатньо захищені від подібного роду загроз.

Так, у 2014 році ЗМІ приділяли багато уваги компанії «Snecma» — європейському лідерові у сфері авіаційних двигунів. Однак у пресу — і це насторожує — так і не поширилося жодної інформації про неприємності її дочірнього підприємства «Messier-Dowty», яка стала жертвою однієї загадкової події. Завод «Messier-Dowty», розташований у Бідосі (департамент Атлантичні Піренеї, Франція), домінує на світовому ринку колісних шасі й обслуговує як цивільну, так і військову авіацію. 2013 року раптово зникли дві деталі шасі останньої моделі бойового літака, що належали концерну «Dassault». Ця модель — «RafaleMarine» — незабаром повинна була надійти на озброєння французького флоту, і деталі, які зникли, а саме: кесон і поворотна стійка переднього шасі, відносилися до розряду стратегічних[77, с.14].

Ще один випадок. Французькі спецслужби реєструють всі переговори, які американські бізнесмени проводять із борта літаків «AirFrance» під час перельоту між Нью-Йорком і Парижем. Цікавляться вони й змістом телефонних переговорів і факсових передач, які здійснюються з території самої країни.

Деякі паризькі готелі обладнані найдосконалішими електронними «жучками», а спеціально вимуштруваний обслуговуючий персонал таких готелів натренований, щоб «випадково» заглядати в кейси з документами[87].

Починаючи з 50-х років минулого століття японський уряд щорічно спонсорує ділові закордонні поїздки більш ніж 10 тис. своїх бізнесменів до країн Європи, не останньою метою яких є збір комерційної інформації. Передбачається, що на ці цілі витрачається до 80% всіх коштів, що виділяються для японських спецслужб. Із грошей, що залишаються, фінансується моніторинг європейських бізнесменів, що відвідують із діловими візитами Японію. Координацією збору й розподілом комерційної інформації займається Зовнішньоторговельна організація Японії, що має представництва в 59 країнах світу, і міністерство міжнародної торгівлі й промисловості.

За 2015 р. у Німеччині було зареєстровано 96 тис. випадків промислового шпигунства, що на 18% перевищило результати попереднього року, а тільки доведений збиток за цими злочинами перевищив 6 млрд. євро — такі невтішні підсумки, підбиті німецькою федеральною службою кримінальної поліції (BKA). Втім, офіційно доведений збиток становить лише малу частину від реальних збитків, понесених економікою країни, — за оцінками тієї ж BKA, справжні розміри втрат, нанесених промисловими шпигунами німецьким компаніям, склали близько 25 млрд. євро — це майже удвічі перевищує витрати німецького федерального бюджету на освіту і порівнюється з федеральним оборонним бюджетом[87].

Від китайських промислових шпигунів сьогодні страждають багато європейських держав. Так, у Франції, за даними місцевих правоохоронних органів, за останні два роки різко зросла шпигунська активність іноземних компаній і розвідок. Громадянка Китаю, проходячи практику в компанії «Valeo», що спеціалізується на виробництві автомобільних запчастин, починаючи з 2012 р. копіювала закриту внутрішню інформацію для передання її одній з китайських компаній. При затримці у практикантки була виявлена значна кількість ксероскопійованих технічних матеріалів, а також кілька дисків,

повністю заповнених файлами, скопійованими зі службових комп'ютерів «Valeo» [78].

Зі схожими проблемами зіштовхуються й британські компанії. Відповідно до заяви, розміщеній на сайті британської контррозвідки «MI5», промислове шпигунство є однією з трьох найбільших сучасних загроз британської безпеки. «Сьогодні набагато більше, ніж у минулому, розвідслужби спрямовують зусилля на комерційні підприємства, — говориться в офіційній заяві MI5. — Щонайменше 20 іноземних розвідслужб у якоюсь мірою діють проти інтересів З'єднаного Королівства. Найбільшу заклопотаність викликають дії російської та китайської розвідок».

Наведені факти промислового шпигунства не можуть не викликати тривоги. Його головною причиною служить величезний вплив, який шпигунство може здійснювати на економічну міць країни у сучасному світі. Як уряди, так і окремі компанії прагнуть не відстати від інших або заволодіти їх секретами виробництва. У наші дні шпигунство є складовою боротьби за вплив, тому промислове шпигунство в широких масштабах — неминуче.

Однією з цілей промислового шпигунства є виробництво підроблених і контрафактних товарів. Найбільше порушення прав інтелектуальної власності в цій галузі, ми можемо побачити на прикладі[68]:

1. Банкноти € 50. У 2015 році Європейський центральний банк опублікував дані про кількість підроблених банкнот євро. Найбільш популярними серед фальшивомонетників були банкноти 50 €. З підроблених банкнот євро кількість банкнот в € 50 склала 43,5%, ще однією з найпопулярніших фальшивих банкнот були номінали в 20 € і 100 €. У першій половині 2015 року в цілому 317 тисяч підроблених банкнот євро було вилучено з обігу. Таким чином, кількість підробок, вилучених з обігу в період з січня по червень 2015 була на 26,3% вище, ніж сума за той же період в 2014 році, і на 13,2% вище, ніж сума відновлення протягом шести місяців до січня 2015 р.(табл. 2.1, 2.2).

Таблиця 2.1

Показник кількості фальшивих купюр у світі (2012-2015 р.р.)

(Складено автором на основі [68])

Період	2012/1	2012/2	2013/1	2013/2	2014/1	2014/2	2015/1
Кількість	387,000	364,000	296,000	310,000	251,000	280,000	317,000

Таблиця 2.2

Відсоткове значення та номінали в загальній кількості фальшивих купюр вилучених з обігу у першому півріччі 2015 р. (Складено автором на основі [68])

Номінал	€5	€10	€20	€50	€100	€200	€500
Показник	0.3%	2.6%	38.0%	44.1%	12.4%	2.0%	0.6%

Як бачимо з наведених вище талб. 2.1 та табл. 2.2 , банкноти номіналами в € 20 € 50 найбільш активно підроблялися у вказаний період. Протягом останніх шести місяців тенденція підроблених банкнот € 20 зменшилася і частка € 50 банкнот збільшилася незначною мірою. Ці дві позиції в сукупності склали 82,1% від загального обсягу в першій половині 2015 року, а банкноти номіналом 100 € - 12,4% від загальної суми. Кількість підроблення інших банкнот (€ 5, 10 €, 200 € і 500 €) є дуже низькою.

2. Сумки «LouisVuitton». Ціна оригіналу: від 650 дол. США. Ціна підробки: 100 дол. США. За неофіційними даними маркетологів тільки 1% продукції, прикрашених монограмою «LV» не є підробкою. Згідно з даними офіційного будинку моди, близько 15 мільйонів євро щорічно витрачається в боротьбу з контрафактною продукцією.

3. «UGG» чоботи. Ціна оригіналу: від 120 дол. США. Ціна підробки 40 дол. США. Найбільша партія з «сірих» товарів, яка обіймала 244 тис. пар різних черевиків «UGG» моделей і кольорів, була затримана в Китаї. У Європі конфіскація фальшивих «UGG «виросла на 245%. Власники марки привели до

закриття 4783 сайтів, які торгували підробками, і усунули з сервісу «eBay» і «Amazon» понад 304 000 оголошень.

4. Годинники «Rolex» Ціна оригіналу: від 4000 дол. США. Ціна підробки 10 дол. США. Кожного року фірма виробляє близько мільйона примірників годинників «Rolex». Кожен годинник отримує спеціальний сертифікат, виданий «Інститутом швейцарського тестування хронометрів». Кожного року на таємних фабриках в південно-східній Азії виробляється близько 40 млн. годинників «Rolex» - підробок марки міцного – у 2014 р. збиток склав 600 млн.дол. США.

5. Духи «Chanel № 5». Ціна оригіналу: від 95 дол. США за 7,5 м. Ціна підробки: 2000 руб. за 50 мл. Ці духи в 2010 році зайняли перше місце в популярності у Франції і четверте місце в Сполучених штатах. За даними британської групи по боротьбі з контрафактною продукцією, кожен третій покупець на світі стає власником підробних парфумів. Підробні зразки пропонують не тільки індивідуальні продавці, але також великі мережі косметичних магазинів [78].

На думку групи міжнародних корпорацій, які є частиною «Бізнес у боротьбі з контрафактом і піратством» (BASCAP), Міжнародної торгової палати (МТП), Росія і Китай є лідерами у виробництві контрафактної та піратської продукції. Приблизно 2/3 всіх контрафактних і піратських товарів, конфіскованих в Європейському Союзі, зроблено в Китаї. На другому місці знаходиться Росія. Меншою мірою зазначені такі держави у виробництві контрафактної продукції: Індія, Бразилія, Індонезія, В'єтнам і Пакистан. Найменша кількість підроблених товарів в США, Канаді, Японії і Західній Європі.

Незаконне копіювання продукції також є одним з головних перешкод на шляху вступу Росії до СОТ. Матеріальний збиток від реалізації контрафактної та піратської продукції з порушенням прав інтелектуальної власності та авторського права, приводяться за даними Всесвітньої організації інтелектуальної власності в розмірі близько 100 млрд. дол.. США на рік.

Організація «Бізнес в боротьбі з контрафактом і піратством», яка включає в себе корпорації, такі як «GeneralElectric», «VivendiUniversal», «EMI Group» і «Microsoft», представляє інтереси великих транснаціональних корпорацій в боротьбі проти контрабанди та підробок. «BASCAP» зазначає основні висновки своєї доповіді: за даними 2015 року, загальна економічна вартість контрафактної та піратської продукції еквівалентна 650 млрд. дол.. США на рік; близько 2,5 млн. робочих місць були ліквідовано через контрафакцію та піратство[78]. Важко оцінити розмір глобального ринку контрафактної продукції, у тому числі незаконної «чорний» ринок. Недавнє дослідження, проведене «GlobalIntelligenceAlliance», має своїм висновком той факт, що чини розвідувальної діяльності (у тому числі - промислового шпигунства), не залишають сумнівів у його зростаючому значенні в діяльності компаній і підприємств. Серед опитаних 989 великих і середніх компаній, що працюють на глобальному рівні, 76% заявили, що систематично проводить економіку розвідку. 93% всіх опитаних компаній зізналися, що вони використовують результати розвідувальної діяльності, і 78% показали, що їхні інвестиції направляються до розвідувальної діяльності. Серед персоналу досліджених підприємств з інформацією, отриманою від розвідки, працює в середньому більш ніж 700 співробітників, а більше, ніж 100 працівників активно бере участь в отриманні інформації [78]. Наведені вище результати дослідження показують, що боротьба проти промислового шпигунства є актуальним завданням будь-якого підприємства, компанії або навіть країни і міжнародної економіки.

У Великобританії постійно розширюється і диференціюється попит на послуги приватних розшукових агентств, які здатні виконати специфічні завдання, що вважаються незаконними для державних правоохоронних органів. Так, агентство «Argen», поряд із розслідуванням справ про промислове шпигунство, забезпеченням заходів безпеки фірм і банків, займається також добуванням конфіденційної інформації про конкурентів або інших приватних підприємств [71].

У цілому до кола питань, що вирішуються британськими приватними агентствами та службами безпеки, насамперед входять: розслідування злочинів, пов'язаних із комп'ютерними системами і шахрайством, забезпечення перевірки та безпеки службових приміщень; виявлення спеціальної техніки, підслуховувальних пристроїв; організація особистої охорони клієнтів і працівників фірм. За даними експертів, тільки з питань безпеки банківських операцій можна виокремити до 18 різновидів протизаконних операцій [5, с. 145]. Цим видам комп'ютерних маніпуляцій сьогодні приділяється особлива увага, оскільки традиційними методами їх складно виявити. До цих видів припинення комп'ютерних злочинів належать: боротьба з шахрайством у сфері електронного переказу вкладів, виявлення махінацій з наданих вкладів; заходи безпеки щодо забезпечення збереження вкладів.

Однією з дієвих форм і приватної, і загальної профілактики та викриття злочинів у Великобританії уважається виплата грошових винагород за надання інформації.

Так, тільки 2015 р. банки Лондона виплатили близько 150 тис. ф. ст. громадянам як винагороду [5, с. 23]. Загальна профілактика охоплює сукупність заходів політичного, економічного, правового, організаційно-ідеологічного характеру на рівні корпорації, фірми, підприємства як об'єкта економічної безпеки.

Свідченням цього є насичення ринку Англії спеціальною технікою для забезпечення безпеки діяльності суб'єктів господарювання, починаючи від броньованих лімузинів і завершуючи мініатюрними підслуховувальними пристроями, також характерною рисою для безпекодіяльності господарюючих суб'єктів є підвищена увага англійських бізнесменів до підбору, перевірки та випробування кадрів для роботи в комерційних структурах, на промислових об'єктах, особливо в службах безпеки бізнесу.

Розглядаючи німецький досвід адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання в контексті промислового шпигунства, слід констатувати, що в цей час державні установи, банки,

концерни, промислові асоціації та приватні господарські компанії Німеччини поряд із використанням власних і самостійних детективно-охоронних агентств активно застосовують національні спеціальні служби для вирішення пріоритетних економічних проблем шляхом створення сучасних контррозвідувальних структур, що виконують функції підрозділів безпеки та охорони. Цікаво, що створені за ініціативою і за підтримки спецслужб, детективно-охоронні фірми та агентства, служби безпеки виконують певну частину оперативно-розшукової діяльності. Вони підтримують регулярні контакти і обмінюються оперативно значущою інформацією з органами поліції і контррозвідки, в деяких випадках здійснюючи навіть спільні заходи. Така діяльність зовсім не характерна, наприклад, для служб безпеки в США і Великобританії, а також України.

Проте є й низка проблем. Так, зосередження поліції ФРН на її ключових завданнях у зв'язку зі скороченням персоналу створює дефіцит запобігання злочинності та сприяє зростанню значення співробітництва з приватними службами, які визнані невід'ємною складовою внутрішньої безпеки і беруть участь у забезпеченні правопорядку, безпеці руху, діють у місцях виконання покарання. Поліція ФРН вимушена укладати договори про кооперацію з приватними службами безпеки, хоч вона більше зацікавлена в розширенні діяльності «добровільної поліцейської служби», яку вважає дешевшою, ніж послуги приватних служб безпеки. Це одна з причин того, що в дискусії про «нову архітектуру безпеки» в Німеччині приватні служби безпеки відсутні. Також слід зазначити, що державні правоохоронні органи в Німеччині і в Україні, «приватизувавши» забезпечення громадської безпеки і запобігання злочинності, не охоче сприяють приватним структурам у реалізації їх послуг. Приватні служби справедливо дорікають державі за те, що вони відсутні в загальній концепції безпеки для Німеччини [5, с. 227].

З огляду на характерні особливості, у Німеччині можна виділити дві великі групи приватних служб безпеки :

– агентства, що надають фірмам і підприємствам, банкам і державним установам комплекс детективно-охоронних послуг із забезпечення безпеки діяльності суб'єктів господарювання, майна та фізичний захист співробітників в контексті промислового шпигунства;

– служби та підрозділи власної (внутрішньої) системи захисту від промислового шпигунства, створені приватними підприємствами і фірмами.

Функції детективних і охоронних бюро Німеччини в цілому охоплюються традиційними рамками, однак мають чимало специфічних особливостей. Так, у зв'язку з переходом країн Східної Європи, безпосередніх сусідів Німеччини, до ринкового ведення господарства, відсутністю будь-яких обмежень у законодавстві країни на створення спільних акціонерних товариств за участю іноземного капіталу і його частки, особлива увага приділяється вивченню іноземців, які прибувають у країну для ведення власного бізнесу.

Проблеми безпеки економічної діяльності на території Німеччини посідають істотне місце. З цього питання складаються спеціальні домовленості, які суворо і педантично дотримуються упродовж усього періоду функціонування спільного підприємства. Іноземці, які працюють у спільних компаніях, постійно вивчаються і знаходяться в полі зору служб безпеки. До цієї діяльності залучаються підрозділи розвідувальної служби ФРН, кримінальної поліції, митної служби та прикордонних військ. Це питання знаходиться під постійною увагою розвідки, МЗС ФРН, відомства федерального канцлера.

Ще однією особливістю є те, що для відкриття служби безпеки в Німеччині потрібно спеціальний дозвіл місцевої влади зокрема на укладання контрактів із замовником, підприємством, приватною фірмою. Критерії надійності та безпеки викладаються, як правило, в директивах урядових органів окремих земель ФРН. У дозволі може бути відмовлено, якщо приватна служба безпеки не в змозі забезпечити потрібний професійний рівень безпеки роботи або не має для цього необхідних ресурсів, зокрема фінансових, технічних.

Представники МВС ФРН спільно з співробітниками приватних промислових і комерційних служб безпеки, керівниками окремих фірм і банків прагнуть до оновлення юридичних норм, які б попереджали промислове шпигунство, витік відомостей, що становлять таємницю як у процесі виробничої діяльності фірм, так і за їх взаємодії з державними, найперше іноземними установами. Також удосконалюється законодавство про відповідальність осіб, які допустили витік відомостей, що становлять комерційну таємницю. Отож, німецьке законодавство сьогодні в сфері адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання достатньо всебічно і комплексно захищає виробничу, комерційну, банківську і податкову таємницю від несанкціонованого розголошення в контексті промислового шпигунства.

У випадку ж розголошення таємниці передбачено покарання строком до трьох років або грошовий штраф. Крім того, закон передбачає відповідальність за розголошування таємниці тієї особи, а також міру відповідальності осіб, що допустили витік цієї інформації.

Окрім покарання, винуватці зобов'язані відшкодувати потерпілій стороні збитки, що виникли у результаті розголошування таємності фірми. Сума збитку може сягати дуже великих розмірів. Злочином вважається також підбурювання або співпраця у розголошуванні комерційної або виробничої таємниці, примусове здійснення таких дій.

На відміну від Німеччини, у Португалії взаємовідносини приватних служб безпеки з державними правоохоронними органами більш координовані. Так, у Португалії, з метою забезпечення відповідної діяльності служб приватної безпеки, діє Рада приватної безпеки (РПБ).

Вивчаючи особливості служб безпеки недержавної правоохоронної діяльності в сфері адміністративно-правового забезпечення діяльності суб'єктів господарювання у Франції, слід констатувати, що для неї у цьому напрямі характерною особливістю є стрімке нарощування діяльності зазначених служб у промислово-торговельних компаніях і фінансових інститутах.

Як свідчить практика, створення приватних служб безпеки відображає потребу національних ділових кіл у зменшенні комерційних ризиків, особливо під час роботи на слабо вивчених ринках, підвищення безпеки господарської діяльності а останніми роками і особистої безпеки бізнесменів. Попит на послуги приватних детективів і, охоронних структур зростає з боку приватних осіб, керівників і високопоставлених співробітників комерційних банків, страхових компаній і адвокатських контор.

У процесі подальшого дослідження французького досвіду було також встановлено, що власниками приватних детективних і охоронних бюро можуть бути лише особи, які мають громадянство Франції, або країн Євросоюзу. Колишні співробітники французької поліції можуть стати власниками таких бюро тільки з дозволу міністра внутрішніх справ країни. Цікаво, що останніми роками у Франції виникло серйозне занепокоєння у зв'язку зі значною кількістю колишніх поліцейських, які переходять на роботу в приватні охоронні та детективні компанії.

До слова, така тенденція характерна і для України. У зв'язку з цим у Франції введена обов'язкова реєстрація в МВС приватних детективів, а також повідомлення МВС у випадках найму на роботу осіб зазначеної категорії.

З огляду на географічне положення, традиції і звичаї, близькі мовні системи і норми законодавства країнам Північної Європи (Фінляндія, Норвегія, Швеція і Данія) [11, с. 110] властиві значно спрощені підходи до організації діяльності комерційних і промислових служб безпеки. У цих країнах приватні детективні та охоронні бюро належать до категорії приватних підприємств. Мається на увазі те, що їхня реєстрація, фінансування, оподаткування, правове становище і діяльність регламентуються загальними нормами чинного законодавства.

Зауважимо, що служби безпеки суб'єктів господарювання та місцеві державні правоохоронні органи активно діють через впливові національні спілки підприємців. Уповноважені співробітники спецслужб на підприємствах спільно з кадровим апаратом служб безпеки суб'єктів господарювання

здійснюють кваліфіковану спецперевірку осіб, що допускаються до роботи з таємними документами і матеріалами, створюють агентурну мережу, поширюють серед персоналу досвід контррозвідувального забезпечення закріплених об'єктів в контексті промислового шпигунства. Простежується тенденція до розширення функцій державних і недержавних правоохоронних органів щодо адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання та їх співпраці у процесі формування в них власних груп і служб безпеки.

Пріоритетне значення в країнах Європи останнім часом отримують завдання боротьби з промисловим і комерційним шпигунством. Основна увага приділяється захисту в приватному секторі технологічної інформації, що має військове значення, а також підвищенню режиму таємності. У зв'язку з цим у країнах Північної Європи актуальні питання протидії комп'ютерним злочинам та їх профілактика. Так, наприклад, у звіті «Комп'ютерна безпека Швеції» зазначається, що національні комп'ютерні мережі слабо захищені від випадкових або навмисних зломів, що може призвести до розлаштування більшої частини систем інформаційного забезпечення країни [13, с. 130].

Аналізуючи практичний досвід країн Європи у сфері адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання в контексті промислового шпигунства, слід констатувати, що в цілому в країнах Європи існує тенденція до створення в промислово-торговельних фірмах потужних недержавних правоохоронних органів в особі служб безпеки, їх тісної співпраці з державними правоохоронними органами, з метою підвищення ефективності роботи з попередження правопорушень і злочинів, а також актів промислового шпигунства.

Отож, опанування зарубіжної практики в сфері адміністративно-правового забезпеченням безпеки діяльності суб'єктів господарювання в контексті промислового шпигунствау ринкових умовах, яка має важливе значення для сучасної України, допоможе краще освоїти тонкощі господарської діяльності у жорсткому конкурентному середовищі.

Зазначене також свідчить про те, що міжнародний досвід підтверджує необхідність створення системи служб безпеки недержавної правоохоронної діяльності суб'єктів господарювання для захисту від промислового шпигунства в Україні як закономірного кроку в подальшому розвитку нашого суспільства на ринкових засадах, а також як фактора у зміцненні демократичних принципів в управлінні державою.

2.3. Дослідження розвитку та проблеми подолання промислового шпигунства в Україні

Перейдемо до розгляду актуальних в Україні типів та показників різного роду шахрайств, в тому числі проявів промислового шпигунства. Випадки промислового шпигунства , направлені до України, є поодинокими. Це основні методи, які в свою чергу діляться на декілька способів отримання конфіденційної інформації (дезінформації, шантаж і підкуп, використання правоохоронних органів, хабарництво, корупція, недобросовісна конкуренція).

Згідно з дослідженнями Якубівської Ю.Є. [59-63] про вплив промислового шпигунства на сферу інтелектуальної власності в Україні показано, що економічне і промислове шпигунство на даний час виражаються в двох основних формах:

1. Придбання знань і набуття інтелектуальної власності, такої як інформація про промислове виробництво, ідеї, методи і процеси, рецепти, формули.
2. Отримання матеріального права на об'єкти інтелектуальної власності, інформаційні операції (бази даних по клієнтах, ціноутвореннях, продажах, маркетинзі, проектах, дослідженнях і розвитку, політиці, стратегічному плануванні та маркетингових стратегіях, змінах в складі виробничих дільниць). Цей аспект включає в себе такі злочини, як крадіжки комерційних таємниць, підкуп, шантаж та технічний нагляд. Суб'єктами промислового шпигунства в Україні виступають не тільки підприємства, але й державні організації

(наприклад, для визначення умов тендеру державних закупівель таким чином, що інші учасники в майбутньому зможуть знизити ціну).

Таблиця 2.3

Типи та показники шахрайства в Україні та світі у 2014 р.

(Джерело: Складено автором на основі[53])

Територіальна одиниця	Хабарництво та корупція (%)	Чини недобросовісної конкуренції (в т.ч. промислове шпигунство), (%)
Україна	60	23
Центрально-Східна Європа	36	12
Міжнародний рівень	24	7

Як бачимо з табл.2.3, рівень хабарництва та корупції в Україні є значно вищим від рівня проявів промислового шпигунства. Однак останній показник в Україні (23%) майже втричі вищий ніж у світі (7%).

Інтерес іноземних розвідслужб до української оборонної сфери простежується фактично весь час її існування, причому особливу активність проявляють саме країни Азіатсько-Тихоокеанського регіону. Так, Україна давно опинилася в прицілі такого «світового промислового шпигуна номер один», як Китай. Варто згадати, наприклад, скандал, що виник в червні 2013 року: світові ЗМІ повідомили, що Китай зібрав прототип свого першого палубного винищувача четвертого покоління «J-15», скопіювавши його з російського Су-33. Копія російського винищувача була зібрана на основі одного з перших його прототипів - Т10К, купленого свого часу Китаєм у України. Після того як «J-15» буде запущений в серію, літаки будуть базуватися на китайському авіаносці «ShiLang» [4, с.118]. Саме про подібні погрози і попереджало українську владу експертне співтовариство в 2011-2013 рр., коли Україна декларативно націлилася на прорив у військово-технічному співробітництві з Китаєм. Українській владі варто пам'ятати, що вона повинна обов'язково враховувати усталене «реноме» Китаю як «промислового шпигуна» і любителя незаконного копіювання

іноземних зразків озброєнь і військової техніки, що видобуваються в т.ч. і в рамках військово-технічного співробітництва. Зокрема, загальновідомі приклади копіювання української техніки - наприклад, авіаційної. В даний час воєнно-повітряні сили Китаю мають на озброєнні літаки «Y-7» і «Y-8» - це модернізовані копії українських «Ан-24» і «Ан-12БК» розробки «Антонова».

Як повідомлялося раніше в заяві Генпрокуратури України, прибувши до Дніпропетровська з Мінська і діючи за попередньою змовою, Сонгчель і Тхекіль намагалися завербувати представника КБ Південне. Громадяни КНДР викрили в Україні співробітники СБУ, за повідомленням від працівника КБ Південного, який був звільнений від відповідальності. Шпигунів цікавили секретні дані, що стосуються обладнання ракетно-космічної техніки, зокрема, паливних систем літальних апаратів, - їх і затримали під час фотозйомки наукових дисертацій під грифом «секретно».

Наукові роботи, що потрапили в приціл розвідників, були присвячені новим прогресивним технологіям ракетних комплексів, космічних літальних апаратів, рідинних двигунів, систем постачання ракетного палива, інших ноу-хау. Офіційно в СБУ цю справу не коментували.

В даному випадку розвідувальна діяльність КНДР безпосередньо стосується і Росії. Зокрема, КБ «Південне» як в минулому розробник міжконтинентальних балістичних ракет (деякі з яких залишаються на озброєнні Росії), бере активну участь у спільних україно-російських проектах. Зокрема, це запуски розроблених в КБ «Південне» ракетоносіїв «Зеніт», які здійснює спільне підприємство SeaLaunch, ракетоносіїв «Дніпро», які здійснює спільне російсько-українське підприємство «Космотрас» з космодрому Байконур і РН «Циклон» російсько-українського підприємства МКУ (Міжнародні Космічні Послуги). А значить, в даному випадку організація промислового шпигунства проти України зачіпає і російські інтереси [21, с. 150].

Помітним є пряме промислове шпигунство, здійснюване китайцями в рамках військово-технічного співробітництва. Зокрема, китайці довгий час демонстрували інтерес до наземного випробувально-тренувального комплексу

авіації НИТКА в Криму, і навіть відвідували його по лінії Міноборони. Також у 2012-2013 роках за завданням китайських спецслужб дві групи шпигунів намагалися викрасти технологію будівництва «НИТКА», але СБУ вдалося зірвати ці задуми і затримати зловмисників на місці злочину. Проте, незабаром було повідомлено, що Китай будує аналогічний комплекс на своїй території, на острові Хулудао.

Як раз в контексті цієї історії варто згадати факт: не так давно, взимку 2011 р. широкий резонанс отримала історія з засудженням до 6 років позбавлення волі Олександра Єрмакова, шпигувавшого проти України на користь Китаю по комплексу «НИТКА» і затриманого в 2010 р. Разом з 35-річним сином Олександр Єрмаков зареєстрував в офшорній зоні фірму з надання посередницьких послуг у сфері поставок зброї.

Основним її профілем став збір військово-технічної, експлуатаційної, методичної, науково-технічної інформації, як за власною ініціативою, так і на замовлення. В кінцевому результаті у Єрмакова замовили збір інформації по комплексу «НИТКА» - добути документацію щодо створення полігону, його використання, пообіцявши $ 1 млн, видавши завдаток і забезпечивши фотоапаратами [42].

У липні 2010 г Військовий апеляційний суд Центрального регіону виніс вирок за звинуваченням в шпигунстві старшого полковника Народно-визвольної армії Китаю, ЯоЦзюня, який у якості слухача проходив курси підвищення кваліфікації в українському вищому навчальному закладі. Звільняючи шпигуна від в'язниці, суд пояснив причину звільнення існуванням «пом'якшуючих обставин», не роз'яснивши, однак, якими саме були ці обставини.

Незважаючи на те що, Яо повністю заперечував висунуті в його адресу звинувачення про крадіжку українських секретів, суд визнав що наявні докази повністю підтверджують факт вчинення злочину передбаченого ч.1 статті 114 Кримінального кодексу України (шпигунство). Які саме секретні дані збирав

китайський шпигун, суддя повідомити відмовився, посилаючись на те, що справа розглядалася в «закритому режимі»[42].

Цікаво, що, з одного боку, українські зброярі в цілому розуміють небезпеку передачі в Китай не тільки технологій, але і зразків озброєнь, а також вузлів і агрегатів з тим, що в КНР можуть зайнятися їх копіюванням. Так, на початку серпня 2014 року голова ради директорів українського підприємства з будівництва авіадвигунів «Мотор Січ» В. Богуслаєв заявив, що у підприємства є твердий контракт з Китаєм на придбання двигунів «АИ-22»2 з форсажною камерою для китайського навчально-тренувального літака «L-15». «Контракт передбачає опцію на постачання 200 моторів, але цього не буде. Вони будуть намагатися зробити двигун самі», - сказав тоді Богуслаєв, підкресливши, що «Мотор Січ» виступає категорично проти передачі технології виробництва двигунів в Китай. Між тим, модифікаціями згаданого авіадвигуна оснащуються російські літаки, а модифікація «АІ-222-25» спочатку розроблялася для російського навчально-тренувального літака «Як-130».

З іншого боку, в липні цього року стало відомо, що Україна і Китай готують розширення укладеного в 2014 році контракту на поставку українських силових установок з двигуном «6ТД-2Е 9» потужністю в 1200 к.с. для китайського основного бойового танка» МВТ-2000». За даними, що потрапили в ЗМІ, обсяг нового контракту може скласти не менше 200 силових установок. Як відомо, попередній контакт на поставку в КНР 50 моторно-трансмісійних установок на базі двигуна «6ТД-2Е» обсягом близько 20 мільйонів доларів був укладений ДП «Завод імені Малишева» в серпні 2014 року і став продовженням контракту, укладеного української та китайської сторонами у 2008 році[42].

А паралельно Україна і Пакистан заявили про те, що розширюють співпрацю в програмі створення пакистанського основного бойового танка «Al-Khalid». Зокрема, як стало відомо з джерел на ДП «Завод імені Малишева», за підсумками минулих переговорів керівництва українського бронетанкобудівого заводу і пакистанської «HeavyIndustries», досягнута домовленість про постачання пакистанській стороні великої партії українських силових

установок з двигуном «6ТД-2» для ОБТ «Al-Khalid» . За попередніми даними, «мова йде про постачання більш ніж 100 силових установок в рамках не менш ніж 5-ти річного контракту». При цьому в ході переговорів сторони підтвердили стратегічний статус співробітництва між Україною та Пакистаном в області бронетанкобудування, що стартував успішною реалізацією укладеного у 90-х роках масштабного контракту на поставку Пакистану українських танків «Т-80УД» [55, с.150].

Тобто, в даному випадку ми бачимо інтерес інших країн до українського танкового двигуна, і спроби його закупівлі великою партією з боку Китаю. На даний момент це, безумовно, вигідні контракти. Але, враховуючи попередній сумний досвід, не можна гарантувати, що незабаром на регіональному ринку не з'являться зроблені в КНР копії українських силових установок для бронетехніки, причому більш дешеві (а скоріше - не самі двигуни, а оснащені ними зразки китайської бронетехніки). На жаль, від такого «побічного ефекту» у співпраці з китайцями не застрахований ніхто.

Що цікаво, загроза промислового шпигунства спільним українським проектам у сфері ОПК відзначалася і з боку «цивілізованої» Європи. Яскравий приклад тому - новий військово-транспортний літак «Ан-70». Суть в тому, що історія «співпраці» України з європейськими країнами по проекту цього літака стала, мабуть, самою блискучою операцією розвідок європейських країн проти України в плані промислового шпигунства. Адже, як відомо, в кінці минулого століття впродовж ряду років європейці під обіцянками величезних контрактів із закупівлі українського літака викачували технічну документацію з виробників. В кінцевому підсумку Європа від «Ан-70» відмовилася на користь свого новоявленого проекту «А-400М». Про успіх цієї операції може судити навіть неспеціаліст. Для цього достатньо лише порівняти фотографію українського літака і європейської «альтернативної пропозиції» - просто брати-близнюки.

Наскільки відомо, «роботою» по «Ан-70» військових аташатів (авт. - іноземних розвідників) посольств деяких європейських країн, акредитованих в

Україні, свого часу займалася військова контррозвідка СБУ. Але і хід цих розслідувань, і їх результати Україна не афішувала. Втім, із зрозумілих причин, - важко одночасно говорити про євроінтеграцію, і звинувачувати міжнародну структуру, в яку ми інтегруємося, в банальній крадіжці[55, 149].

Одним з останніх прикладів промислового шпигунства на українському ринку була подія з присутністю російських кондитерів під час огляду фабрики «Рошен», що характеризувалася промисловим шпигунством. Відносно цього випадку міністр аграрної політики і продовольства України висловив невдоволення присутністю представниками російських кондитерських компаній у складі інспекції з Росії при перевірці кондитерської фабрики «Рошен». Варто відзначити, що із дати запровадження на той час заборони на імпорт продуктів «Рошен» в Росію пройшло два з половиною місяці.

Раніше йшла мова про пошук токсичних речовин бензопірену в продуктах виробника. Українська сторона заперечувала це твердження. Російське інформаційне агентство пізніше повідомило, що «...основною причиною невідповідності солодощів є відсутність актуального законодавства у сфері захисту прав споживачів (вимоги до маркування харчових продуктів, невідповідність інформації про поживну цінність продуктів, зазначених на етикетці)» [19]. Проте Росія скасувала запит на непридатність продукції української компанії «Рошен» і наполягала на доступі своїх фахівців до виробництва. Огляд розпочався з Києва - кондитерської корпорації, більш відомої в пострадянських країнах, як кондитерська фабрика «Карла Маркса». Відзначимо, що представники і інспектори мають доступ до всіх видів секретної комерційної інформації[54].

Всі ці випадки показують, наскільки активно діють спецслужби іноземних держав проти військово-промислового потенціалу України. А це, в свою чергу, означає, що Україна, демонструючи курс на відкритість і зміцнення військово-технічної співпраці з іншими країнами, повинна враховувати всі виникаючі ризики, бо в розвідці і бізнесі друзів не буває.

І в більшості випадків нехай навіть мільйонні прибутки від такого співробітництва сьогодні дуже легко здатні звернутися в мільярдні збитки в майбутньому.

Висновки до розділу 2

Порівняльний аналіз окремих аспектів відповідальностіза порушення режиму охорони комерційної таємниці та захисту від промислового шпигунстваУкраїні та світі від протиправних посягань дозволив сформулювати певні висновки. Існуюча правозастосовна практика щодо кримінальних справ про зловживання з відомостями в контексті промислового шпигунства, що становлять комерційну таємницю, чітко вказує на «інтелектуальні» способи скоєння відповідних посягань, переважно із залученням сучасних технологій електронної обробки інформації. Зокрема більшість випадків незаконного заволодіння такими відомостями поєднуються з використанням мережі Інтернет, сервісів електронної пошти, електронних засобів збереження інформації та сканування документації, мобільних пристроїв тощо. Звертають на себе увагу кардинально відмінні в Україні таСША підходи до тлумачення ознак злочинних порушень порядку обігу відомостей в контексті промислового шпигунства.

Росія і Китай є лідерами у виробництві контрафактної та піратської продукції. Приблизно 2/3 всіх контрафактних і піратських товарів, конфіскованих в Європейському Союзі, зроблено в Китаї. На другому місці знаходиться Росія. Найменша кількість підроблених товарів в США, Канаді, Японії і Західній Європі.

РОЗДІЛ ІІІ
УДОСКОНАЛЕННЯ СИСТЕМИ БОРОТЬБИ З ПРОМИСЛОВИМ ШПИГУНСТВОМ В УКРАЇНІ: ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНОГО ДОСВІДУ В НАЦІОНАЛЬНУ ПРАКТИКУ

3.1. Вдосконалення українського законодавства у сфері протидії промисловому шпигунству

Основним об'єктом промислових шпигунів є інформація, причому інформація, основу якої становить комерційна та банківська таємниця. Саме відомості, віднесені до такої категорії інформації, є найбільш цікавими для конкурентів банку і саме вони є об'єктом пильної уваги промислових шпигунів. Сьогодні практично немає чіткого визначення поняття «промислове шпигунство». Існує багато різних форм і методів промислового шпигунства. Але всі вони обумовлені переважно самою природою промислового шпигунства як таємною формою конкурентної боротьби.

Відповідно до чинного законодавства за недобросовісну конкуренцію передбачається адміністративна, цивільна або кримінальна відповідальність. Кримінальна відповідальність передбачена за злочини, що порушують вимоги законодавства про охорону комерційної таємниці, охорону прав на товарний знак, а також за злочини, що пов'язані з досягненням неправомірних переваг у конкуренції. Цивільно-правовою санкцією за недобросовісну конкуренцію є відшкодування збитків. Збитки, заподіяні внаслідок вчинення дій, визначених законом як недобросовісна конкуренція, підлягають відшкодуванню за позовами заінтересованих осіб у порядку, визначеному цивільним законодавством. Адміністративна відповідальність передбачає дві спеціальні санкції за окремі види порушень, що визнаються недобросовісною конкуренцією. Однією з них є вилучення товарів з неправомірно використаними позначками та копій виробів іншого суб'єкта господарювання. Другою - офіційне спростування за рахунок порушника поширених ним

неправдивих, неточних або неповних відомостей у строк і способом, визначеним законодавством. Крім того, згідно зі ст. 164.3 Кодексу України про адміністративні правопорушення у випадках неправомірного використання ділової репутації суб'єкта господарювання, створення йому перешкод у процесі конкуренції та досягнення неправомірних переваг, а також за наявності фактів неправомірного збирання, розголошення та використання комерційної таємниці на порушників може бути накладено штраф у розмірі від п'яти до 44-х неоподатковуваних мінімумів доходів громадян [20].

Рекомендуємо способи захисту прав інтелектуальної власності в контексті проявів промислового шпигунства в Україні:

1.Адміністративні і правові способи захисту. Адміністративний спосіб полягає в вирішенні та розгляді суперечки органом державного управління. Процедура розгляду суттєво простіша, ніж у цивільному судочинстві. Правовою основою є Кодекс України про адміністративні правопорушення, а також закони України: «Про захист від недобросовісної конкуренції», «Про охорону прав на промислові зразки», «Про охорону прав на знаки для товарів і послуг», «Про охорону прав на винаходи і корисні моделі», «Про охорону прав на сорти рослин» тощо[25; 33-41].

Відносно об'єктів промислової власності даний спосіб захисту прав передбачає накладення штрафів за неправомірне використання торгівельних марок, знаків для товарів та послуг, брендів та фірмових (комерційних) найменувань. Засобом захисту в цьому випадку є скарга, яку у встановленому адміністративним законодавством порядку подають у відповідний орган державного управління.

Здійснення дій, обумовлених законодавством України як недобросовісна конкуренція, спричиняє накладення Антимонопольним комітетом України штрафів, а також адміністративну і цивільно-правову відповідальність. До таких дій відносяться:

- неправомірне використання чужого імені, фірмового найменування, торговельних марок;

- введення в обіг під своїм позначенням товару іншого виробника;

- відтворення зовнішнього вигляду виробу іншого суб'єкта господарської діяльності і введення його в господарський оборот;

- неправомірний збір, розголошення і використання комерційної таємниці, а також інші протиправні дії.

Тобто Антимонопольним комітетом України розглядаються скарги щодо дій після вводу об'єктів права інтелектуальної власності до господарського обороту.

Типовими видами адміністративних стягнень можуть бути: попередження, штраф, виправні роботи, адміністративний арешт тощо.

Так, незаконне використання об'єкта права інтелектуальної власності, привласнення авторства на такий об'єкт або інше умисне порушення права інтелектуальної власності тягне за собою накладення штрафу від 10 до 200 неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції, а також обладнання і матеріалів, що призначені для їх виготовлення.

Щоб встановити поле боротьби з недобросовісною конкуренцією в контексті промислового шпигунства на території України законодавством врегульовані:

1. Закон України «Про захист від недобросовісної конкуренції» [35].

2. Закон України «Про Антимонопольний комітет України» [32].

3. Закон України «Прозовнішньоекономічну діяльність» [33].

4. Закон України «Прообмеження монополізму і недопущення недобросовісної конкуренції у підприємницькій діяльності» [34].

Відповідно до ст. 16-19 Закону України «Про захист від недобросовісної конкуренції» актами недобросовісної конкуренції у контексті боротьби проти промислового шпигунства (авт.), є: а) Неправомірне збирання комерційної таємниці; б) Розголошення комерційної таємниці; в) Схилення до розголошення комерційної таємниці; г) Неправомірне використання комерційної таємниці [35]. Вважаємо, що він повинен бути доповненим за змістом терміном

«передача чужої конфіденційної інформації, яка порушує інтереси підприємця», тому що потенційним виникає промислове шпигунство.

Термінологія щодо недобросовісної конкуренції визначена у ст. 1 глави 1 Закону «Про обмеження монополізму і недопущення недобросовісної конкуренції у підприємницькій діяльності» [34]. Проте, Закон [34] визначає сутність категорії «конкуренція», але не подає дефініції значення термінів «недобросовісна конкуренція» та «комерційна таємниця».

Доречно термінологічний аспект українського законодавства у сфері подолання проявів недобросовісної конкуренції удосконалити. Прикладом може бути формулювання ст. 11 закон Республіки Польща від 16 квітня 1993 року «Про боротьбу з недобросовісною конкуренцією» [90], який визначає поняття «комерційної таємниці», як таке, що не розкривається в публічній технічній, технологічній, організаційній документації підприємства або іншої інформації, що має комерційну цінність, конфіденційність якої необхідно зберегти.

2. Цивільно-правовий спосіб захисту. Спори, що пов'язані з порушенням прав інтелектуальної власності в контексті протидії промисловому шпигунству, підпорядковані судам загальної юрисдикції та вищому господарському суду. Якщо хоча б однією зі сторін у суперечці є фізична особа, то зазначена суперечка підвідомча суду загальної юрисдикції.

Власник прав на об’єкти інтелектуальної власності має право вимагати від порушника: визнання прав власника; відновлення положення, що існувало до порушення права; припинення дій, що порушують право чи створюють погрозу його порушенню; відшкодування збитків, включаючи втрачену вигоду тощо.

На наш погляд, враховуючи положення європейського законодавства [12; 19; 23; 31], слід доповнити цей список наступним:

- ліквідувати результати незаконної діяльності;

- повернути незаконно отриманий прибуток на загальних підставах.

Якщо в результаті незаконного використання об’єкта інтелектуальної власності в контексті промислового шпигунства порушник одержав доход, потерпілий має право вимагати відшкодування втраченої вигоди в розмірі не меншому, ніж сума такого доходу.

Якщо одночасно з порушенням майнових прав порушені особисті немайнові права автора, то він може зажадати майнову компенсацію за нанесення йому морального збитку, розмір якої визначається судом. Порушенням прав авторства є присвоєння результатів чужої творчої праці і спроба видати ці результати за власну розробку.

Суд має право прийняти рішення чи визначення про заборону випуску твору, використання постанови, фонограми передачі в ефір чи по проводах, про припинення їхнього поширення, про вилучення, конфіскацію всіх примірників твору, якщо буде досить даних про порушення авторського права і суміжних прав, у тому числі - промислового шпигунства. У Великобританії, Німеччині і низці інших країн функціонують спеціалізовані патентні суди. Це дозволяє вам сконцентруватися досвід в патентній тяжби, щоб створити умови для правильного і однакового застосування правил для того, щоб зменшити кількість випадків, вирішення спорів, в тому числі промислового шпигунства.

В Україні, на жаль, немає патентних судів, але такого роду практика функціонує, наприклад, на Вищому господарському суді України із залученням до розгляду справ суддів, які мають спеціальну підготовку у сфері інтелектуальної власності і тому можуть грамотно вирішити спори, що стосуються інтелектуальної власності та промислового шпигунства. Вважаємо, що формування в Україні спеціалізованих судів у справах інтелектуальної власності матиме своїм результатом позитивні зрушення в контексті зміцнення рівня захисту інтелектуальної власності від проявів промислового шпигунства.

3. Кримінальна відповідальність. Поряд з нормами цивільно-правового захисту прав на об’єкти інтелектуальної власності, чинним законодавством

передбачена також кримінальна відповідальність (ст. 176, 177 Кримінального кодексу України) [17].

Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у значному розмірі, винаходу, корисної моделі, промислового зразка, топографії інтегральної мікросхеми, сорту рослин, раціоналізаторської пропозиції, привласнення авторства на них, або інше умисне порушення права на ці об'єкти в контексті промислового шпигунства, якщо це завдало матеріальної шкоди у значному розмірі, караються штрафом від 200 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років, або позбавленням волі на той самий строк, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

Зазначимо, що у ст. 176 та 177 матеріальна шкода вважається завданою в значному розмірі, якщо її розмір у 20 і більше разів перевищує неоподатковуваний мінімум доходів громадян, у великому розмірі - якщо її розмір у 200 і більше разів перевищує неоподатковуваний мінімум доходів громадян, а завданою в особливо великому розмірі - якщо її розмір у 1000 і більше разів перевищує неоподатковуваний мінімум доходів громадян.

У ст. 23-24. Закону Республіки Польща від 16 квітня 1993 року «Про боротьбу з недобросовісною конкуренцією» [90] сказано: «Той, хто всупереч своїм обов’язкам по відношенню до підприємця, передає іншій особі або використовує у своїй діяльності комерційну таємницю, і якщо це приносить збиток підприємцю, підлягає окладенню штрафом, тюремним ув'язненням або

позбавленням волі на строк до 2 років. Хто, за допомогою технічних засобів репродукування, копіювання зовнішнього вигляду виробу або просто створюючи можливість введення клієнтів в оману щодо виробника чи , власне, продукції, і який заподіює шкоду підприємцеві, накладається штрафом, обмеженням волі або позбавлення волі на строк до 2 років». Вважаємо, що різниця в змісті кримінальної відповідальності залежно від країни виникнення правової та економічної ситуації в області захисту інтелектуальної власності в контексті протидії та боротьби з промисловим шпигунством.

Українське законодавство теж передбачає кримінальні санкції за незаконне порушення комерційної таємниці. Цей злочин незаконний збір інформації є комерційної таємниці (шпигунські), якщо в наслідку чого великої матеріальної шкоди підприємству. Як покарання намір використовувати штраф у розмірі від 200 до 2000 неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від двох до п'яти років більше.

Окремим випадком є захист прав інтелектуальної власності в контексті протидії промисловому шпигунству на кордоні. Митний кодекс України [25] (ст. 74) показує, що Особливий випадок - захист прав на об’єкти інтелектуальної власності в контексті протидії промисловому шпигунству при перетинанні кордону. Митним кодексом України (ст. 74) товари й інші предмети, виготовлені з порушенням прав інтелектуальної власності в контексті промислового шпигунства, не можуть як експортуватися, так й імпортуватися через митний кордон України.

4. Захист прав інтелектуальної власності в контексті протидії промисловому шпигунству відповідно до Угоди ТРІПС [52]. Угода TRIPS є однією з найважливіших угод Світової організації торгівлі (СОТ). Неодмінною умовою для вступу України до СОТ е обов'язкове виконання угоди TRIPS. Ця угода визнана світовим співтовариством як правовий документ, що охоплює питання, пов'язані з охороною прав на об’єкти інтелектуальної власності, в тому числі в контексті промислового шпигунства які розглядаються як товар.

Відповідно до вимог частини III Угоди TRIPS «Захист прав інтелектуальної власності» країни-учасниці зобов'язуються забезпечити на своїй території дію таких процедур, які дозволяють реалізувати заходи, що запобігають порушенню законодавства у сфері охорони прав інтелектуальної власності (у тому числі в контексті протидії промисловому шпигунству)та їх недопущення.

Підсумовуючи все сказане, можна констатувати, що сьогодні в Україні вже сформована організаційна й законодавча системи державних органів, які прямо або опосередковано забезпечують захист прав у сфері інтелектуальної власності в контексті промислового шпигунства.

3.2. Формування системи заходів протидії та боротьби з промисловим шпигунством на підприємстві

Промислове шпигунство є злочином, що полягає в зборі інформації що становить комерційну таємницю і передачі їїконкурентам з тієї ж або в іншій країні. На додаток до економічного шпигунства, часто проводяться спроби промислового шпигунства отримати комерційні таємниці з підприємства, що стосуються технології виробництва чи технічних рішень. Шпигунство може бути попереджено. Якщо керівництво чи служба безпеки знає про чутливу позицію, вразливу для атаки, то може вжити належних захисних заходів. Підприємства України характеризуються наявністю факторів, які не тільки призводять до недобросовісної конкуренції, а й можуть викликати порушення в галузі прав інтелектуальної власності, в тому числі промислового шпигунства. На думку автора, можна визначити наступні фактори, що викликають загрозу і запропонувати ряд відповідних рекомендацій з профілактики та контролю промислового шпигунства на підприємстві:

1. Проводити інвентаризацію інформаційних ресурсів. Інформацію, яку варто захищати в контексті промислового шпигунства можна класифікувати наступним чином:

- державна таємниця;
- комерційна таємниця;
- інформація бухгалтерії й кадрової служби;
- важлива інформація окремих співробітників;
- технологічна інформація;
- бази даних і знань;
- know-how;
- аналітична інформація;
- результати наукових досліджень.

Основний обов'язок технічного персоналу становить в забезпеченні функціонування корпоративної мережі захисту від промислового шпигунства. За захищеність інформації вони відповідальності не несуть. Ця задача вирішується, у найкращому разі, у межах забезпечення захисту функціонування ресурсів і технологій на прийнятному для них рівні.

2. Проводити інвентаризацію всіх технічних засобів зберігання, обробки й передачі інформації й інших технологічних елементів і скласти перелік: робочі станції, включаючи мобільні; сервери; засоби резервного копіювання; телекомунікаційне устаткування корпоративної мережі; пристрої вводу/виводу, включаючи персональні; персональні носії інформації – усілякі накопичувачі, включаючи телефони й фотоапарати;інші засоби зв'язку із зовнішнім миром, включаючи мобільні; самі інформаційні технології, включаючи програмні засоби; все інше, що упущено вище.

Але породжують інформацію не комп'ютерні системи, вони лише обробляють одні повідомлення й виробляють інші, а інформація у формі відомостей породжується в голові людини, яка потім обробляються і повертається йому у вигляді нових відомостей, що представляють інтерес вже для більше широкого кола споживачів.

3. Виявитиосновні групи користувачів інформацією: співробітники; клієнти; партнери; обслуговуючий персонал; особи, які перевіряють; випадкові люди; зловмисники й конкуренти.

Із прийнятним ступенем точності класифікуватиінформацію по важливості для наступного вибору засобів захисту й визначення прав доступу.

4. Виявити доступність інформації, що підлягає захисту в контексті промислового шпигунства, перерахованим групам користувачів, при цьому помітити, що кожна із груп, і, насамперед, співробітники, не повинні мати повний доступ до всієї інформації. Необхідно визначити їх права по доступу до інформації, побудувавши своєрідну матрицю «інформації-права доступу» або «інформації-групи користувачі» і визначити й розмежувати повноваження.

Перераховані раніше дії цілком під силу зацікавленим співробітникам підприємства, які мають відповідні повноваження, але, оскільки вони не є фахівцями в сфері захисту інформації й інформаційної безпеки, залишаються виключення: настроювання конфігурацій програмно-технічних засобів забезпечує їх функціонування й не відповідають вимогам безпеки; традиційна (історично сформована) архітектура мережі, як правило, не забезпечує необхідний захист інформаційних ресурсів і технологій їх обробки; не можна перевіряти самого себе – рішення співробітників можуть містити помилки; технічний персонал не володіє повною інформацією про ступінь важливості різних даних; технічний персонал не може оцінювати доцільність прийнятих адміністративних рішень [44, с.34].

5.Погодитиотримані дані. Необхідно переконаємось, що параметри операційних систем (ОС)робочих станцій, як правило й на жаль, відповідаютьнастройкам постачальника ОС, а всі зміни, якщо й проводилися, були зроблені з єдиною метою забезпечення необхідного функціонування. Те ж саме відноситься й до штатних служб та іншим сервісах, у тому числі й діючих на серверах підприємства, що неприпустимо. Приміром, паролі постачальників устаткування, залишені за умовчанням – часта причина дискредитації систем аутентифікації й авторизації, що надає повний доступ з максимальними правами будь-якому бажаючому в самих захищених системах. Відключення бездіяльних і непотрібних служб, як одного з вимог підвищення захищеності систем, без точних знань їхнього призначення може призвести до

непередбачених наслідків, відпереустановки операційних систем до втрати даних. Настроювання телекомунікаційного устаткування не менш важливо, тому що неправильно сконфігуровані профілі й функції також можуть призвести до перехоплення керування ресурсами. Ці обставини диктують нові умови продовження роботи, а подальші кроки вимагають залучення фахівців для погодженої роботи із захисту інформації.

Необхідно звернутися до спеціалізованих служб та компаній для виконання комплексу робіт, перерахованих вище. Переваги такого підходу в тому, що персонал притягнутої служби або компанії має штат експертів з унікальним обсягом знань і практичним досвідом у суміжних областях IT-сферіінформаційна безпека й захист інформації, у т.ч. моделювання процесів, аналіз ризиків і погроз;архітектура телекомунікаційних мереж; операційні системи й штатні сервіси; прикладне програмне забезпечення, додатки; захисне програмне забезпечення; технічні та програмні засоби захисту інформації; інші IT-технології й засоби;

Отже, виняткові обставини переборені, частина специфічних функцій покладена на провайдера інформаційної безпеки, зокрема, пропозиції по застосуванню й вибір технічних засобів захисту інформації при реальній необхідності захисту від промислового шпигунства.

6. Настроїти програмно-технічні засоби по наданих рекомендаціях та привести у відповідність архітектуру корпоративної системи, впровадити політику парольного захисту, розділити і/або ізолювати незалежні інформаційні й бізнес-процеси, впровадити розмежування прав доступу до інформаційних ресурсів. Також необхідно з’ясувати штатні можливості наявних програмно-технічних засобів – журнали реєстрації системних подій, функції поточного аудита, системи виявлення й попередження вторгнень, захисне ПО, можливості шифрованого зберігання й передачі даних, можливості перерозподілу навантаження, контентній фільтрації, керування внутрішнім і зовнішнім трафіком і багато чого іншого. Однак, сама людина, як джерело відомостей й їх основний споживач поки залишається осторонь, а «людський» фактор –

найбільш часта причина витоку або втрати інформації, тобто безпека підприємства та держави визначається й мірою відповідальності працівника за дії, які він робить, і без впровадження або деталізації формальних відносин поставлена мета залишиться як і раніше не вирішеною.

7. Провестирозробку й впровадження організаційно-адміністративних мір, що регулюють правила роботи з інформаційними ресурсами й дії персоналу в позаштатних ситуаціях. Масштаб роботи,глибина пророблення й формалізації процесів і кінцева кількість документів визначаються спільною роботою групи відповідального управлінського персоналу підприємства й фахівцями компанії. Необхідно проаналізувати трудові контракти, посадові інструкції й діючі на підприємстві інструкції на предмет визначення зон відповідальності й угод про конфіденційність, визначити перелік необхідних інструкцій і правил роботи із програмними й технічними засобами, регламенти резервного копіювання, визначити методи доступу до інформаційних ресурсів, зокрема, розробити політику парольного захисту, передбачити правила дії співробітників у позаштатних ситуаціях.

Політика парольного захисту – це організаційно-правовий і технічний документ одночасно і при його складанні треба спиратися на принцип розумної достатності. Зрозуміло, що в компанії з єдиним системним адміністратором захоплення розробкою нормативною документацією призведе до невиправданих витрат на розробку документів, а їх педантичного виконання безглуздо поглинатиме час виконавців. Тому, в загальному випадку, цілком достатньо веськомплекс необхідних процедур обмежити мінімальним набором правил і зафіксувати їх в одному документі, наприклад «інструкція по парольному захисту».

Варто передбачити й спосіб доведення розроблених документів до персоналу компанії. Наприклад, постійне подання на внутрішньому корпоративному web-сайті компанії при обов’язковому підписанні окремих документів відповідальними працівниками, тоді, навіть ненавмисні, порушення безпеки будуть мати конкретних авторів. Природно, перелік і склад кожного

документа для кожного підприємства унікальні й нерідко відрізняються для різних підрозділів одного підприємства, але при цьому відповідають єдиній політиці інформаційної безпеки, доцільність розробки якої теж визначається на поточному кроці. Щоб уникнути можливих колізій із чинним законодавством зміст документів й їх легалізацію варто погодити з юридичною службою.

8. Розробити й впровадити метод і засоби аналізу захищеностіресурсів та захисту від промислового шпигунства, визначити інтервали й призначаємо відповідальних серед штатного персоналу за проведення систематичного контролю створеної системи інформаційної безпеки. Для аналізу програмно-технічних засобів можна застосувати програмні сканери безпеки й впровадити їх у корпоративну систему, а розроблену нормативну документацію приводити у відповідність при змінах характеру й складу бізнес-процесів, змінах архітектури мережі й, з іншого боку, регулярно піддавати створену систему захисту інформації аналізу на відповідність вимогам документації, тобто проводити регулярний внутрішній аудит.

Впровадження розроблених мір займе деякий час, як і підготовка персоналу, перш, ніж захист інформації буде забезпечений на належному рівні. Але є ще кілька питань, від вирішення яких залежить досягнутий рівень захисту інформації. По-перше, розвиток технологій, у тому числі і тих, які використовують зловмисники, це постійний процес, вимагає й удосконалювання засобів захисту. По-друге, ніхто не гарантує, що при впровадженні навіть незначних змін і наступної експлуатації корпоративної інформаційної системи в ній не з’являться нові вразливості. На жаль, але, на відміну від розвинених країн, у нашій країні практика страхування інформаційних ризиків поки ще відсутня.По-третє, неможливо якісно перевірити самогосебе.

Єдине рішення – в проведенні періодичного зовнішнього аудиту для підтвердження й підтримки заданого рівня захищеності. Поява «слабкої» ланки в побудованій системі призведе до послаблення системи в цілому. Регламент і регулярність проведення зовнішнього аудита можуть бути визначені в процесі

розробки організаційних мір і закріплені у відповідних розпорядницьких документах. Запропонована послідовність дій визначена виходячи з досвіду провідних компаній для захисту від промислового шпигунства, які займаються інформаційною безпекою підприємств із різними формами власності, різних сфер діяльності й різної величини – від декількох робочих місць в одному приміщенні до територіально розподіленої структури з багатотисячним колективом. Безумовно, даний підхід має деякі недоліки з погляду побудови комплексної системи керування інформаційною безпекою, але це вже інше завдання.

Перевагами запропонованого підходу є: досягнуто поставлену мету – конфіденційна інформація захищена від промислового шпигунства; значна частина робіт виконана штатним зацікавленим персоналом; документовано поточний стан інформаційної системи підприємства; запропонований підхід дозволить уникнути невиправданої бюрократичної тяганини з розподілом обов'язків при виконанні робіт; гранично знижені витрати на досягнення мети; створена логічно пов'язана система захисту інформації та протидії промисловому шпигунству; створено базу для побудови системи інформаційної безпеки; істотно підвищений рівень безпеки підприємства та держави.

Таким чином, запропонований підхід є раціональним, щодо захисту конфіденційної інформації від промислового шпигунства напідприємствах при застосуванні принципу доцільності витрат на забезпечення даного захисту.

3.3. Застосування PR-методів уконкурентній розвідці як легальнаальтернатива промисловому шпигунству

У контексті розвитку соціокомунікативних процесів особливе значення надається питанням пошуку та захисту інформації від промислового шпигунства. Запеклі інформаційно-комунікаційні війни та конкурентна боротьба, що точаться в окремих сегментах сучасного суспільства, стали поштовхом до виникнення так званої конкурентної розвідки(варіанти назв —

«корпоративна розвідка», «промислове шпигунство», «промислова розвідка»). Цей напрямок із часом став окремою галуззю, яку можна вважати типовим допоміжним комунікаційним процесом поруч із такими як менеджмент, логістика, консалтинг тощо. При цьому особливо актуальнимсьогодні є вивчення комунікаційної складової порушеного питання.

Слід зазначити, що добірка прийомів та засобів у промисловому шпигунствузагалом подібна до тієї, яка використовується у класичній розвідці. У більшості цивілізованих країн ця галузь офіційно визнана та регулюється низкою нормативно-правових актів, в арсеналі яких передбачено як попереджувальні норми, так і кримінальну відповідальність [49, с.355, с. 28].

Цивілізована конкурентна розвідка базується на так званому «золотому правилі», згідно з яким від 70 до 90% потрібної інформації знаходиться у відкритих джерелах [49, с. 356]. Відповідно, головним завданням є знайти її та належним чином проаналізувати. При цьому не потрібно вербувати особливо цінних працівників-інсайдерів у структурах конкурентів, копирсатися у сміттєвих кошиках у їхніх офісах або зламувати сейфи з важливими документами. Варто просто ретельно збирати факти та аналізувати ситуацію, що складається навколо конкуруючої організації, бо саме з незначних, на перший погляд, клаптиків можна побудувати загальну картину.

Виходячи з того, що головною метою в розвідці є цінна інформація, цілком зрозумілим стає важливість PR-складової цього процесу загалом. Специфіка роботи у галузі промислового шпигунства передбачає два базових рівні — розвідку та контррозвідку. Тобто видобування конкурентної інформації та захист власної від зазіхань конкурентів відповідно. Базові завдання PR у форматі промислового шпигунства знаходяться в контексті двох напрямків діяльності — аналітичної роботи та оперативного збору інформації.

Аналітична робота.Головними джерелами для аналітичної роботи є інформаційні носії, що відносяться до вихідного інформаційного каналу:

- прес-релізи;
- ньюс-релізи;

- матеріали на корпоративному сайті;
- інтерв'ю та авторські статті фахівців досліджуваного об'єкта;
- відкриті звіти та презентаційні матеріали;
- рекламна поліграфія (буклети, флаєри, прайси та ін.);
- офіційна галузева статистика.

Обробка цих матеріалів поділяється на первинну та поглиблену аналітику. До першої можна віднести моніторинг ЗМІ та оцінку соціально-економічних показників конкурента. Друга орієнтується на проведення поглиблених пошуків у форматі маркетингових та соціологічних досліджень. Важливе значення в процесі видобування інформації має її достовірність та актуальність, які можна забезпечити лише шляхом індивідуального підходу та максимального наближення безпосередньо до джерела. Саме тут особливого значення набувають інструменти та навички фахівців із PR. Здобувач інформації має бути активною комунікабельною особистістю, що володіє навичками встановлення контактів та налагодження ефективних стосунків з конкретним об'єктом. Усі ці вміння будуть актуальними саме в контексті оперативної роботи.

Оперативна робота .Робота під «легендою» журналіста.Останні кілька століть найефективнішим камуфляжем для видобувача інформації в класичній розвідці був образ журналіста. Саме працівник мас-медіа сьогодні може, не викликаючи підозри, ставити різноманітні запитання, відвідувати важливі заходи, вимагати будь-яку інформацію (окрім тієї, що становить державну таємницю), посилаючись на відповідні статті профільного законодавства. Зокрема, в Україні журналістську діяльність забезпечують Конституція, Закон України «Про інформацію», Закон України «Про друковані засоби масової інформації (пресу) в Україні», Закон України «Про телебачення та радіомовлення». Зазначені нормативно-правові акти дають журналісту не тільки можливість отримувати потрібну інформацію, а й захищають від намагань офіційних або приватних осіб перешкодити його діяльності.

Таким чином, озброєний журналістським посвідченням сучасний промисловий шпигун є одним із найефективніших інструментів видобування конкурентної інформації. Зрозуміло, що виходу на оперативний збір інформації передує тривала підготовка, яка передбачає:

- формування легенди журналіста (реальна журналістська робота);
- розробку переліку відкритих та опосередкованих питань, відповіді на які потрібно знайти;
- визначення переліку осіб у конкуруючих структурах, що є носіями важливої інформації, та попереднє ознайомлення з їхніми досьє;
- визначення переліку документів, що можуть містити важливу інформацію;
- заглиблення «журналіста» в проблематику галузі.

У процесі збору інформації особливого значення набуває вміння помічати дрібні деталі, враховувати інтереси та настрій осіб, з якими відбувається спілкування, та інші комунікаційні аспекти. До цільової групи в процесі оперативного збору інформації можна віднести кілька пріоритетних. Найцінніша знахідка — це марнославні працівники середнього та ТОП-рівня. Після кількох комплементів щодо їхнього професіоналізму та значущості здатні видати важливу інформацію або навіть стати постійним джерелом інформації, своєрідними інсайдерами, не підозрюючи того. Зазвичай найкоротший доступ до важливої інформації мають секретарі ТОП-менеджерів, які переважно є особами жіночої статі. При відповідному підході вони можуть бути не тільки разовими інформаторами, а й стабільними інсайдерами.

Пересічні працівники, не зв'язані зобов'язанням про збереження корпоративної таємниці, можуть надавати фрагментарну інформацію, яку в подальшому аналітики використовуватимуть для побудови загальної картини. Увага з боку журналіста та бажання вислухати думку пересічного працівника викликають з боку останнього готовність викласти все, що він знає з конкретного питання. Головне — вислухати людину, дати відчути її значущість і цінність. Ключовим моментом у роботі журналіста-розвідника є спілкування з першою особою конкуруючої структури. Основа успіху полягає у знанні та

розумінні психології співрозмовника, кола його інтересів, уподобань, біографії, та, звичайно, належним чином складених запитань для інтерв'ю.

Робота під «легендою» партнера або клієнта. Звернення до працівників конкуруючої структури під виглядом клієнта або потенційного партнера також дає можливість отримувати відповіді на важливі питання, не викликаючи зайвих підозр. У цьому випадку головна увага розвідника концентрується на працівниках відділів по роботі з клієнтами та окремих профільних фахівцях. Добірка комунікаційних інструментів стандартна — увага та прояв поваги до співрозмовника.

Робота під час публічних заходів. Не викликаючи підозр, отримувати важливу інформацію про конкурентів можна на конференціях, семінарах, презентаціях, торговельно-промислових виставках та ярмарках та інших публічних заходах, де обговорюються відповідні питання. Об'єктами уваги при цьому можуть бути ТОП-менеджери, керівники середньої ланки та профільні фахівці. Особливо результативними для збору інформації є фуршет або бенкет. Саме коли офіціоз зникає, а людина розслаблена, доволі часто під дією алкоголю, вона максимально відкрита для цілеспрямованого спілкування.

При цьому слід зазначити, що працювати можна як на чужих публічних заходах, так і на власних. В останньому випадку більш специфічним є проведення роботи через разові тематичні заходи, системно працюючі професійні клуби, навчальні курси. Під час їх роботи можна стимулювати дискусії на професійні теми, водночас з'ясовувати логіку, специфіку та особливості роботи конкурентів. Іноді такі заходи використовують для пошуку інноваційних ідей і рішень, які згодом застосовують у власних інтересах. Остання форма видобування інформації зараз є доволі поширеним інструментом, який застосовують у бізнес-колах країн Європи та США.

Боротьба з несанкціонованою втратою інформації є одним із найважливіших завдань для організації, яка працює в щільному конкурентному середовищі. При цьому головними напрямками роботи є:

- контроль за вихідною інформацією;

- контроль за особистими контактами та професійними зв'язками важливих працівників;
- психологічна підготовка персоналу щодо упередження інсайдерства.

Контроль за вихідною інформацією. Задля впровадження ефективної практики захисту корпоративної інформації необхідно передбачити комплекс формальних процедур, що мають стати обов'язковими для контролю усіх інформаційних носіїв, які складають вихідний інформаційний канал. Насамперед слід визначити процедуру підготовки, редагування та цензурування таких документів, як прес-реліз та ньюс-реліз, а також матеріалів, що йдуть на корпоративний сайт та у ЗМІ. Для цього:

- складається список тем та проблемних питань, заборонених для висвітлення (переглядається відповідно до зміни корпоративних акцентів);
- складається список ЗМІ, а також окремих журналістів, контакти з якими слід зводити до мінімуму або здійснювати під особистим контролем;
- призначається коло фахівців, які можуть надавати коментарі або матеріали для підготовки інформаційних матеріалів;
- призначається відповідальний за цензурування вихідних інформаційних матеріалів.

Відповідно до цих правил визначається алгоритм проходження інформаційних документів від моменту добору базового матеріалу до його надання кінцевому адресату (хто пише, хто складає, хто рецензує, хто цензурує, хто відправляє). Природно, що ключову роль у цій процедурі відіграє підрозділ по роботі з громадськістю та ЗМІ, маючи широкі повноваження щодо отримання робочої інформації та відповідальність за її трансляцію.

Контроль за контактами цінних працівників. У багатьох країнах розвинутої демократії абсолютно законно та беззаперечно з боку найманих працівників існує практика попередньої перевірки (при прийомі на роботу) та подальшого контролю офіційних та неофіційних контактів цінних працівників. Зазначена функція певною мірою належить до кола обов'язків двох типових корпоративних структур — служби безпеки та HR-підрозділу. І оскільки

останній є частиною підрозділу по роботі з громадськістю та ЗМІ, до вирішення зазначених питань залучають і фахівців із PR.

Ключовими особами мають стати керівники HR-відділу та відділу по роботі зі ЗМІ, бо саме вони відповідають за добір та професійну підготовку персоналу, а також за організацію публічних заходів, де цінні працівники можуть мати небажані контакти. Для налагодження системної роботи в цьому плані та ефективної співпраці з підрозділом безпеки необхідно:

- підготувати досьє на журналістів, що входять до пулу організації (базова тематика, перелік видань з якими працює або працював тощо);
- скласти список журналістів — персон «нон-грата»;
- скласти перелік дружніх, нейтральних та ворожих (таких, що належать конкурентам) ЗМІ;

Враховуючи, що публічні заходи є потенційно небезпечним полем для втрати важливої інформації, необхідно запровадити певні правила інформаційної безпеки, а саме:

- обов'язкова попередня акредитація ЗМІ на власних заходах та відстеження небажаних гостей;
- розробити сценарії заходів таким чином, щоб максимально ускладнити можливість вільного спілкування журналістів та інших гостей з працівниками організації;
- поставити поруч із власними «проблемними» особливо цінними працівниками контролюючу особу;
- зважено підходити до складання меню фуршетів та бенкетів (особливо щодо алкогольних напоїв).

Психологічна робота з персоналом. Найкращим варіантом боротьби з інсайдерством та несанкціонованим проникненням в корпоративне інформаційне поле є робота на попередження. В її основі два напрями — формування духу корпоративного патріотизму та навчання із розпізнавання дій, що свідчать про намагання прихованого та відкритого вербування.

Формування корпоративного духу є складною та тривалою процедурою, що залежить від багатьох чинників — матеріальної зацікавленості, особистої мотивації, міжособистих відносин та інших моментів, які є складовими частинами будь-якого колективного утворення. У цьому плані відповідальність безперечно покладається на піарників. А точніше на HR-підрозділ. Навчальна підготовка до виявлення фактів вербування відбувається у форматі тематичних тренінгів, за які відповідає служба безпеки. Заняття проводять профільні фахівці, що мають відповідний досвід та власні напрацювання, утім можна загалом визначити кілька моментів, які дозволять навіть недосвідченим виявити класичні риси вербування. Серед них:

- необґрунтовано підвищена увага до конкретної особи;
- усі варіанти «безкоштовного сиру» (цінні подарунки, запрошення у дорогі ресторани та інші розважальні заклади);
- намагання ущільнити особистий контакт із боку сторонньої особи.

Підбиваючи підсумки, вважаємо за необхідне подальше вивчення комунікаційної складової, а саме PR-технологій у системі інформаційної безпеки, конкурентної розвідки та промислового шпигунства. Зрозуміло, що створення моделі корпоративної інформаційної безпеки потребує більш системного та індивідуального підходу, який би враховував усі особливості внутрішньокорпоративної політики, навколишнього середовища, специфіку діяльності організації, її потенційних та реальних конкурентів, а також характер їхньої діяльності. Це вимагає значних матеріально-технічних затрат та часу. Утім, слід пам'ятати, що головним принципом її функціонування є активна співпраця фахівців із PR та профільних структур, які забезпечують захист корпоративного інформаційного поля від зовнішніх проникнень та промислового шпигунства.

Висновки до розділу 3

Отже, опанування зарубіжної практики в сфері протидії промисловому шпигунству у ринкових умовах, яка має важливе значення для сучасної України, допоможе краще освоїти тонкощі господарської діяльності у жорсткому конкурентному середовищі та запобігти проявам недобросовісної конкуренції, в т.ч. промисловому шпигунству. Зазначене також свідчить про те, що міжнародний досвід підтверджує необхідність створення системи служб безпеки недержавної правоохоронної діяльності суб'єктів господарювання в Україні як закономірного кроку в подальшому розвитку нашого суспільства на ринкових засадах, а також як фактора у зміцненні демократичних принципів в управлінні державою в контексті протидії промисловому шпигунству.

Ефективна співпраця з іноземними уповноваженими органами має здійснюватися за напрямами: розробки та впровадження (законодавчого закріплення) спрощених механізмів оперативного обміну інформацією щодо операцій з ознаками зловживань або підробок продукції, у тому числі для цілей випуску ноу-хау, ідентифікації осіб, причетних до їх проведення; обміну позитивним досвідом роботи у сфері боротьби з промисловим шпигунством з правоохоронними й контролюючими органами іноземних держав, проведення спільних конференцій з питань забезпечення «прозорості» розвідувальних операцій, організації спеціальної системи підготовки фахівців правоохоронних і підприємницьких структур України на базі відповідних навчальних закладів країни зі значним практичним досвідом протидії злочинам у сфері запобігання промисловому шпигунству та кіберзлочинності.

ВИСНОВКИ

Магістерська робота присвячена дослідженню феномену промислового шпигунства як загрози для економічної безпеки підприємства. Врезультаті аналізу сучасних тенденцій правопорушень у сфері економічної безпекибула запропонована система заходів попередження промислового шпигунства на підприємстві. Основні положення магістерської роботи:

1. Визначено поняття «промислове шпигунство» в контексті його відмінності від економічного шпигунства та розвідувальної діяльності. Промислове шпигунство - це один з видів недобросовісної конкуренції, умисне пошкодження промислового обладнання, інформаційних систем на підприємстві, використання психологічного тиску на працівників, що призвело до викрадення комерційною таємниці (нелегальним методом) та можливої подальшої дискредитації або ліквідації бізнесу конкурентів. Економічне шпигунство – це один з методів нецивілізованої, недобросовісної конкурентної боротьби, що полягає в розкраданні конфіденційної інформації на державному рівні.Розвідувальна діяльність - це збір та аналіз даних про партнерів і конкурентів, мета якого полягає у виявленні реальної ситуації в корпорації, дослідженні сильних і слабких сторін його діяльності (легальним методом).

2. Досліджено складові класифікації видів промислового шпигунства, яке в свою чергу поділяється на: комерційне, технологічне, науково-технічне. Проаналізовано спеціальні форми і методи промислового шпигунства: завуальовані питання фахівцям конкурента; підступні пропозиції для фахівців, що працюють в конкурента з пропозицією заповнити текст зі спеціально відібраних питань; переговори з конкурентом в питанні щодо товарів, або ліцензії, і після отримання необхідної інформації відмова від подальших; для пряме спостереження за об'єктом, яким може бути відділ або фахівець підприємства; використання професіоналів-шпигунів в цілях отримання інформації; напад на майно конкурента; підкуп співробітників ключових відділівпідприємства;розмова-допит з конкурентом; крадіжки креслень, зразків,

документів; шантаж і тиск; незаконне придбання інформації корумпованих представників в уряді.

3. Охарактеризовано інструменти промислового шпигунства: спеціальні пристрої запису і пристрої для перехоплення телефонних ліній; міні аудіо і відео камери; обладнання для отримання інформації з вікон з використанням лазерних випромінювачів; навідні мікрофони; спеціальна система спостереження і передачі відео; спеціальне фотографічне обладнання; пристрої спостереження; пристрої нічного бачення; пристрої для виявлення випромінювання і т.д.

4. Проаналізовано системи правозастосування для боротьби з промисловим шпигунством на міжнародному та національному рівнях: міжнародний захист промислової власності (Паризька конвенція встановлює заборону недобросовісної комерційної практики між країнами-членами; Угода з торговельних аспектів прав інтелектуальної власності (ТРІПС) базується основі мірою на актуальних положеннях Паризької конвенції з охорони промислової власності та Бернської конвенції з охорони літературних і художніх творів;розділ 7 положення ТРІПС під назвою: «Захист секретної інформації». Іншою важливою особливістю положення ТРІПС стосується захисту прав інтелектуальної власності); Європейська система захисту комерційної таємниці (умова договірного права, спрямованим на захист комерційної таємниці за допомогою пункту про конфіденційність); Закон про захист від недоброзосісної конкуренції регламентує відповідальність за порушення права власника за захист своєї інформації, коли зроблено неправомірне привласнення комерційної таємниці конкурентами, які не мають договірних відносин з власником, або шляхом розкрадання, шпигунства, вторгнення в приватне життя, електронного шпигунства і т.д.).

5. Аналізуючи практичний досвід країн Європи у сфері адміністративно-правового забезпечення безпеки діяльності суб’єктів господарювання в контексті промислового шпигунства, зазначено, що в цілому в країнах Європи існує тенденція до створення в промислово-торговельних фірмах потужних

недержавних правоохоронних органів в особі служб безпеки, їх тісної співпраці з державними правоохоронними органами, з метою підвищення ефективності роботи з попередження правопорушень і злочинів, а також актів промислового шпигунства. Досвід країн Європи є потенційно ефективним в Україні.

6. Зазначено, що термінологія щодо актів недобросовісної конкуренції визначена у ст. 1 глави 1 Закону «Про обмеження монополізму і недопущення недобросовісної конкуренції у підприємницькій діяльності». Проте, Закон визначає сутність категорії «конкуренція», але не подає дефініції значення термінів «недобросовіснаконкуренція» та «комерційна таємниця».Доречно термінологічний аспект українського законодавства у сфері подолання проявів недобросовісної конкуренції удосконалити. Прикладом може бути формулювання ст. 11 закон Республіки Польща від 16 квітня 1993 року «Про боротьбу з недобросовісною конкуренцією», який визначає поняття «комерційної таємниці», як таке, що не розкривається в публічній технічній, технологічній, організаційній документації підприємства або іншої інформації, що має комерційну цінність, конфіденційність якої необхідно зберегти.

7. Рекомендовано розширення кола відповідальності за порушення прав інтелектуальної власності в контексті проявів промислового шпигунства в Україні: адміністративно-правові способи захисту (накладення штрафів за неправомірне використання торгівельних марок, знаків для товарів та послуг, брендів та фірмових (комерційних) найменувань); цивільно-правовий спосіб захисту (визнання прав власника; відновлення положення, що існувало до порушення права; припинення дій, що порушують право чи створюють погрозу його порушенню; відшкодування збитків, включаючи втрачену вигоду; рекомендовано доповнити: ліквідування результатів незаконної діяльності, повернення незаконно отриманого прибутку на загальних підставах); кримінальна відповідальність (штраф або виправні роботи, або позбавленням волі , з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм,

програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення).

8. Запропоновано ряд відповідних заходів з профілактики та контролю промислового шпигунства на підприємстві: проводити інвентаризацію інформаційних ресурсів, проводити інвентаризацію всіх технічних засобів зберігання, обробки й передачі інформації й інших технологічних елементів, виявити основні групи користувачів інформацією, виявити доступність інформації, що підлягає захисту в контексті промислового шпигунства, погодити отримані дані, настроїти програмно-технічні засоби по наданих рекомендаціях та привести у відповідність архітектуру корпоративної системи, впровадити політику парольного захисту, розділити або ізолювати незалежні інформаційні й бізнес-процеси, впровадити розмежування прав доступу до інформаційних ресурсів, провести розробку й впровадження організаційно-адміністративних мір, що регулюють правила роботи з інформаційними ресурсами й дії персоналу в позаштатних ситуаціях, проаналізувати трудові контракти, посадові інструкції й діючі на підприємстві інструкції на предмет визначення зон відповідальності й угод про конфіденційність, визначити перелік необхідних інструкцій і правил роботи із програмними й технічними засобами, регламенти резервного копіювання, визначити методи доступу до інформаційних ресурсів, зокрема, розробити політику парольного захисту, передбачити правила дії співробітників у позаштатних ситуаціях.

9. Запропоновано базові завдання PR-методів у конкурентній розвідці як легальний аналог формату промислового шпигунства: система методів складається з двох напрямків діяльності — аналітичної роботи (прес-релізи,ньюс-релізи, матеріали на корпоративному сайті, інтерв'ю та авторські статті фахівців досліджуваного об'єкта, відкриті звіти та презентаційні матеріали, рекламна поліграфія (буклети, флаєри, прайси та ін.), офіційна галузева статистика) та оперативного збору інформації (робота під «легендою» журналіста, робота під «легендою» партнера або клієнта, робота під час публічних заходів).

10. Співпраця у сфері боротьби з промисловим шпигунством має бути спрямована на розробку та реалізацію конкретної програми, яка повинна включати такі заходи: навчання слідчих органів, прокуратури й судових органів методів та особливостей боротьби з промисловим шпигунством, порушеннями у сфері інтелектуальної власності, охороні комерційної таємниці в контексті нормативно-правового забезпечення в Україні, проявів недобросовісної конкуренції, фінансовими махінаціями у сфері високих інформаційних технологій, у тому числі у сфері платежів із застосуванням платіжних карток; посилення підрозділів правоохоронних органів, органів кримінальної експертизи та суду, відповідальних за провадження справ, пов'язаних з махінаціями та шахрайством; поліпшення взаємодії між підприємствами, комерційними структурами й правоохоронними органами з питань боротьби з промисловим шпигунством, розробка та запровадження на підприємствах України заходів щодо оперативного виявлення й запобігання злочинним операціям з комерційними таємницями; створення Єдиної інформаційної бази суб'єктів – активних промислових шпигунів світу з метою анти шахрайства та обміну інформацією (спільні дії НАБУ, НБУ та правоохоронних органів), що надасть можливість запобігти типовим схемам промислового шпигунства, мінімізувати наслідки виявлених нападів, відстежити слабкі й найменш захищені місця в системах інформаційного захисту підприємств; удосконалення законодавства України стосовно дефініції категорії «промислове шпигунство» та злочинів у сфері використання агентурних та технічних методів.

Підводячи підсумок всьому вищесказаному, можна сказати, що сьогодні в Україні вже склалася правова та інституційна системи органів державної влади, які прямо чи опосередковано забезпечують захист інтелектуальної власності, здійснюють боротьбу з недобросовісною конкуренцією та її результатом - промисловим шпигунством. Дослідження феномену промислового шпигунства є актуальною тематикою дослідження на майбутнє.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. АширлієваШ.ПромисловийшпіонажнапідприємствахУкраїни:правовіаспектиборотьби:[Електроннийресурс]/Ш.Аширлієва,Є.Малюкова.-Режимдоступу:http://5fan.info/jgernapolatyujgqas.html

2. Бажал, Ю. М. http://irbis-nbuv.gov.ua/cgi-bin/irbis64r_81/cgiirbis_64.exe?Z21ID=&I21DBN=VFEIR&P21DBN=VFEIR&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=M=&S21COLORTERMS=0&S21STR=Ціл і входження України в європейський інтелектуальний простір / Ю. М. Бажал // Проблеми та перспективи входження України в європейський інтелектуальний простір: освітні аспекти : зб. наук.-експерт. мат. : Національний ін.-т стратегічних досліджень, 2015. – С. 8.

3. Базилевич В. Д. Інтелектуальна власність: креативи метафізичного пошуку : монографія / В. Базилевич, В. Ільїн. — К. : Знання, 2008. — 687с. - (Серія "Київському національному університету імені Тараса Шевченка 175 років").

4. Бегма В. М. Військово-технічне співробітництво: шляхи удосконалення : [монографія] / В. М. Бегма, О. М. Рябець та ін. – К.: ЦНДІ ОВТ ЗСУ, 2010. – 216 с.

5. Бизнесразведка. Внедрениепередовыхтехнологий / Кристофер Бо-ган, Майкл Инглиш; пер. с англ.; подобщ. ред. Б. Л. Резниченко. – М.: Верши-на, 2015. – 328 с.

6. Гончарова Н.О. Підвищення рівнів економічної безпеки підприємства на сучасному етапі / Н.О. Гончарова, Т.М. Головченко // Фінансова криза та шляхи мінімізації впливу її негативних наслідків на економіку області. – Херсон. – 2009. – С. 79.

7. Геєць В. М. Суспільство, держава, економіка:феноменологія взаємодії та розвитку / Валерій Михайлович Геєць. – К., 2009. – 864 с.

8. Гнесюк М. Удосконалення національного законодавства у сфері захисту прав інтелектуальної власності / М. Гнесюк // Право інтелектуальної власності на відкриття . – 2014. – № 7. – С. 71-73.

9. Гордієнко С. Г. Забезпечення інтересів України у сфері захисту інтелектуальної власності : нормативно-правове регулювання : [монографія] / Сергій Георгійович Гордієнко. — К. : Скіф, 2014. — 248с.

10. Гусаковська Т. О. Особливості охорони об'єктів ноу-хау в процесі їх комерціалізації / Т. О. Гусаковська // Вісник Національного технічного університету „Харківський політехнічний інститут". Технічний прогрес та ефективність виробництва. – Харків: НТУ „ХПІ". – 2015. - № 33. – С. 67 – 70.

11. Дениелс Д. Международныйбизнес: внешняясреда и деловыеоперации / Джон Д. Дениелс, Ли Х. Радеба. Пер. с англ. Л. Євенко. - М. : Дело ЛТД, 2015. – 784 с.

12. Договір про закони щодо товарних знаків : [багатостороння угода (не СНД)] від 27.10.1994 р. // Юридичний вісник України.- 1999. - №5. - С.14.

13. Дрыночкин А. В. ВосточнаяЕвропакакэлементглобальныхрынков / А. В. Дрыночкин. – М. : ЗАО «Оолита», 2014. – 240 с.

14. Жаліло Я. Економічна стратегія держави: теорія, методологія, практика: монографія / Я. Жаліло. – К.: НІСД, 2013. – 368 с.

15. Интернет-магазиншпионскогооборудования [Електронний ресурс]. -Режим доступу: http://www.spyline.ru/

16. Клепицкий И. А. Система хозяйственныїхпреступлений / И. А. Клепицкий. - М. : Статут, 2015. - 571 с.

17. Кримінальний кодекс України від 5 квітня 2001 р. № 2341–III // Відомості Верховної Ради України. – 2001. – № 25–26.

18. Кримінальне право (Особлива частина) : [підручник] / за ред. О. О. Дудорова, Є. О. Письменського. - Т. 1. - Луганськ : видавництво ≪Елтон-2≫, 2012. - 780 с.

19.Ліссабонська угода про захист зазначень походження та їхню міжнародну реєстрацію : [міжнародний договір] від 31 жовтня 1958 року.

20. Лепина Т. Г. Уголовно-правоваяохранаинтеллектуальнойсобственности : дисс. ... кацд. юрид. наук / Т. Г. Лепина. - Курск, 2014. - 235 с.

21.Лук’яненко Д. Г. Економічна інтеграція та глобальні проблеми сучасності : [Навчально-методичний посібник] / Д. Г. Лук’яненко. – К.: КНЕУ, 2015. – 206 с.
22.
23. Мадридська угода про міжнародну реєстрацію знаків від 14.04.1891р. // Зібрання чинних міжнародних договорів України. – 1990. – № 1. – С. 348.
24. Мандрона М. М. Порівнльний аналіз закладних пристроїв для несанкціонованого отримання акустичної інформації / М. Мандрона, Р. Сало/ Науковий вісник НЛТУ України. – 2014. – Випуск 24.2. – С. 343-347.
25. Митний кодекс України від 21 квітня 2012 р. //„Голос України”. - №73-74 - 2012.
26. Мошак Г. Г. Розвиток запобігальної діяльності приватних служб (на матеріалах ФРН і України) / Г. Г. Мошак // Часопис Київського університету права. – 2010. – № 1. – С. 227–232.
27. Нагорна І.І. Організаційно-економічний механізм у забезпеченні стійкої економічної безпеки промислових підприємств: Автореф. дис… канд. екон. наук: 08.00.04. / Інна Іванівна Нагорна; [Інст-т проблем ринку та економікоеколог.досліджень]. – Одеса, 2008. – 20 с.
28. Навроцький В. О. Господарські злочини : [лекції для студ. юрид. факту] / В. О. Навроцький / Львів. держ. ун-т ім. І. Франка. - Львів, 2014. - 60 с.
29. Нерсесян А. С. Кримінально-правова охорона прав інтелектуальної власності : [монографія] / А. С. Нерсесян. - Хмельницький : Видавництво Хмельницього університету управління та права, 2010. - 192 с.
30.Онищенко В. Модернізація як імператив розвитку України / Володимир Пилипович Онищенко // Економіка України. - 2011. - № 7. - С. 4-14.
31.Паризька конвенція про охорону промислової власності від 20 березня 1883 року // Юридичний вісник України. – 2002. - № 43.
32. Про Антимонопольний комітет України: Закон України від 26 листопада 1993 року // Відомості Верховної Ради України. — 1993. — № 50. — Ст. 472.
33. Про зовнішньоекономічну діяльність: Закон України// Відомості Верховної Ради України.-1991.-К 29.

34. Про обмеження монополізму і недопущення недобросовісної конкуренції у підприємницькій діяльності: Закон України//Голос України.-1992.- 29 квіт.

35. Про захист від недобросовісної конкуренції: Закон України від 7червня 1996 р. № 236/96-ВР // Відомості Верховної Ради України. – 1996. – № 36.

36.Про охорону прав на винаходи і корисні моделі : Закон України від 15 грудня 1993 р. // Відомості Верховної Ради України. - 1994.- № 7.- Ст.32; в редакції Закону України від 1 червня 2000 р. // Урядовий кур'єр. - 2001.- 14 лютого.

37. Про охорону прав на зазначення походження товарів : Закон України від 16 червня 1999 р. // Відомості Верховної Ради України. - 1999. - № 32. - Ст. 267.

38. Про охорону прав на знаки для товарів і послуг : Закон України від 15 грудня 1993 р. // Відомості Верховної Ради України. - 1994.- № 7.- Ст. 36.

39. Про охорону прав на промислові зразки : Закон України від 15 грудня 1993 р. // Відомості Верховної Ради України. - 1994. - № 7. - Ст. 34.

40. Про охорону прав на знаки для товарів і послуг : Закон України № 3689-XII від 15.12 1993 в редакції від 10.04.2008 року // Відомості Верховної Ради України. – 1994. – № 7. – С. 36.

41. Про охорону прав на топографії інтегральних мікросхем : Закон України від 05.11.1997 р. № 621/97–ВР // Відомості Верховної Ради України. – 1998. – № 8 . – С. 28.

42. Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : дис... канд. юрид. наук / О. Е. Радутний. - Х., 2014. - 204 с.

43.Рогоженко І. Промислове шпигунство, конкурентна розвідка, бенч-маркинг й етика цивілізованого бізнесу / І. Рогоженко // Практичний маркетинг. — 2015. — 22 січня. — С. 36—50.

44. Сергєєва В. Способи захисту прав на комерційну таємницю / В. Сергєєва / / Юридичний журнал. - 2014. - № 6. - С. 32-38.

45. Тимчук Д. Українська «оборонка» і промислове шпигунство: [Електронний ресурс] /Дмитро Тимчук //Військова панорама.- 2012. - Режим доступу: http://wartime.org.ua/2900-ukrayinska-oboronka-promislove-shpigunstvo.html

46. Ткачук Т. Ю. Міжнародний досвід організації економічної безпеки підприємств / Т. Ю. Ткачук // Бизнес и безопасность. – 2009. – № 4. – С. 12–15.

47. Ткачук Т. Ю. Сучасні реалії та загрози інформації з обмеженим доступом на підприємстві / Т. Ю. Ткачук. – Право України. – 2011. – № 3. – С. 243–252.

48. Ткачук Т. Ю. Взаємодія служби безпеки підприємства з право-охоронними органами як важлива складова забезпечення інформаційної безпеки підприємства / Т. Ю. Ткачук // Бизнес и безопасность. – 2010. – № 6. – С. 22–28.

49. Тітомер Є. В. Суб'єктивна сторона злочинів, передбачених ст.ст. 231, 232 КК України / Є. В. Тітомер / / Актуальні проблеми держави і права. - 2015. - № 55. - С. 353-357.

50. Ткачук Т.Ю. Конкурентна розвідка / Тарак Ткачук .— К.: НА СБ України. - 2015. – 296 с.

51. Топалова Л. Д. Правовий режим комерційної таємниці : автореф. дис. ... канд. юрид. наук / Л. Д. Топалова. - Донецьк, 2012 - 20 с.

52. Угода щодо торгових аспектів прав інтелектуальної власності (ТРІПС) : [багатостороння угода (не СНД)] від 15.04.1994 року // Українська інвестиційна газета. – 2006. - № 29.

53. Украина. Всемирныйобзорэкономическихпреступлений [Електронний ресурс] / PWC. – Режим доступу:https://www.pwc.com/ua/en/services/forensic/assets/gecs_2014_report_ukraine_rus.pdf

54. Україна обурена присутністю російських кондитерів при перевірках заводів Roshen, допускаючи промислове шпигунство :[Електронний ресурс] // Корреспондент. net, 2013. - Режим доступу: http://ua.korrespondent.net/business/companies/1618128-ukrayina-oburena-prisutnistyu-rosijskih-konditeriv-pri-perevirkah-zavodiv-roshen-dopuskayuchi-promislo

55. Франчук В.І. Загрози корпоративній безпеці як об’єкт дослідження / В.І. Франчук // Актуальні проблеми економіки. – 2015. – №9. – С.148-154.

56. Харламова С. О. Кримінальна відповідальність за незаконні дії з відомостями, що становлять комерційну або банківську таємницю : дис... канд.юрид. наук / С. О. Харламова. - К., 2013. - 221 с.

57. Харченко В.Б. Кримінально-правова охорона прав на об'єкти інтелектуальної власності в Україні: перспективи розвитку та гармонізації з європейським законодавством: Автореф. дис. ... д-ра юрид. наук / В. Б. Харченко. - Х., 2011. - 36 с.

58. Цивільний кодекс України : станом на 20 червня 2005 року. – К.: Велес, 2005. – 278 с.

59. Якубівська Ю. Є. Вплив промислового шпигунства на сферу інтелектуальної власності / Ю. Є. Якубівська // Зовнішня торгівля: право та економіка. Науковий журнал. - № 3(43) / 2013. -К.: УДУФМТ, 2013. - С.158-162.

60. Якубівська Ю. Є. Передумови формування системи економічної безпеки України в умовах євроінтеграції / Ю. Є. Якубівська //Проблеми трансформаційних економік в умовах глобалізації: матеріали V-ої міжнародної науково-практичної конференції, м.Тернопіль, 25 квітня 2013 р. / ТКІ.; Наук. ред. В.Ф. Мартинюк. – Тернопіль: Вектор, 2013. – С. 136-139.

61. Якубівська Ю. Є. Порушення права інтелектуальної власності як загроза економічній безпеці / Ю.Є.Якубівська // Фінансово-економічна безпека держави, регіону, підприємства: погляд молодих вчених. Матеріали Всеукраїнської наукової конференції студентів і молодих вчених, м.Тернопіль, 11 квітня 2014 р. / ТНЕУ. – Тернопіль, 2014. – С.127-129.

62. Якубівська Ю.Є. Стимулювання розвитку індустрії програмної продукції в контексті формування стратегії імпортозаміщення України / Ю. Є. Якубівська // Вітчизняний та світовий досвід правового регулювання відносин у сфері інтелектуальної власності / Збірник наукових праць за матеріалами науково-практичної інтернет-конференції, 17-18 квітня 2014 р. / За заг. ред. А.І.Кузьмінського, О.П.Орлюк. – Черкаси: Чабаненко Ю.А., 2014. – С. 73-77.

63. Якубівська Ю.Є. Цільові атаки в контексті промислового шпигунства» / Ю.Є.Якубівська // Проблемыразвитиявнешнеэкономическихсвязей и привлеченияиностранныхинвестиций: региональный аспект: сб. науч. тр. - Т.2, Донецк: ДонНУ, 2014. – С. 368-372.

64. Adamczak,AlicjaiDuVall,Michał.2010.Ochronawłasnościintelektualnej.Warszawa:Uniwersyteckiośrodektransferutechnologii UniwersytetuWarszawskiego.(397s.).

65. Anti-counterfeintinggroup [Electronicresourse] /The ACG Organization: 2014. - Access: http://www.a-cg.org/

66. Ambos,Bjornand.Schelgelmilch,BoboB.TheuseofinternationalR&Dteams:anempiricalinvestigationofselectedcontingencyfactors:ScienceandDirect,JournalofWorldBusiness:Elsevier. - 2004. - N39. - p.37–48.

67. Barrachina,AlexandTauman,Yair.Entryandespionagewithnoisysignals:Gamesandeconomicbehavior:Elsevier. - 2014. - N83. - p.127-146.

68. Biannualinformationoneurobanknotecounterfeiting[Electronicresourse]. Europeancentralbank: 2015 - Access:.http://www.ecb.europa.eu/press/pr/date/2015/html/pr130719.en.html

69. Blair D., Huntsman J. Protect U.S. IntellectualPropertyRights[Electronicresourse] / TheWashingtonPost. – 2013. – Access: https://www.washingtonpost.com/opinions/dennis-blair-and-jon-huntsman-protect-us-intellectual-property-rights/2013/05/21/b002e10e-c185-11e2-8bd8-2788030e6b44_story.html

70. Ciecierski,Marek.Szpiegostwoprzemysłoweopanowałocyberprzestrzeń [Electronicresourse] /InteriaBiznes: 2013. - Access: http://biznes.interia.pl/wiadomosci/news/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen,1885978,4199

71. Commissionproposesrulestohelpprotectagainstthetheftofconfidentialbusinessinformation:[Electronicresourse] / EuropeanCommission,Pressrelease:Brussels,28November2013:- Access: http://europa.eu/rapid/press-release_IP-13-1176_en.htm

72. CommissionRegulation(EC)No772/2004of27April2004ontheapplicationofArticle 081(3)oftheTreaty(nowArticle101(3)oftheTFEU)tocategoriesoftechnologytransferagr eements(TTBER) [Electronicresourse] :- Access: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0772:EN:HTML>

73. CommissionNotice-GuidelinesontheapplicationofArticle81oftheECTreaty(nowArticle101oftheTFEU)tote chnologytransferagreements(TechnologyTransferGuidelines): [Electronicresourse] / Access: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004XC0427%2801%29:EN :HTML>

74. Directive2004/48/ECoftheEuropeanParliamentandoftheCouncilof29April2004ont heenforcementofintellectualpropertyrights[Electronicresourse] / Access: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:EN:PDF>

75. Dyrektywa2005/29/WEParlamentuEuropejskiegoiRadyzdnia11maja2005r.onieuc zciwychpraktykachhandlowychdotyczącanieuczciwychpraktykhandlowychstosowany chprzezprzedsiębiorstwawobeckonsumentównarynkuwewnętrznymorazzmieniającain nedyrektywy,Dz.Urz.UELz2005r.Nr149,s.22.

76. Elliott,SharonMollman.Thethreatfromwithin:tradesecrettheftbyemployees:Patents ,NaturePublishingGroup:Wisconsin. - 2007. - Vol.25,N3. - p.293-295.

77. Everett,Bernet.Opticallytransparent:theriseofindustrialespionageandstatesponsore dhacking:Feature,InfoGuard. -2013. - p.13-17.

78. Globalimpactstudy [Electronicresourse] / BASCAP.Theworldbusinessorganization/ - 2014. - Access:http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/

79. HagueConventiononChoiceofCourtAgreements [Electronicresourse] . - Access:http://www.hcch.net/index_en.php?act=conventions.text&cid=98

80. Hare,ForrestandGoldstein,Jnathan.Theindependentsecurityprobleminthedefensein dustrialbase:Anagent-

basedmodelonasocialnetwork:Criticalinfrastructureprotection,Elsevier,ScienceDirect. -2010. - N3. -p.128-139.

81. HowCriminalsMade $18 MillionByHoldingOurDataHostage [Electronicresourse] / AmericanSocietyforIndustrialSecurity (ASIS). – 2016. – Access: https://sm.asisonline.org/Pages/Held-Hostage.aspx

82. Lee,Chang-Moo.TheStrategicMeasuresfortheIndustrialSecurityofSmallandMediumBusiness:HindawiPublishingCorporation,ScientificWorldJournal. -2014. - p.1-4.

83. Miller,LesleyEllis.InnovationandIndustrialEspionageinEighteenth-CenturyFrance:AnInvestigationoftheSellingofSilksthroughSamples:JournalofDesign History. -2015. - Vol.12,No.3. -p.271-292.

84. Minott,Nathaniel.TheEconomicEspionageAct:isthelawallbarkandnobite?:Information&CommunicationsTechnologyLaw:Routledge. -Vol.20,No.3. -2011. -p.201–224.

85. Morris,Mel.Intelligence,knowledgeandorganisedcrime:ComputerFraud&Security: CEO,Prevx. -2010. - p.13-15.

86. CcCallion,Jane [Electronicresourse] / NewEUrulesonindustrialespionageissued:ITPro. - 2013. - Access:http://www.itpro.co.uk/hacking/20163/new-eu-rules-industrial-espionage-issued

87. Rosenfeld,Steven [Electronicresourse] / CorporateEspionageTacticsUsedAgainstLeadingProgressiveGroups,ActivistsandWhistleblowers:Alternet. - 2013. Access:http://www.alternet.org/activism/corporate-espionage-against-progressive-nonprofits

88. TheReportoftheCommissionontheTheftofAmericanIntellectualProperty [Electronicresourse] / The IP Commission. – 2015. – Access: http://www.ipcommission.org/report/ip_commission_report_052215.pdf

89. TRIPS(WTOAgreementonTradeRelatedAspectsofIntellectualPropertyRights) [Electronicresourse] / - Access:http://www.wto.org/english/tratop_e/trips_e/trips_e.htm

90. Ustawaz16kwietnia1993r.ozwalczaniunieuczciwejkonkurencji,t.j.Dz.U.z2003r.Nr 153,poz.1503zezm.

91. Ustawaz30czerwca2000r.-Prawowłasnościprzemysłowej,t.j.Dz.U.z2003r.Nr119,poz.1117,zezm.

92. Ustawaz23sierpnia2007r.oprzeciwdziałaniunieuczciwympraktykomrynkowym,Dz.U.z2007r.Nr171,poz.1206,zezm.

93. WorldIntellectualPropertyOrganisation(WIPO)-WhatisaTradeSecret? [Electronicresourse] -Access: http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm