Тернопільський національний економічний університет
Юридичний факультет
Кафедра фінансово-економічної безпеки та інтелектуальної власності

МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА

на тему:

«ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ В УКРАЇНІ»

Студента 1 курсу магістратури
групи ФЕБм - 11
Галузі знань 1801 – специфічні категорії
Спеціальності 8.18010014 “Управління фінансово-економічною безпекою”
Кучера В. С.

Керівник _____
_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Національна шкала _____
Кількість балів: _____Оцінка: ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали

м. Тернопіль – 2016 рік

ЗМІСТ

ВСТУП

Причиною непорозуміння між визначеннями понять «промислове шпигунство» і «бізнес-розвідка» або «економічна розвідка» є неправильне розуміння саме 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-дільності включають перепродаж товарів та надання послуг, то на перший погляд здається, що проблеми з шпигунством у таких компаній немає. Даний аспект визначає актуальність теми дослідження. Забезпечення успішного підприємництва, розвиток вільної конкуренції, створення безпечного середовища для розвитку бізнесу сприяють активному залученню розвідувальної діяльності, а промислове шпигунство розглядається як діяльність, спрямована на тактичне або стратегічне (конкурентне) отримання переваги над конкурентом, ідентифікації 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.

В основу написання цієї курсової роботи покладено результати дослідницької роботи таких вітчизняних і зарубіжних учених, як Аширлієва Ш., Гончарова Н, Жаліло Я., Мошак Г., Ткачук Т., Тимчук Д., Туралінські К., Франчук В, Якубівська Ю. 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.

Метою курсової роботи є загальнотеоретичний аналіз тенденцій розвитку та протидії промисловому шпигунству в Україні, а також дослідження системи права у сфері адміністративно-правового забезпечення безпеки суб'єктів господарювання в контексті запобігання промисловому шпигунству. Одним із різновидів цієї діяльності є створення за підтримки і за ініціативою спецслужб детективно-охоронних фірм, служб і агентств безпеки, які беруть активну участь у профілактиці правопорушень, розслідуванні справ про промислове шпигунство та забезпеченні інших заходів безпеки підприємств.

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

- охарактеризувати термінологічні аспекти категорії «промислове шпигунство» в контексті його відмінності від економічної розвідки;
- дослідити класифікацію видів промислового шпигунства;
- проаналізувати тенденції розвитку та ,відповідно, методи протидії та боротьби з проявами промислового шпигунства в рамках Європейського Союзу та Східної Європи;
- 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.

Об'єктом дослідження є феномен промислове шпигунство.

Предметом дослідження є система запобігання і боротьби з промисловим шпигунством в Україні.

1. ПРОМИСЛОВЕ ШПИГУНСТВО І КОНКУРЕНТНА РОЗВІДКА: ПОНЯТТЯ, ВИДИ ТА ОСНОВНІ КРИТЕРІЇ ВІДМІННОСТІ

На сучасному етапі розвитку суспільства масштаби економічного шпигунства різко зростають. Інформація про результати чужих прикладних і фундаментальних досліджень дозволяє заощадити власні сили й кошти і зосередити всю увагу на виробництві та маркетингу. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкуренції як «війни всіх проти всіх» роблять викрадення чужих таємниць особливо прибутковою, і тому дуже перспективною справою.

Якщо звернутись до американського досвіду, то ще в 1990 р. Президент США Джордж Буш у своїй доповіді «Стратегія США в галузі національної безпеки» проголосив економічну розвідку пріоритетним напрямком у діяльності американських спецслужб. Наприкінці 1993 р. Біл Клінтон дав вказівку керівництву розвідувального співтовариства США про поглиблення досліджень у сфері економічної розвідки. Було виділено три пріоритетних напрямки розвідки:

– макроекономічна – збір стратегічної інформації про глобальні процеси в економіках інших держав;

– мікроекономічна – збір тактичної й оперативної інформації про діяльність окремих компаній;

– контррозвідка – протидія замахам іноземних комерційних фірм і державних спецслужб завоювати американські торгово-економічні й технологічні секрети [4].

Втрати Німеччини від промислового шпигунства оцінюють в 20 млрд. євро щорічно. Втрати США – від 100 млрд. дол. США щорічно [2].

Промислове шпигунство щодо підприємництва — це різновидність економічного шпигунства, якому притаманне звуження розмірів завдань з одержання інформації, що цікавить, від державного — до масштабу однієї або

декількох фірм-конкурентів. Отже, для підприємництва промислове шпигунство — просто спосіб конкурентної боротьби.

Промислове шпигунство, зазвичай, має дві мети:

−отримання інформації конкурентів, передусім конфіденційної, про тактичні й стратегічні наміри їхнього підприємництва;

−здобуття конкурентної переваги на ринку, через знищення або витіснення конкурента.

Промислове шпигунство описують як вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність.

Варто одразу розмежувати поняття розвідка і промислове шпигунство. Метою як промислового шпигунства, так і конкурентної розвідки є одержання інформації, яка б дала змогу вибороти конкурентну перевагу на ринку. Головною різницею між конкурентною розвідкою та промисловим шпигунством є методи й способи отримання інформації. Все, що використовується розвідником, є законним (тобто дотримуються етичні норми). Промисловий шпіонаж, навпаки, передбачає нелегальні технології й методи. Служба конкурентної розвідки користується тільки відкритими джерелами, оскільки робота розвідника — інформаційно-аналітична, тобто збір та обробка різних даних, що впливають чи можуть вплинути на розвиток бізнесу.

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

Сукупність методів, притаманних промисловому шпигунству, можна об'єднати у дві групи.

1) Методи агентурні.
2) Методи технічні.

Агентурний метод одержання інформації включає два напрямки діяльності: вербування і впровадження своєї людини.

Методи вербування – гра на бажанні самоствердитись в очах оточення, на самолюбстві, авантюризмі, марнославстві, на лестощах з боку «друзів». Одним із методів добору кандидатів для подальшого вербування є інсценоване інтерв'ю нібито з метою пошуку кандидатів на престижну роботу.

Наступним методом є шантаж. У даному випадку вся отримана в результаті попереднього інсценованого інтерв'ю інформація використовується для шантажу. І останній метод – хабар, гроші.

До технічних методів промислового шпигунства (виробництво й збут такої техніки врегульовано законодавчо) належать:

–Радіопрослуховування. Якісні результати дає монтаж в приміщеннях конкурентів електронних підслуховуючи пристроїв – радіозакладок. Їхнє застосування обтяжує проблема впровадження в потрібне місце і, до того ж, навіть вдало встановлений пристрій може просто вийти з ладу. Безліч підприємств продають системи пошуку таких приладів. Ці системи дозволяють розкривати закладку майже в 100% випадків. Більш того, виявлений пристрій може бути використаний для умисної дезінформації конкурента. Вибір «жучків» великий, коштують вони від 10–20 дол. до 100–200 дол., однак є і саморобні — примітивні [25].

–Підключення до ліній зв'язку. За даними спеціалістів, в Україні найпоширенішим з усіх технічних засобів зняття інформації є негласне підключення до телефонних ліній [20]. Прослуховування телефонів популярне через дешевизну й простоту. Випадки прихованого відеоспостереження одиничні. Сьогодні відомо багато методів «сканування» телефонних переговорів — від простих, як, зокрема, перехоплення сигналу радіотелефонів, до технічно складних і дорогих, як високочастотне нав'язування (коли телефонна лінія може використовуватися не тільки як безпосереднє джерело повідомлення, а й як канал передачі інформації, отриманої з іншого джерела, наприклад, за допомогою акустичного «жучка», а також як джерело живлення для спеціальних підслуховуючих пристроїв, що передають інформацію по радіоканалах).

–Мобільне шпигунство За словами продавців захисного устаткування, за останній рік суттєво зріс попит на блокатори стільникових телефонів. Існують зовнішні пристрої, при використанні яких навіть відключений мобільний телефон (якщо з нього не витягнуть акумулятор) можуть активувати і «змусити» його передавати розмову власника та й усі розмови в приміщенні, де знаходиться цей телефон. Для протидії «мобільному» прослуховуванню спеціалісти розробили різноманітні шумогенератори для мобільних телефонів (найпростіші з них коштують 250–300 дол. США). Притому, якщо такий іноземний пристрій просто робить 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. доларів США [2].

–Інтернет-шпигунство. Новий напрям промислового шпигунства, що набуває популярності в усьому світі, а також і в Україні, — це отримання конфіденційної інформації за підтримкою Інтернету.

В Україні більше 22 підприємств мають ліцензію на розробку й виготовлення підслуховувальних закладних приладів [17].

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

Конкурентна розвідка — це сталий процес нагромадження, збору, структуризації, аналізу даних про зовнішнє й внутрішнє середовище підприємства й надання вищому менеджменту підприємства інформації, що дозволяє йому передбачати зміни в обстановці й приймати вчасні оптимальні рішення щодо керування ризиками, впровадження змін у підприємництві й відповідних заходів, спрямованих на задоволення майбутніх запитів споживачів і підтримку прибутковості.

Важливою є та обставина, що конкурентна розвідка реалізує збір інформації про навколишнє бізнес-середовище тільки легальними методами.

Методи конкурентної розвідки схематично можна поділити на цілком законні («білі») та методи, котрі за своєю формою не порушують норм законів, але не завжди відповідають морально-етичним нормам ведення чесної конкурентної боротьби («сірі» методи).

До першої групи методів конкурентної розвідки, тобто до легальних, належать:

−вивчення, обробка та аналіз матеріального заохочення співробітників конкурента з метою прилюдної інформації про конкурента.

−вивчення й аналіз публікацій конкурента.

−До другої групи методів належать такі:

−вивідування інформації у службовця конкурента;

−«переманювання» фахівців конкурента і отримання в них відомостей, що мають обмежений доступ;

−отримання конфіденційної інформації;

−проведення підставних переговорів з метою вивідування конфіденційної інформації;

−одержання потрібної інформації про конкурента через зв'язки в контролюючих та правоохоронних органах.

Залежно від спрямованості виділяють наступні види конкурентної розвідки:

1. Розвідка проти компанії.

а) методичний аналіз інформаційного поля. Як відомо, чим більше підприємство, тим легше зібрати й проаналізувати інформацію, оскільки великий бізнес, зазвичай, є публічний і завжди намагається заявити про себе й свої дії самостійно. Хоч дійсно реальні показники завжди приховуються, це обумовлено податковою політикою. Аналіз відповідної інформації в пресі дає основу для досить точних висновків про стратегію підприємства, його виробничі потужності, плани, величини його прибутку і оборотів. А також, за

присутності потужного аналітичного підрозділу, проведення дослідження аналітичних статей окремих експертів (іноді ще й службовців підприємства-конкурента) дає виразну картину його мети й стратегії .

б) Аналіз статутних і установчих документів та організаційної структури підприємства. Ця інформація не підпадає під категорію комерційної таємниці, її вільно отримати у відповідних органах влади. Аналіз структур і їхніх господарських взаємозалежностей допоможе дізнатися про склад групи контрагентів, їхні перспективи.

Для складання цілої картини потрібне повторне дослідження інформаційного поля по кожному із суб'єктів розробки.

в) Співбесіда при «наймі» на роботу працівників конкурента, установлення хибних партнерських зв'язків через дружні підприємства

Якщо стоятиме потреба уточнення докладної інформації, можна скористатися опитуванням службовців підприємства щодо того, що їх інтересує. Для цього можуть бути застосовані різні форми маскування й легендування: установлення помилкових партнерських зв'язків через дружні підприємства, співбесіда при «наймі» на роботу тощо.

2. Розвідка проти персони:

а) Аналіз біографії керівників компанії конкурента.

б) Аналіз комунікативних контактів і ділових зв'язків осіб, які приймають рішення.

в) Аналіз позаділового життя керівників компанії конкурента.

3. Фінансовий моніторинг. Загрози будуть оцінені недостатньо, якщо не здійснюється фінансовий моніторинг. Фінансовий моніторинг дозволяє розкрити економічну потужність загроз, використовуючи наступні методи:

а) Метод аналогії. Потрібно знати декілька аналогічних підприємств із схожою структурою бізнесу, щоб оцінювати роль оборотів і рентабельності досліджуваного бізнесу.

б) Метод розрахунку за непрямими ознаками. Якщо відомі виробничі потужності підприємства, знаючи середньогалузевий відсоток завантаження цих потужностей, з огляду на сезонний фактор і становище підприємства на

ринку, можна розрахувати передбачувану рентабельність й систему виторгу. Або виконавши аналіз дистриб'юторської сітки конкурента й провівши належні заходи щодо розвідки відносно підприємств-конкурентів, можна оцінити економічну потужність підприємства.

в) Метод інтерполяцій. Одержавши дані про підприємство з органів державної статистики й, знову ж таки, знаючи показники зростання ринку й середньогалузеві економічні показники, можна розрахувати прогнозовані показники виторгу.

4. Оцінка інвестиційних проектів конкурентів. Якщо розвідувальні дії здійсняються регулярно, то інформації буде досить для проведення швидкої оцінки інвестиційних проектів конкурентів, використовуючи наступні методи:

а) Метод експертного інтерв'ю. Якщо інвестиційні проект не є інноваційним, то для оцінки ризиків проекту буде вигідний метод опитувань спеціалістів, що вже брали участь в схожих проектах. Необхідною є формалізація результатів опитування й присвоєння коефіцієнтів ваги думкам окремих експертів. У даному разі одержується матриця, що дозволить провести багатофакторний аналіз неуспішності або успішності потенційного проекту.

б) Вивчення адміністративного й ділового оточення конкурента. Цей метод використовується в основному для аналітичної обробки вже наявних матеріалів.

Отже, використання методів економічної розвідки необхідне найперше за таких випадків:

−появи нового конкурента;

−зміни поводження на ринку конкурента;

−відкриття нового напряму бізнесу;

−появи у бізнесі проблем зовнішнього характеру (компрометуючі факти в пресі, зриви поставок, поява проблем з контролюючими органами влади).

У зв’язку з певними історично-культурними особливостями суб’єкти недержавної правоохорони, а саме охоронні та розшукові агентства Великобританії, протягом багатьох років мають специфічний почерк: відмінні

особливості діяльності, принципові, властиві тільки для них, методи і напрями діяльності.

У Великобританії постійно диференціюється і розширюється попит на послуги приватних розшукових агентств, які здатні реалізувати характерні 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 видобуванням конфіденційної інформації про конкурентів або інших приватних підприємств [5].

У цілому до кола питань, що вирішуються британськими службами безпеки та приватними агентствами, передусім входять: забезпечення перевірки та безпеки службових приміщень; розслідування злочинів, пов'язаних із комп'ютерними системами і шахрайством, виявлення спеціальної техніки, підслуховувальних пристроїв; організація особистої охорони працівників фірм і клієнтів.

Однією з дієвих форм і приватної, і загальної профілактики та викриття злочинів у Великобританії уважається виплата грошових винагород за надання інформації. Так, тільки 2005 р. банки Лондона виплатили близько 150 тис. ф. ст. громадянам як винагороду [17, с. 23]. Загальна профілактика охоплює сукупність заходів економічного, політичного, правового, організаційно-ідеологічного характеру на рівні корпорації, фірми, підприємства як об'єкта економічної безпеки. Свідченням цього є насичення ринку Англії професійною 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, випробування та перевірки кадрів для роботи в комерційних структурах, на промислових об'єктах, особливо в службах безпеки підприємництва.

Розглядаючи німецький досвід адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання, слід відзначати, що в цей час

банки, державні установи, 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 охорони та безпеки. Цікаво, що створені за ініціативою і за підтримки спецслужб, служби безпеки, детективно-охоронні фірми та агентства виконують певну частину оперативно-розшукової діяльності. Вони підтримують систематичні контакти і обмінюються оперативно значущою інформацією з органами контррозвідки і поліції, в деяких випадках здійснюючи навіть колективні заходи. Така діяльність зовсім не характерна, зокрема, для служб безпеки в США і Великобританії, а також України.

Однак є й ряд проблем. Так, зосередження поліції ФРН на її першорядних завданнях у зв'язку зі скороченням персоналу створює дефіцит запобігання злочинності та сприяє зростанню ролі співробітництва з приватними службами, які визнані невід'ємною складовою внутрішньої безпеки і беруть участь у безпеці руху, забезпеченні правопорядку, 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 [8, с. 227].

З огляду на характерні особливості, у Німеччині можна виділити дві великі групи приватних служб безпеки [17, с. 24]:

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

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.

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

Проблеми безпеки економічної діяльності на території Німеччини посідають істотне місце. З цього питання складаються спеціальні домовленості, які дотримуються протягом 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 МЗС ФРН, розвідки, відомства федерального канцлера [15, с. 13].

Ще однією особливістю є те, що для відкриття служби безпеки в Німеччині необхідно спеціальний дозвіл місцевої влади, наприклад, на укладання контрактів із підприємством, замовником, 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, приміром, технічних, фінансових.

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 витік даних, що становлять таємницю як у процесі виробничої діяльності фірм, так і за їх взаємодії з державними, найперше іноземними установами. Також вдосконалюється законодавство про відповідальність осіб, які допустили витік

відомостей, що становлять комерційну таємницю. Отож, німецьке законодавство зараз в сфері адміністративно-правового забезпечення безпеки діяльності суб'єктів господарювання, що стосується протидії промисловому шпигунству та захисту інтелектуальної власності в контексті протидії промисловому шпигунству, достатньо всебічно і комплексно захищає комерційну, виробничу, банківську та податкову таємницю від несанкціонованого розголошення. У випадку ж розголошення таємниці передбачено покарання строком до 3-х 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 повинні відшкодувати потерпілій стороні збитки, що з'явилися у результаті розголошування таємності підприємства. Сума збитку може сягати дуже великих розмірів. Злочином вважається також співпраця або підбурювання 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. З ціллю забезпечення відповідної діяльності служб приватної безпеки, діє Рада приватної безпеки.

До її компетенції входять наступні завдання:

а) перевірка здійснення приватними фірмами норм безпеки відбору і прийняття на службу своїх службовців;

б) координація діяльності і надання допомоги у визначенні функцій і змісту контролю та перевірки, розроблення вказівок компетентним органам у цій області;

в) направлення на адресу ради доповідей приватних фірм безпеки;

г) розгляд скарг у зв'язку із незаконними діями приватних служб безпеки і розроблення пропозицій міністрові внутрішніх справ із цих питань;

ґ) інспекція центрів підготовки службовців приватних організацій безпеки та інших спеціалізованих установ з метою перевірки їх можливостей щодо професійного навчання персоналу підрозділів охорони і захисту тощо.

г) дозвіл на уживання додаткових коштів приватними фірмами безпеки.

Вивчаючи особливості служб безпеки недержавної правоохоронної діяльності в контексті протидії промисловому шпигунству 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 в контексті протидії промисловому шпигунству, 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 функціонерів страхових компаній, комерційних банків і адвокатських контор. Попередніми роками у Франції з'явилося серйозне занепокоєння у зв’язку зі помітною кількістю колишніх поліцейських, котрі переходять на роботу в приватні охоронні та детективні компанії [2, с. 74].

Така тенденція характерна і для України. У зв’язку з цим у Франції введена неухильна реєстрація в МВС приватних детективів, а також повідомлення МВС у випадках найму на роботу осіб зазначеної категорії.

З огляду на географічне положення, звичаї і традиції, близькі норми законодавства країнам Північної Європи (Норвегія,Фінляндія, Данія і Швеція) властиві значно спрощені підходи до організації діяльності комерційних і промислових служб безпеки з протидії промисловому шпигунству. У цих країнах охоронні та детективні бюро належать до категорії приватних підприємств. Мається на увазі те, що їхня реєстрація, оподаткування, фінансування, правове становище і робота регламентуються загальними нормами чинного законодавства. Зазначимо, що служби безпеки суб’єктів господарювання та місцеві державні правоохоронні органи активно діють через впливові національні спілки підприємців. Уповноважені службовці спецслужб на підприємствах разом з кадровим апаратом служб безпеки суб’єктів господарювання здійснюють кваліфіковану спецперевірку осіб, що створюють агентурну мережу, допускаються до роботи з таємними матеріалами і

документами, поширюють серед персоналу досвід контррозвідувального забезпечення закріплених об’єктів. Простежується тенденція до розширення призначень недержавних і державних правоохоронних органів щодо адміністративно-правового забезпечення безпеки діяльності суб’єктів господарювання в контексті протидії промисловому шпигунству 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 шпигунством. Головна 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 промисловому шпигунству.

Аналізуючи прикладний досвід країн Європи у галузі адміністративно-правового забезпечення безпеки діяльності суб’єктів господарювання, що стосується захисту та охорони об’єктів інтелектуальної власності від проявів 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 кооперації з державними правоохоронними органами, з ціллю підвищення ефективності роботи з попередження правопорушень і злочинів, а також актів промислового шпигунства.

2. ДОСЛІДЖЕННЯ РОЗВИТКУ ТА ПРОБЛЕМИ ПОДОЛАННЯ ПРОМИСЛОВОГО ШПИГУНСТВА В УКРАЇНІ

Промислове шпигунство в Україні вважається свого роду різновидом економічного шпигунства, який характеризується звуженням кола завдань, з тою метою, щоб одержати інформацію про одного або декількох конкурентів нелегітимним шляхом. Таким чином, для підприємства промислове шпигунство є єдиним способом конкуренції. Якщо суб'єктом в контексті економічного шпигунства (активної сторони) виступає країна в особі свого розвідувального підрозділу, то для промислового шпигунства це є окрема людина, фірма, компанія, юридична або фізична особа.

Промислове шпигунство в Україні, як правило, має дві мети: отримати інформацію про конкурентів, наприклад, конфіденційних стратегічних і тактичних напрямків їхньої діяльності; отримати конкурентну перевагу на ринку через усунення або дискримінацію конкурента. В наукових джерелах описується категорія промислового шпигунства як форма недобросовісної конкуренції в контекст незаконної діяльності з придбання інформації, яка становить комерційну цінність. Ключовим словом в цьому визначенні є поняття «незаконноості». Історичний аспект бізнес-розвідки торкається військових і політичних шпигунських операцій. Дослідження актуальних джерел інформації про основні тенденції і наміри діяльності ділових конкурентів, аналіз ризиків і загроз, був професіонально виправданим на Заході, в країнах з більш розвиненими ринками, та отримав назву «конкурентна розвідка». Основна відмінність між конкурентною розвідкою та промисловим шпигунством полягає у різниці між методами і способами отримання інформації. Усі наявні різновиди бізнес-розвідки є законними. Промислове шпигунство навпаки охоплює незаконні методи і прийоми отримання інформації. Шпигунство полягає, головним чином, в оперативній роботі, зокрема, в незаконному за ангажуванні до середовища діяльності конкурента, прослуховуванні телефонних розмов, спостереженні, підкупі, шантажі, викраденні інформації і т.д.

Сукупність методів, придатних для промислового шпигунства в Європі, водночас і в Україні, можна розділити на дві групи: розвідувальні методи і технічні методи. Розвідувальні методи отримання інформації - це основа будь-якого роду шпигунства. Є два типи такого роду діяльності: рекрутмент або залучення третьої особи. Обидва методи мають свої властиві переваги. У кожній комерційній структурі є «друга» і «третя» особа-працівник, чиї знання і досвід дають їм можливість просування по службі та отримання доступу до конфіденційної інформації. Якщо метою промислового шпигунства є знищення конкурентних фірм або отримання торговельних (в т.ч. комерційних) таємниць, то залучення осіб ззовні мають значні переваги, оскільки дають впевненість в людині.

Перейдемо до актуальних в Україні технічних методів промислового шпигунства з метою отримання інформації. Виробництво і продаж таких пристроїв в Україні регулюється законодавством. Для перехоплення і запису аудіо інформації існує широкий спектр різних інструментів, мікрофонів, електронних стетоскопів, радіомікрофонів, мікрофонів, лазерних, магнітних записуючих пристроїв. На думку деяких українських учених, в Україні, найпоширенішим з усіх технічних засобів пошуку інформації є негласне підключення до телефонної лінії. Прослуховування телефонів є популярним через простоту встановлення і дешевизну. Випадки відеоспостереження є поодинокими. Це основні методи промислового шпигунства, які в свою чергу діляться на декілька способів отримання конфіденційної інформації (дезінформації, шантаж і підкуп, використання правоохоронних органів).

Згідно з дослідженнями Якубівської Ю.Є. [21] 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 1

Види та рівень шахрайства в Україні та світі у 2014 р. [18]

Географічний регіон	Хабарництво та корупція (%)	Прояви недобросовісної конкуренції (в т.ч. промислове шпигунство), (%)
Україна	60	23
Центрально-Східна Європа	36	12
Світовий рівень	24	7

Джерело: Складено автором на основі: Украина. Всемирный обзор экономических преступлений [Електронний ресурс] / PWC. – Режим доступу: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2014_report_ukraine_rus.pdf

Як бачимо з табл..1., рівень корупції в Україні є значно вищим від рівня проявів недобросовісної конкуренції, в контексті якої ми розглядаємо промислове шпигунство. Однак рівень проявів недобросовісної конкуренції в Україні (23%) майже втричі вищий ніж у світі (7%).

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.

Таблиця 2

Порівняльна характеристика показників окремих видів економічної злочинності в Україні та світі у 2014 р. [18]

Вид	Україна (%)	Світовий показник (%)
Недобросовісна конкуренція	23	7
Кіберзлочинність	17	23

Джерело: Складено автором на основі:Украина. Всемирный обзор экономических преступлений [Електронний ресурс] / PWC. – Режим доступу: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2014_report_ukraine_rus.pdf

Як бачимо з табл..2, для України у порівнянні зі світовим показником більш поширеним злочином у сфері економічної злочинності є недобросовісна конкуренція (яка згідно досліджень включає прояви промислового шпигунства). На противагу цьому кіберзлочинність в Україні становить близько ¾ світового показника, що пояснюється наявністю застарілих технологій та відсутності заінтересованості в промисловому кіберпросторі ззовні.

В Україні, широко поширені в області промислового шпигунства цільові атаки. Діяльність такого роду раніше досліджувалася в тексті наукових статей [21-25], в яких зазначено, що такий крок необхідний для захисту національних операторів від промислового шпигунства і запобігання проявам даного процесу

з їхнього боку. Це вимагає не тільки державної підтримки, але, насамперед, гармонізації законодавства в галузі прав інтелектуальної власності, зокрема, по відношенню до захисту від проявів недобросовісної конкуренції. Ця комбінація повинна нейтралізувати потенційні загрози, а також стимулювати економічне зростання в контексті розвитку системи економічної безпеки.

Для України проблема промислового шпигунства не є новою. Розглянемо деякі з них. У 2013 році громадяни Корейської народно-демократичної республіки були викриті в Україні співробітниками СБУ за повідомленням від працівника, конструкторського бюро «Південне», який був звільнений від відповідальності. Промислових шпигунів цікавили секретні дані, що стосувалися 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 коментувала. В даному випадку розвідувальна діяльність Корейської народно-демократичної республіки безпосередньо стосувалася і Росії. Зокрема, конструкторське бюро «Південне» як в минулому розробник міжконтинентальних балістичних ракет (деякі з яких залишаються на озброєнні Росії), брало активну участь у спільних україно-російських проектах. Зокрема, це запуски розроблених в конструкторському бюро «Південне» ракетоносіїв «Зеніт», які здійснювало на той час спільне підприємство «Sea Launch», ракетоносіїв «Дніпро», які здійснювало спільне російсько-українське підприємство «Космотрас» з космодрому Байконур і ракети-носія «Циклон» російсько-українського підприємства «МКУ» («Міжнародні Космічні Послуги») [14]. А відтак, в даному випадку організація промислового шпигунства проти України зачіпає і російські інтереси.

Проте нездоровий 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. 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» був запущеним в серію, літаки базувалися на китайському авіаносці «Shi Lang» [1]. 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» [14].

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». Співпраця України з європейськими країнами по проекту цього літака стала, мабуть, самою яскравою 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», що являє собою аналог до українського літака, документація на який вивчалася європейською стороною [14].

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.

Таблиця 3

Види шахрайства та ймовірності їх активності в Україні в 2015-2016 рр. (за результатами опитування міжнародної компанії PWC) [18]

Вид шахрайства	Очікувана ймовірність (% від загальної кількості респондентів)
Хабарництво і корупція	42
Порушення прав інтелектуальної власності	36
Незаконне присвоєння майна	35
Махінації з фінансовою звітністю	25
Кіберзлочинність	25
Прояви недобросовісної конкуренції	24
Відмивання коштів	17
Податкове шахрайство	14
Торгівля інсайдерською інформацією	12
Промислове шпигунство	10

Джерело: Украина. Всемирный обзор экономических преступлений [Електронний ресурс] / PWC. – Режим доступу: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2011_report_ukraine_rus.pdf

Аналізуючи дані табл..3, можемо об’єднати такі види шахрайства, як: порушення прав інтелектуальної власності, кіберзлочинність, прояви недобросовісної конкуренції, торгівля інсайдерською інформацією, і власне промислове шпигунство (для наочного показу ми виділили дані види у такбиці), оскільки вони найбільш повно доповнюють один одного в контексті прояву останнього. Низький показник очікування саме промислового шпигунства (а саме 10%) пояснюється насамперед низьким рівнем інноваційного розвитку України, відсутністю державної підтримки та наявністю застарілих технологій на виробництвах, які не викликають заінтересованості з боку третіх осіб.

3. 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.

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» [13].

2. Закон України «Про Антимонопольний комітет України» [10].

3. Закон України «Прозовнішньоекономічну діяльність» [11].

4. Закон України «Прообмеження монополізму і недопущення недобросовісної конкуренції у підприємницькій діяльності» [12].

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 [13]. 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 діяльност» [12]. Проте, Закон [12] 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» [29], 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 [27-30], 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) [6].

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» [29] 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 [7] (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 [27]. 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.

ВИСНОВКИ

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.

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.

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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Аширлієва Ш. Промисловий шпіонаж на підприємствах України: правові аспекти боротьби: [Електронний ресурс] / Ш. Аширлієва, Є. Малюкова. - Режим доступу: http://5fan.info/jgernapolatyujgqas.html
2. Бизнес разведка. Внедрение передовых технологий / Кристофер Бо-ган, Майкл Инглиш; пер. с англ.; под общ. ред. Б. Л. Резниченко. – М.: Вершина, 2015. – 328 с.
3. 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.
4. Жаліло Я. Економічна стратегія держави: теорія, методологія, практика: монографія / Я. Жаліло. – К.: НІСД, 2013. – 368 с.
5. Информационный менеджмент: новые технологии // Бизнес-разведка. – 2012. – № 7. – С. 14. [Електронний ресурс]. – Режим доступу: http://www.amulet.ru/articles/2006/07/046373.htm
6. Кримінальний кодекс України від 5 квітня 2001 р. № 2341–III // Відомості Верховної Ради України. – 2001. – № 25–26.
7. Митний кодекс України від 21 квітня 2012 р. //„Голос України”. - №73-74 - 2012.
8. 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.
9. 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.

10. Про Антимонопольний комітет України: Закон України від 26 листопада 1993 року // Відомості Верховної Ради України. — 1993. — № 50. — Ст. 472.

11. Про зовнішньоекономічну діяльність: Закон України// Відомості Верховної Ради України.-1991.-К 29.

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

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

14. 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

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

16. Ткачук Т. Ю. Сучасні реалії та загрози інформації з обмеженим до-ступом на підприємстві / Т. Ю. Ткачук. – Право України. – 2011. – № 3. – С. 243–252.

17. 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.

18. Украина. Всемирный обзор экономических преступлений [Електронний ресурс] / PWC. – Режим доступу: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2014_report_ukraine_rus.pdf

19. 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

20. Франчук В.І. Загрози корпоративній безпеці як об'єкт дослідження / В.І. Франчук // Актуальні проблеми економіки. – 2009. – №9. – С.148-154.

21. 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.

22. 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.

23. 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.

24. 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.

25. Якубівська Ю.Є. Цільові атаки в контексті промислового шпигунства» / Ю.Є.Якубівська // Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: сб. науч. тр. - Т.2, Донецк: ДонНУ, 2014. – С. 368-372.
26. Griffin Robert J. Just Do It: Establishing a Corporate Business Intelligence Function at IBM, Proceedings, SCIP 12th Annual International Conference and Exhibits. – Vol. II. – 2004. – P. 123–133.
27. TRIPS (WTO Agreement on Trade Related Aspects of Intellectual Property Rights): <http://www.wto.org/english/tratop_e/trips_e/trips_e.htm>
28. Turaliński, Kazimierz. 2011. Wywiad gospodarczy i polityczny. metodyka, taktyka i źródła pozyskiwania. Radom: "Media Polskie". (446 s.).
29. Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, t. j. Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.
30. Ustawa z 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym, Dz. U. z 2007 r. Nr 171, poz. 1206, ze zm.