УДК 342.98:35.08

О.М. Кравченко,
аспірант кафедри конституційного, адміністративного та господарського права Академії праці, соціальних відносин і туризму

КОМЕРЦІЙНЕ ШПИГУНСТВО

Анотація. У статті досліджено актуальні проблеми охорони комерційної таємниці суб'єктів господарювання, від комерційного шпигунства. Потрібно зауважити, що в Україні відсутній Закон «Про комерційну таємницю», який наприклад існує у більшості країн СНД та у США. Також потрібно зазначити, що підприємствам, установам і організаціям потрібно будувати сучасну систему захисту від комерційного шпигунства.

Ключові слова: комерційна таємниця, охорона комерційної таємниці, комерційне шпигунство, промислове шпигунство, економічне шпигунство, недобросовісна конкуренція.

Постановка проблеми. Без надійного захисту інформації, що становить комерційну таємницю, підприємство, установа чи організація може залишитись без прибутку або й взагалі припинити своє існування. Саме тому, надійний захист комерційної таємниці і буде сприяти надійній протидії комерційному шпигунству.

Актуальність наукової статті підвищується в зв'язку з загрозами, які існують у сучасному світі від комерційного шпигунства, щодо комерційної таємниці, а саме інформації, що має комерційну цінність.

Аналіз досліджень. В основу написання даної наукової статті покладено аналіз нормативно-правових актів України з питань комерційної таємниці, та погляди на цю проблематику науковців. А саме, різним аспектам проблематики захисту комерційної таємниці від комерційного шпигунства в дослідженнях приділяють увагу такі фахівці, як О. Дудоров, О. Івченко, Г. Жаворонкова, В. Вовченко, І. Степанов, Д. Зеркалов, І. Березін.

Проведений аналіз свідчить, що в Україні вирішенням проблеми повґязаної з комерційною таємницею, повинно стати побудова дієвої системи сучасного захисту комерційної таємниці на підприємстві, виходячи звичайно з фінансових можливостей.

Метою даної наукової статті є визначення найбільш ефективних методів протидії комерційному шпигунству.

Виклад основного матеріалу. Спочатку потрібно визначити, що таке комерційне шпигунство — це цілеспрямована поведінка винної особи, котра може діяти з власної ініціативи або, як правило, за завданням того, хто зацікавлений у вилученні і заволодінні комерційною таємницею [1].

У статті 231 Кримінального кодексу України (далі — ККУ) незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, караються штрафом від трьох тисяч до восьми тисяч неоподаткованих мінімумів доходів громадян. А у статті 232 ККУ розголошення комерційної або банківської таємниці, умисне розголошення комерційної або банківської таємниці без згоди її

власника особою, окрім штрафу від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян, ще й з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років [2].

В статті 164 з позначкою 3 недобросовісна конкуренція, Кодексу України про адміністративні правопорушення, також передбачена матеріальна відповідальність, а саме накладання штрафу [3].

На нашу думку, досить м'яке покарання за розголошення комерційної таємниці в Україні на противагу законодавства ЄС чи США.

Економічна розвідка як невід'ємний компонент історичного розвитку продуктивних сил змінювала характер, форми і прояви відповідно до еволюції способів виробництва та рівня розвитку науки і техніки. Слід зазначити,що в історичному аспекті економічна розвідка більш давня, ніж військова та політична. За оцінкою незалежних західних експертів, у більш ніж 80% випадків результати розвідувальної діяльності використовуються саме для економічного (промислового) шпигунства [4].

Сьогодні термін «економічне, промислове, комерційне, науково-технічне шпигунство (розвідка)» означає активні дії, спрямовані на збір, крадіжку, накопичення і обробку цінної інформації, закритої для доступу сторонніх осіб. Мета цієї розвідки — нанесення шкоди конкуренту чи випередження його в економічному розвитку.

У звіті американської контррозвідки, опублікованому на початку листопада 2011 р., сказано, що оскільки США є лідером у галузі розробки нових технологій, «спроби іноземних держав зібрати інформацію щодо економічних та технологічних галузей США будуть продовжувати здійснюватися на високому рівні, представляючи зростаючу і постійну загрозу для економічної безпеки США». У доповіді стверджується також, що економічне шпигунство може коштувати економіці США не менш як 400 млрд. дол. США у рік, проте наголошується, що цифра може бути нижчою за різних методів збору даних і за браком інформації [5]. США виходять з того, що проти американської економіки регулярне шпигунство ведуть розвідки 23-х країн, у т.ч. провідні європейські держави [6]. Директор ФБР Роберт Мюллер (2001–2013 р.) визначив контррозвідку другим (після боротьби з тероризмом) пріоритетом для ФБР. Відділ економічного шпигунства призначений для боротьби із загрозою економічного шпигунства. Сфера зацікавленості відділу включає розробку навчальних та просвітницьких матеріалів, участь у конференціях, відвідування приватних підприємств, роботу з правоохоронними органами та розвідувального співтовариства на вимогу питань, і надання конкретної секретної та несекретної презентацій. ФБР дає такі рекомендації (шість кроків), які необхідно здійснити для захисту свого бізнесу від шпигунства: 1) визначення інсайдерів і аутсайдерів, що становлять загрозу для компанії; 2) ідентифікація і оцінка комерційної таємниці; 3) реалізація активного плану щодо охорони комерційної таємниці; 4) захист фізичних та електронних версій комерційної таємниці; 5) обмеження інтелектуальних знань лише з потреби знати основне; 6) забезпечення професійної підготовки співробітників з питань інтелектуальної власності компанії і план безпеки [7].

Тепер розглянемо реальний приклад притягнення до кримінальної відповідальності за комерційне шпигунство

у США з позбавленням волі винного китайского шпигуна на 7-м років. Американський суд штату Індіана у грудні 2011 р. засудив ученого, вихідця з КНР Кесюе Хуана до 7 років тюремного ув'язнення за промислове шпигунство на користь Китаю. За даними слідства, підсудний працював у двох великих аграрних американських компаніях Dow AgroSciences і Cargill Inc і в період з 2007 по 2010 роки, коли він керував дослідницькими проектами у сфері розробок органічних пестицидів, передавав до Китаю інформацію, що являє собою комерційну таємницю компаній. У подальшому дані, які стосувалися розробки і дослідження органічних пестицидів, використовувалися в стратегічних цілях КНР в науці. Про крадіжку біотехнологій та економічне шпигунство 46-річний вчений-інсайдер зізнався ще у серпні 2011 року. Згідно зі свідченнями експертиз його діяння завдали збитку компанії Cargill на 7–20 млн. дол. Помічник генпрокурора Бройер заявив: «Дії Кесюе Хуана становлять небезпеку для американської економіки і ставлять під загрозу лідерство США у сфері інновацій».

Щоб якісно зібрати факти проти китайського шпигуна, американські компанії тривалий час співпрацювали з ФБР і прокуратурою. Правоохоронні органи прочитували електронну пошту Кесюе Хуана. І після того як один з китайських аспірантів у Німеччині, якому Кесюе передаввкрадені матеріали, захотів їх реалізувати, у того був проведений обшук. У листопаді 2010 р. Кесюе Хуана офіційно звинуватили у викраденні інформації у Cargill Inc. [8].

А у справі "Lumex v Highsmith", позивач вимагав дотримання угоди, згідно з якою відповідачу (колишньому співробітнику) протягом 6 місяців після звільнення з компанії-позивача було заборонено перехід на роботу до конкурента. Суд також задовольнив цей позов, вказавши,що відповідач, ознайомлений в деталях маркетингової політики компанії, не вправі відразу ж переходити на роботу до конкурента. Однак суд відхилив позов компанії "FMC", яка вимагала повної заборони на перехід у будь-якій якості свого колишнього службовця до конкурента. Противники застосування доктрини «неминучого розкриття» вважають, що позивачі, які звертаються до неї, перетворюють угоду про не розкриття ділових секретів в угоду про неучасть у конкуренції. У зв'язку з цим необхідно забезпечувати інтереси компанії, вимушеної охороняти свої ділові секрети, не зачіпаючи прав службовців, які підшукують нову роботу [9].

Проблема охорони комерційної таємниці підприємства зводиться до необхідності і вміння керівників та працівників зберігати і захищати інформацію, що становить комерційну таємницю. Система захисту, щодо охорони комерційної таємниці будується відповідно до фінансових можливостей підприємства, установи чи організації. Існує світова статистика усереднених оцінок. Так, в Швейцарії кошти, витрачені на захист комерційних виробничих таємниць становлять 1,5–2% загальних виробничих витрат. За даними "The Boston Globe", компанії, що входять в число «500 самих щасливих», витрачають сотні тисяч доларів, щоб протистояти електронному шпигунству. [10].

Таким чином, можна зауважити, що чим більші фінансові можливості підприємства, установи чи організації, тим більше коштів можна витратити на захист комерційної таємниці, і виходячи з цього можна побудувати більш надійну систему захисту комер-

ційної таємниці, залучивши при цьому професіоналів своєї справи, яким потрібно за це платити гідну заробітньою плату.

11 травня 2016 року Конгресом США був прийнятий Defend Trade Secrets Act of 2016 (DTSA) — Закон про комерційну таємницю (далі — Закон). Закон передбачає можливість притягнення до відповідальності співробітників і підрядників за розголошення комерційної таємниці компанії. Примітно, що, якщо раніше кожен штат встановлював правила охорони комерційної таємниці окремо, то тепер це питання врегульоване і на федеральному рівні. Дія Закону поширюється на комерційні таємниці, пов'язані з продуктами та (або) послугами, які використовуються, або ж призначені для використання в торгівлі між штатами, а також у зовнішній торгівлі [11].

Закон передбачає наступні засоби захисту комерційної таємниці: 1. компанії можуть звернутися до суду з метою накладення арешту на незаконно привласнені предмети (носії інформації, які містять комерційну таємницю), що знаходяться у володінні співробітників/підрядників; 2. надання можливості накладення судової заборони з метою запобігання загрози або припинення незаконного привласнення комерційної таємниці з боку співробітника/підрядника.

Крім того, плата за надані адвокатські послуги (гонорари) підлягає стягненню з співробітника/підрядника в разі доведення умисних і зловмисних дій з його боку. У свою чергу, співробітник/підрядник може піти таким же шляхом у разі неправомірних звинувачень і вимагати відшкодування витрат на адвокатські послуги з боку компанії.

Згідно з цим Законом не буде вважатися незаконним розголошенням комерційної таємниці розкриття співробітником/підрядником такої інформації в державних органах, або ж в судовому порядку. Однак таке розкриття буде вважатися правомірним тільки в разі наявності підозр про порушення компанією норм законодавства. Кожен співробітник і підрядник компанії повинні бути проінформовані про можливість отримання такого імунітету в порядку передбаченому законодавством.

Дія норм цього Закону поширюється не тільки на громадян і компанії США, а й на фізичних та юридичних осіб інших країн, в тому числі України [11]. У Главі 4 Неправомірне збирання, розголошення та використання комерційної таємниці, Закону України «Про захист від недобросовісної конкуренції» ст.ст. 16-19, мова йде лише про визначення термінів про неправомірні дії щодо комерційної таємниці. А у Главі 5 цього закону вказано про відповідальність лише за недобросовісну конкуренцію, а саме накладання штрафу за недобросовісну конкуренцію, відшкодування шкоди, вилучення товарів з неправомірно використаним позначенням та копій виробів іншого суб'єкта господарювання [12]. В законодавстві України на рівні кодифікованих законів визначені основні положення про комерційну таємницю, а саме: ст. 162 Господарського кодексу України [13] передбачає правомочності суб'єктів господарювання, щодо комерційної таємниці, а глава 46 Цивільного кодексу України [14] встановлює право інтелектуальної власності на комерційну таємницю, зокрема, поняття комерційної таємниці, майнові права інтелектуальної власності на комерційну таємницю, охорону комерційної таємниці органами державної влади, а також строк чинності права інте-

лектуальної власності на комерційну таємницю. Тепер розглянемо Закон України «Про інформацію» (далі — Закон), а саме статтю 20 доступ до інформації, а саме за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. А стаття 21 Закону конкретизує, що інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація [15]. Закон України «Про доступ до публічної інформації» має визначення, що є таємна інформація. А саме стаття 8 таємна інформація — це інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю в тому числі й комерційну таємницю [16].

На думку Д.В. Зеркалова, який зазначає, що промислове шпигунство — це добування протизаконним шляхом конфіденційних відомостей про діяльність конкурентів, розкрадання відомостей, зі складових ноу-хау, ведення недобросовісної конкуренції, одержання персональних даних для їх використання в злочинних цілях. Сучасне промислове шпигунство — це ще й свідоме приведення в непридатність виробничого обладнання, інформаційних систем, здійснення психологічного тиску на співробітників з метою дестабілізації діяльності конкурента [17].

Тепер розглянемо технічні методи промислового шпигунства, які використовують техніку, виробництво й збут якої врегульовано законодавчо. Для перехоплення і реєстрації акустичної інформації існує величезний арсенал різноманітних засобів: мікрофони, електронні стетоскопи, радіомікрофони («радіозакладки»), лазерні мікрофони, апарати магнітного запису. Непомітне підкидання радіопередавальних (частіше закамуфльованих) пристроїв — досить поширений спосіб добування інформації. Такі предмети протягом декількох годин або декількох днів, поки не «сяде» елемент живлення, «усмоктують» всю озвучену в приміщенні інформацію. А якщо в зловмисників є бажання якомога довше «попрацювати» на «ворожій» території, то вони підключають «вухо» стаціонарно до електромережі; тоді підслуховувальний пристрій працюватиме доти, доки його не знайдуть. До речі, дешеві «жучки» можна використовувати для підслуховування розмов на вулиці, розкидаючи «шкідливих комах» у траві й листі, покриваючи такою «мережею» великі території. Їх можна придбати на будь-якому радіоринку, щоправда, якщо вас порекомендують авторитетні особи.

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

Пристрої прослуховування, які найчастіше встановлюють у офісах, залежно від джерел електроживлення

можуть бути стаціонарними або автономними. Зокрема, автономні «жучки» черпають енергію від невеликих батарейок або акумуляторів, до яких приєднують мініатюрні мікрофони й передавачі. Цих «комах» зловмисники непомітно «залишають» у приміщенні, де вони й працюють, поки вистачає заряду батареї (зазвичай 7—10 діб). Рік від року зростає популярність «мобільного» шпигунства й захисту від нього. За словами продавців захисного устаткування, за останній час значно зріс попит на блокатори стільникових телефонів. Існують зовнішні пристрої, при використанні яких навіть відключений мобільний телефон (якщо з нього не виймуть акумулятор) можуть активувати і «змусити» його передавати розмову власника та й усі розмови в приміщенні, де перебуває цей телефон. Для протидії «мобільному» прослуховуванню фахівці розробили різноманітні шумогенератори для мобільних телефонів. Причому, якщо такий закордонний пристрій просто створює шумові перешкоди в радіодіапазоні роботи мобільного телефону, то вітчизняні пристрої працюють більш широко: вони блокують таким чином, що «убивають» тільки синхроімпульс зв'язку з базою і ніяк себе не демаскують [18].

Проаналізуємо тепер ще один метод, а саме, агентурний метод одержання інформації — це основа основ, будь-якого виду шпигунства. Тут можливі два напрями діяльності: або вербування, або впровадження своєї людини. Обидва способи мають свої переваги. У будь-якій комерційній структурі є «другі» або «треті» особи, які за своїми знаннями й досвідом наближаються до рівня вищої ланки і які здатні самостійно вести свою гру. Результатом вербування може бути те, що вигідні замовлення підуть тим особам, які й організували бізнес-шпигунство на свою користь. Якщо кінцевою метою промислового шпигунства є знищення фірми-конкурента, або отримання комерційної таємниці, то варіант із впровадженням має істотні переваги, тому що довіра до своєї людини, звичайно, є більша.

Об'єктами агентурної розробки можуть бути не тільки, скажімо, «другі» або «треті особи» фірми-конкурента, а й будь-які співробітники, навіть, нижчої ланки. Вони цілком спроможні здійснити приховане встановлення відповідної апаратури («жучків», «комарів» тощо). Для цього необхідно від декількох секунд до двох-трьох хвилин. Для того, щоб встановити обладнання для перехоплення телефонних повідомлень, взагалі не потрібно проникати в офіс, варто лише знайти телефоніста, який погодиться знайти потрібний телефонний кабель. [4].

Висновки

Підводячи підсумки, потрібно зауважити, що на нашу думку в Україні потрібно систематизувати законодавство про комерційну таємницю в один закон, як наприклад це було зроблено у травні 2016 року в США, для більш ефективної боротьби з комерційним шпигунством та іншими сучасними загрозами. А також для підприємства, установи чи організації дуже важливим є побудова сучасної системи захисту інформації з обмеженим доступом, а саме охорони комерційної таємниці, звичайно виходячи з фінансових можливостей підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Дудоров О.О. Злочини у сфері господарської діяльності: кримінально-правова характеристика 2003.

2. Кримінальний кодекс України[Електронний ресурс] // Верховна Рада України. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14/page7

3. Кодекс України про адміністративні правопорушення [Електронний ресурс] // Верховна Рада України. — Режим доступу: http://zakon5.rada.gov.ua/laws/show/80731-10/page9

4. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контрозвідка // Юридичний журнал. — 2003. — № 7. — [Електронний ресурс] / Режим доступу: http://justinian.com.ua/magazines.php.

5. Китай і Росія: «агресивні» спонсори кібер-шпигунства — контррозвідка США // TheEpochTimes Україна 15.11.2011. [Електронний ресурс] / Режим доступу: http://www.epochtimes.com.ua/world/conflicts/kitay-i-rosiya-agresivni-sponsori-kiber-shpigunstvakontrrozvidka-ssha-99960.html.

6. Экономический шпионаж. [Електронний ресурс] / Режим доступу: http://www.agentura.ru/library/hirschmann/part4/.

7. EconomicEspionage.[Електронний ресурс] / Режим доступу: http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage. 8.Жаворонкова Г. Суд США засудив ученого до 7 років в'язниці за шпигунство на користь КНР / The Epoch Times Україна 22.12.2011. [Електронний ресурс] / Ре жим доступу: http://www.epochtimes.com.ua/world/conflicts/sud-ssha-zasudiv-uchenogo-do-7-rokiv-v-yaznitsi-za-shpigunstvo-na-korist-knr-100630.html.

9. Практика защиты коммерческой тайны и интеллектуальной собственности в США. — К.: Хрещатик, 1992. — 168 с.

10. Вовченко В.В. Проблемы защиты информации от экономического шпионажа / В.В. Вовченко, И.О. Степанов // [Електронний ресурс] — Режим доступу http://www.analitika.info

11. DEFEND TRADE SECRETS ACT OF 2016 [Електронний ресурс] — Режим доступу: https://www.congress.gov/bill/114th-congress/senate-bill/1890/text

12. Закон України України «Про захист від недобросовісної конкуренції» [Електронний ресурс] // Верховна Рада України. — Режим доступу:http://zakon5.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80

13. Господарський кодекс України [Електронний ресурс] // Верховна Рада України. — Режим доступу:http://zakon3.rada.gov.ua/laws/show/436-15/page6

14. Цивільний кодекс України[Електронний ресурс] // Верховна Рада України. — Режим доступу:http://zakon3.rada.gov.ua/laws/show/435-15/page9

15. Закон України «Про інформацію» [Електронний ресурс] // Верховна Рада України. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12

16. Закон України «Про доступ до публічної інформації» [Електронний ресурс] // Верховна Рада України. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/2939-1

17. Зеркалов Д.В. Безопасность бизнеса. Контрразведка и шпионаж / Д.В. Зеркалов — К. : Наук. світ, 2008. — 64-66 с.

18. Березин І. Промислове шпигунство, конкурентна розвідка, бенчмаркинг й етика цивілізованого бізнесу / Практичний Маркетинг. — 2005. — № 101. — 22 липня.

Кравченко А.Н.

Коммерческий шпионаж.

Аннотация. В статье исследованы актуальные проблемы охраны коммерческой тайны субъектов хозяйствования, от коммерческого шпионажа. Нужно заметить, что в Украине отсутствует Закон «О коммерческой тайне», который например существует в большинстве стран СНГ и в США. Также нужно отметить, что предприятиям, учреждениям и организациям нужно строить современную систему защиты от коммерческого шпионажа.

Ключевые слова: коммерческая тайна, защита коммерческой тайны, коммерческий шпионаж, промышленный шпионаж, экономический шпионаж, недобросовестная конкуренция.

O. Kravchenko

Commercial espionage.

Annotation. The article examines the topical problems of protection of trade secrets of economic entities from commercial espionage. It should be noted that in Ukraine there is no Law "On Trade secret", which for example exists in most CIS countries and in the United States of America. It should also be noted that enterprises, institutions and organizations need to build a modern system of protection against commercial espionage.

Keywords: trade secret, protection of trade secret, commercial espionage, industrial espionage, economic espionage, unfair competition.