УДК 347.775
DOI: http://dx.doi.org/10.18524/2411-2054.2019.34.169548

А. О. Гачкевич, канд. юрид. наук, старший викладач
Національний університет «Львівська політехніка»
Кафедра міжнародної інформації
вул. Степана Бандери, 12, Львів, 79013, Україна

Т. Р. Казарян, магістрант-дослідник з міжнародних відносин,
суспільних комунікацій та регіональних студій,
Національний університет «Львівська політехніка»,
вул. Степана Бандери, 12, Львів, 79013, Україна

ВЖИТТЯ АДЕКВАТНИХ ЗАХОДІВ ЯК ОЗНАКА КОМЕРЦІЙНОЇ ТАЄМНИЦІ: АНАЛІЗ ДОСВІДУ США

Стаття присвячується вивченню питання, які саме заходи необхідно вжити по відношенню до конфіденційної інформації підприємством для того, щоб вона визнавалася комерційною таємницею. В основі дослідження знаходиться аналіз особливостей правової системи США, держави з багатими традиціями у сфері охорони прав на комерційні таємниці.

Ключові слова: комерційна таємниця, розумні заходи, судова практика, економічне шпигунство, інформаційна безпека.

Постановка проблеми. Згідно зі ст. 505 Цивільного кодексу України однією з ознак комерційної таємниці є те, що відповідна інформація стала предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Разом з тим, перелік таких заходів не розкривається, а тому в кожному конкретному випадку може виникнути сумнів з приводу того, чи вжиті заходи є достатніми для наявності комерційної таємниці. Зважаючи на необхідність встановлення цієї ознаки, показовим є досвід США як держави, відомої багатими традиціями щодо забезпечення нерозголошення комерційних таємниць. Впродовж останнього століття у США сформувалася велика нормативно-правова база щодо охорони прав на комерційну таємницю, яка доповнює принципи загального права, що знаходили своє відображення у рішеннях американських судів. При цьому навіть у праві США розуміння вжиття «заходів щодо збереження її секретності», які отримали закріплення в законодавчій площині у формулюванні «розумні заходи», викликає ряд труднощів, що підтверджують результати дослідження С. Граймса та Ш. Мерфі. Вони проаналізували судові справи про захист комерційної таємниці у судах США за 2009-2018 рр. та виявили, що в 11 % справ вимоги позивача не задовольнялися через те, що він не обґрунтував факт вжиття «розумних заходів» [1].

Аналіз останніх досліджень і публікацій. З-поміж українських вчених поняття комерційної таємниці вивчається не тільки в контексті цивільно-правової підгалузі права інтелектуальної власності (Л. Дадерко, О. Світличний), але й в дослідженнях з господарського (О. Кравченко, С. Чікін, В. Черненко), кримінального (О. Курман, Л. Полуніна), міжнародного (О. Гороховська, І. Семенюк), трудового права (Н. Вапнярчук, Д. Юсупова). Відзначимо, що ознакам комерційної таємниці приділяли увагу такі вчені, як Н. Попова, М. Ситницький, Г. Сляднєва та ін. Деякі з них, наприклад, Г. Андрощук, розглядали більш детально явище комерційної таємниці в правовій системі США, згадуючи про категорію «розумних зусиль» (як варіант перекладу словосполучення «reasonable measures») [2, 82]. Однак окремих досліджень, присвячених аналізу питання вжиття адекватних заходів як ознаки комерційної таємниці, відштовхуючись від можливості запозичення досвіду США у сфері охорони комерційної

таємниці, до цього часу проведено не було, хоча воно є саме одним з тих питань, коли законодавчий припис особливо гостро потребує практичних рекомендацій.

Метою даної статті є розкриття переліку «адекватних існуючим обставинам заходів щодо збереження її секретності», вжиття яких передбачене законодавством України по відношенню до конфіденційної інформації, щоб та могла отримувати правову охорону як комерційна таємниця, виходячи з вивчення традицій правової системи США. Для досягнення поставленої мети було визначено наступні завдання: охарактеризувати ознаки комерційної таємниці відповідно до законодавства США; розглянути питання «розумних заходів» на основі судової практики США у справах щодо економічного шпигунства; розробити рекомендації з урахуванням досвіду США щодо вжиття підприємством адекватних заходів в українських реаліях.

Виклад основного матеріалу. Хоча правова система США істотно відрізняється від правової системи України, однак, комерційна таємниця охороняється в обох державах не тільки як об'єкт приватноправових відносин, але й нормами публічного права. Разом з тим, у США, зважаючи на особливості національного права, необхідність охорони комерційної таємниці забезпечується як на рівні штатів, так й у федеральних законах. У праві України судове рішення, як правило, не породжує виникнення загальнообов'язкової норми права, хоча й за останні роки спостерігається тенденція до надання окремим рішенням сили прецедентів, а також до створення рекомендацій вищими судовими органами, які, узагальнюючи існуючу практику, формулюють роз'яснення нижчим з приводу окремих, як правило, особливо проблемних правових аспектів (наприклад, у Листі Вищого господарського суду України порушується питання цивільної відповідальності за порушення майнових прав інтелектуальної власності на комерційну таємницю чи прав на «ноу-хау») [3]. Натомість у США як державі сім'ї загального права судовим прецедентам відводиться основоположне значення у розбудові правового фундаменту, але це аж ніяк не означає, що вони повністю замінюють нормативно-правові акти.

Одним з ключових завдань прийняття та вдосконалення законодавства щодо охорони комерційної таємниці є визначення ознак, за наявності яких певна інформація, пов'язана з діяльністю компанії, отримує статус комерційної таємниці. Здійснивши синтез судової практики наприкінці 1930 р., американські юристи підготували Зведення норм деліктного права, де було відображеним і поняття комерційної таємниці («будь-яка формула, схема, прилад або компілювання інформації, які використовуються в цілях будь-чиєї підприємницької діяльності та надають можливість набувати перевагу над конкурентами, котрі з ними не ознайомлені або не застосовують їх» (параграф 757) [4, с. 372][1]. При цьому, взявши за основу коментарі «b» до цього параграфу, можна зробити висновок, що вичерпного переліку загальноприйнятних ознак, на підставі яких та чи інша інформація автоматично набуває правового режиму комерційної таємниці, не існує та не може існувати, проте, на практиці важливе значення відводилося наступним факторам:

1) в якій мірі ця інформація є відомою поза підприємницькою діяльністю конкретного суб'єкта;
2) в якій мірі вона є відомою працівникам та іншим особам, які мають відношення до підприємницької діяльності конкретного суб'єкта;
3) які саме заходи було вжито суб'єктом для забезпечення її секретності;
4) цінність інформації для нього та його конкурентів;
5) обсяг зусиль чи грошових коштів, витрачених ним для розробки цієї інформації;
6) легкість або складність реалізації можливості набуття належним чином такої інформації або її копіювання іншими особами [4, с. 372].

[1] Зауважимо, що такий результат аналітико-правової діяльності як зведення норм, котрий відомий доктрині США, для пересічного українського юриста є не до кінця зрозумілим, однак, в загальному його можна порівняти зі згаданими вище рекомендаціями вищих судових органів України, які підлягають підготовці колегіальним органом – Американським інститутом права в даному випадку, до складу якого належать не тільки судді, але й інші авторитетні правознавці (понад 4000 осіб).

Таким чином, з великою ймовірністю національний суд США комерційною таємницею конкретного суб'єкта вважав би таку цінну для нього та його конкурентів, але важкодоступну інформацію, у створення якої він вкладав фінансові та інші ресурси і яка не була би повністю відомою поза діяльністю цього суб'єкта (в тому числі його працівникам, крім випадків, коли їх службові обов'язки вимагають цього), за умови вжиття ним широкого комплексу заходів, що мають на меті збереження її конфіденційності. На таких позиціях стояли і експерти Комісії з уніфікації права, які підготували у 1979 р. Єдиний закон про комерційну таємницю[1]. Під поняттям «комерційної таємниці» у тексті Закону розуміють «інформацію, включаючи формулу, зразок, компілювання, програму, прилад, метод, техніку або процес, що, по-перше, становить самостійну економічну цінність, як дійсну, так і потенційну, через те, що вона не є загальновідомою та не є легкодоступною за допомогою відповідних засобів для інших осіб, які можуть отримати економічну користь від її розголошення або використання, по-друге, стала предметом зусиль щодо забезпечення її секретності, які є розумними в даних обставинах» [5].

На території США також діє федеральний Акт про економічне шпигунство, що має на меті притягнення до кримінальної відповідальності за злочинні дії стосовно комерційної таємниці як об'єкта незаконної економічної розвідки. У відповідності до пар. 1839, крім розширеного пояснення, які саме відомості можуть бути комерційною таємницею, наведено дві ознаки, які дуже схожі до положень Єдиного закону («власник вжив розумних заходів для того, щоб ця інформація залишалася таємною»; «інформація породжує самостійну економічну цінність, дійсну чи потенційну, у зв'язку з тим, що вона не встановлюється безперешкодно громадськістю завдяки використанню відповідних засобів» [6].

Крім злочинів, якими займаються федеральні органи на підставі федерального законодавства, правоохоронна система кожного зі штатів здійснює кримінальне переслідування за злочини, передбачені кримінальними кодексами штатів. Вагомий вплив на формування кримінального законодавства більшості штатів мали положення Модельного кримінального кодексу, розробленого Американським інститутом права на початку 1960-их, однак, на відміну від Закону 1979 р., він не отримав настільки широкої загальнодержавної рецепції. Слід відзначити, що у Кодексі відсутні норми стосовно кримінальної відповідальності за злочини, пов'язані з комерційною таємницею. Разом з тим, в кримінальних кодексах окремих штатів таки існують статті, що забороняють крадіжку комерційних таємниць. Наприклад, Кримінальний кодекс штату Техасу, відповідно до параграфу 31.05 якого комерційною таємницею є (або як одне ціле, або в будь-якій частині) «наукова та технічна інформація, зразок, процес, процедура, формула чи вдосконалення, яке має свою цінність та з приводу якого власник вжив заходів, щоб запобігти доступності для усіх осіб, крім тих, кого він обрав, щоб надати доступ в обмежених цілях» [7, 15].

Як бачимо, у нормативно-правових актах, що покликані охороняти права на комерційні таємниці у США (різної галузевої приналежності та різного адміністративного рівня) одним з критеріїв комерційної таємниці, є необхідність вжиття її власником певних мір, які в формулюваннях Акту 1996 р. називаються «розумними заходами». З одного боку, такі міри застосовуються для того, щоб цінна для компанії інформація не просочувалася назовні, а отже слугують забезпеченню інформаційної безпеки компанії, з іншого боку, факт застосування являє собою необхідну передумову набуття статусу комерційної таємниці. На жаль, перелік таких заходів у законодавстві США не було наведено, проте, завдяки вивченню судової практики можуть бути встановленими основні правила. Для аналізу вивчаються три судові справи, що стосуються порушень Акту 1996 р.: «США проти Чанга», «США проти Лью», «США проти Джин». Вибір справ пояснюється низкою підстав: кожна з них порушувалася за обвинуваченнями фе-

[1] Єдиний закон про комерційну таємницю являє собою модельний нормативно-правовий акт у сфері цивільно-правової охорони комерційної таємниці, розроблений для подальшого прийняття в окремих штатах (на сьогодні діє майже у всіх).

деральних правоохоронних органів, а судові рішення виносилися федеральними судами, що дозволяє розглядати отримані результати дослідження як такі, що відображають універсальні, а не регіональні підходи до трактування розумних заходів у США; розгляд усіх справ пов'язаний з захистом національних інтересів та зумовлений протидією економічному шпигунству, а отже здійснюючи доказування того, що відповідна інформація містить комерційну таємницю, сторона обвинувачення представляла позицію держави з цього питання; усі справи об'єднує те, що крадіжка комерційної таємниці відбувалася в інтересах китайських компаній особами, які за своїм походженням були китайцями, а це, в свою чергу, свідчить про тенденційність.

1. Справа *«США проти Чанга»* розглядалася Федеральним окружним судом Центрального округу Каліфорнії в першій інстанції та Апеляційним судом Дев'ятого округу в 2009-2010 рр. на підставі обвинувачення Д. Чанга в тому, що він передавав китайському уряду відомості, які становили комерційну таємницю та мали відношення до секретів виробництва компанії «Боїнг», на яку він працював тривалий час (близько 30 років). Було з'ясовано, що контакт з представниками китайських спецслужб він встановив у 1980-их та підтримував його постійно. Обшуки будинку Д. Чанга відбулися у 2006 р. після виявлення федеральними органами зачіпок при розслідуванні зовсім іншої справи. В результаті знайшли велику кількість інкримінуючих документів, зокрема детального опису плану подорожей підозрюваного до Китаю та його зустрічей зі спецагентами, а також десятки тисяч сторінок, де були представлені різного роду відомості про космічні кораблі, гелікоптери, винищувачі та обладнання, яке використовується у них. В процесі розгляду справи постало питання, чи документи, відомості з яких підсудний незаконно повідомляв представникам китайської влади, справді містили комерційні таємниці з огляду на достатність «розумних заходів», які були вжитими. Д. Чанг наполягав на тому, що компанією «Боїнг» не було вжито достатніх заходів для того, щоб зберегти секретність своїх комерційних таємниць. Як один з аргументів він назвав те, що окремі відомості були представлені інженерами «Боїнгу» під час презентації на конференції, яка проводилася з ініціативи Національного управління з аеронавтики і дослідження космічного простору, проте, суд повністю заперечив таке твердження. Служба безпеки контролювала доступ на територію приміщень, де зберігалися відповідні документи, за допомогою системи перепусток, а також здійснювався обшук речей та транспортних засобів осіб, які знаходились всередині, в тому числі працівників компанії. Крім того, укладалися спеціальні угоди про конфіденційність, згідно з якими особа, яка була ознайомлена з секретною інформацією про виробничий процес, зобов'язувалася не розголошувати її. Також згадувалося про проведення роз'яснень для працівників компанії щодо неприпустимості надання будь-кому відомостей такого характеру. Дуже важливим кроком з боку компанії «Боїнг» стало позначення як своєї власності деяких з документів, статус комерційної таємниці яких підсудний намагався оскаржити. Суд не знайшов підстав для того, щоб не вважати інформацію, яку Д. Чанг надавав іноземним агентам, комерційної таємницею. Його було визнано винним та засуджено до понад 15 років позбавлення волі [8].

2. Справа *«США проти Лью»* була порушеною перед Окружним судом Північного округу Каліфорнії та Апеляційним судом Дев'ятого округу в 2013-2017 рр. з огляду на обвинувачення В. Лью та його компанії «USA Performance Technology, Inc.» відповідно до Акту 1996 р. у крадіжці комерційної таємниці компанії «Дюпон», насамперед інформації, що стосувалася процесу виробництва фарбуючого пігменту (діоксиду титану – TiO2). Цей пігмент використовується для створення «найбілішого» з-поміж усіх відтінків білого кольору в різних сферах виробництва – від автомобілів до паперу. Як з'ясувалося в ході розгляду справи, Р. Мегерл, інженер, який працював у компанії «Дюпон» протягом 35 років, разом з ще одним колишнім працівником Т. Спітлером надавали консультації стосовно того, як отримати потрібну речовину, тим самим розкривши секрет пігменту в інтересах В. Лью. Той, в свою чергу, заявив в 2004 р., що його компанія винайшла прогресивну технологію виробництва TiO2 та готова підпи-

сати контракт про її передачу китайській компанії «Pangang Group», яка в минулому так і не змогла домовитися з «Дюпоном» про відповідний дозвіл. Відзначимо, що в процесі апеляційного оскарження вироку, згідно з яким В. Лью було засуджено до 180 місяців ув'язнення (покарання також передбачалося для його дружини, Р. Мегерла та компанії «USA Performance Technology, Inc.»), в Апеляційному суді Дев'ятого округу піднімалося питання, чи в даному випадку доведеною є наявність комерційної таємниці. Предметом дослідження суду стало не тільки «правило Монсанто», яке заслуговує окремої уваги, але й достатність «розумних заходів», які були вжиті. Так, в апеляційній скарзі було поставлено під сумнів те, чи правильно розглядати як комерційну таємницю інформацію, яка використовувалася в процесі виробництва на заводі в Ештабулі після того, як його було продано (хоча й суд заперечив доцільність застосування за таких обставин «правила Монсанто» в інтересах В. Лью, враховуючи те, що на цьому заводі використовувався не той самий секретний спосіб). Апеляційна інстанція у своєму рішенні таки підтвердила статус комерційної таємниці, керуючись не в останню чергу принципом «безпечних очей підрядчиків», впроваджених компанією «Дюпон» як методу корпоративної політики в цілях забезпечення інформаційної безпеки. По-перше, вона обирала підрядчиків, яким надавався доступ до секретів виробництва, з-поміж тих, з ким тривалий час співпрацювала, за умови того, що вони проявили себе як надійні. По-друге, було встановлено вимогу укладати договори про конфіденційність. По-третє, інформація надавалася лише на основі гострої виробничої необхідності. По-четверте, було унеможливлено винесення носіїв інформації як джерел комерційної таємниці за межі приміщень компанії [9]. Компанія «Дюпон» надійно охороняла технологію виготовлення діоксиду титану в фізичному розумінні, адже заводські приміщення були оточені високими парканами, їх патрулювали охоронці, а відвідувачів, яким забороняли здійснювати фотозйомку, супроводжували спеціальні працівники під час перебування на території. Крім того, компанія підписувала з особами, котрі мали будь-яке відношення до її діяльності, а отже могли отримувати доступ до цінної для неї конфіденційної інформації, договори про нерозголошення. Відзначимо, що виробничий процес було організовано таким чином, що кожний відділ мав доступ лише до певної ділянки всього виробничого процесу. Зважаючи на всі «розумні заходи», вжиті керівництвом Дюпон із захисту комерційних таємниць, суд визнав, що викрадена інформація становила комерційну таємницю [10].

3. Справа *«США проти Джин»* розглядалася у 2011-2013 рр. Федеральним окружним судом Північного округу Іллінойсу в першій інстанції та Апеляційним судом Сьомого округу на підставі виявлення крадіжки комерційної таємниці та вчинення економічного шпигунства з боку обвинуваченої. Було встановлено, що вона, пропрацювавши тривалий час у компанії «Моторола» в якості інженера програмного забезпечення, розпочала співробітництво з китайською компанією «Sun Kaisens», предмет якого був пов'язаним з інформацією, що стала їй відомою під час діяльності на користь «Мотороли» (технологія зв'язку iDEN [Integrated Digital Enhanced Network]). Її було затримано у лютому 2007 р. в аеропорту Чикаго, звідки вона планувала відправитися безповоротно до Китаю, при цьому, мала при собі велику суму готівкою та електронні носії, на яких було збережено тисячі документів з конфіденційними даними, завантаженими напередодні з інформаційних ресурсів компанії. У свій захист Х. Джин заявила, що документи було одержано для того, аби оновити свої знання, а не для того, щоб передавати комусь всупереч інтересам «Мотороли», а також заперечувала комерційну цінність відповідної технології для самої компанії, зважаючи на її застарілість [11]. Разом з тим, в рішенні суду першої інстанції наводиться детальний перелік безпекових заходів, запроваджених компанією з метою захисту конфіденційної інформації. Такі заходи було поділено на декілька категорій: фізична безпека; комп'ютерна та мережева безпека; Кодекс поведінки та політика комп'ютерних ресурсів.

Заходи фізичної безпеки реалізовувалися такими інструментами, як встановлення камер безпеки та сигналізації, а також запровадження системи обмеженого доступу, до якої залучено 40 працівників служби безпеки підприємства. При цьому ворота у приміщення компанії відчиняються та зачиняються або представником служби безпеки, або завдяки картці доступу (доступ надається лише до тих приміщень, де працівник здійснює свої службові обов'язки). Входи до приміщень обладнані камерами безпеки, в деяких випадках – контролюються співробітниками служби безпеки. Хоча, як правило, охоронці не перевіряють речі працівників, їм дозволено це робити в крайніх випадках, коли виникають підозри. При працевлаштуванні новим працівникам проводять тренінг щодо необхідності захисту конфіденційної інформації компанії, а також попереджають про їх відповідальність за можливі порушення. Час від часу (кілька разів на тиждень) службою безпеки проводяться вибіркові перевірки з приводу того, наскільки відповідально працівники виконують вказівки щодо охорони комерційної таємниці. В інформаційній системі «Motorоли», призначеної для обміну файлами, яка називається «Compass», в залежності від рівня вразливості даних, документи класифікуються на такі категорії: «Загальна інформація про бізнес», «Для внутрішнього використання», «Конфіденційна і службова інформація» і «Зареєстрована секретна службова інформація». Основні принципи політики компанії стосовно забезпечення своєї інформаційної безпеки представлені в програмі «Охорона нашої службової інформації».

Заходи комп'ютерної та мережевої безпеки реалізовувалися, по-перше, зусиллями фахівців Центру безпеки операцій, які цілодобово спостерігали за інформаційними системами компанії, своєчасно реагуючи на будь-які прояви неналежної поведінки; по-друге, інтранет «Motorоли», об'єднуючи файлові сервери, сервери електронної пошти та інші елементи інфраструктури, підлягав доступу на підставі унікальних логінів та паролів, що присвоювалися його користувачам; по-третє, інформаційна база «Compass», якою користувалися працівники компанії по цілому світу, перебувала під певним захистом та моніторингом. Крім того, інформаційна політика компанії передбачає встановлення стандартів щодо покладення юридичних зобов'язань на працівників стосовно охорони комерційної таємниці. З моменту виконання своїх повноважень працівник зобов'язаний підписати ряд документів, серед яких не тільки трудовий договір, але й Кодекс поведінки та правила належного використання комп'ютерних ресурсів. Відповідно до трудового договору передбачається заборона використовувати або опубліковувати, або іншим чином оприлюднювати як під час, так і після трудової діяльності будь-яку конфіденційну інформацію про компанію, крім випадків, коли цього вимагають посадові обов'язки. Крім того, було згадано про необхідність передати уповноваженому представнику «Motorоли» усі документи, які мають відношення до її діяльності. Обов'язок щодо нерозголошення конфіденційної інформації про компанію було також виокремлено в Кодексі поведінки [12]. Відзначимо, що в апеляційній інстанції суд не тільки не скасував покарання для Х. Джин у вигляді 4 років позбавлення волі, але й висловив своє здивування з приводу того, що вона не отримала більш жорстке покарання, враховуючи ряд наведених у рішенні обставин [11].

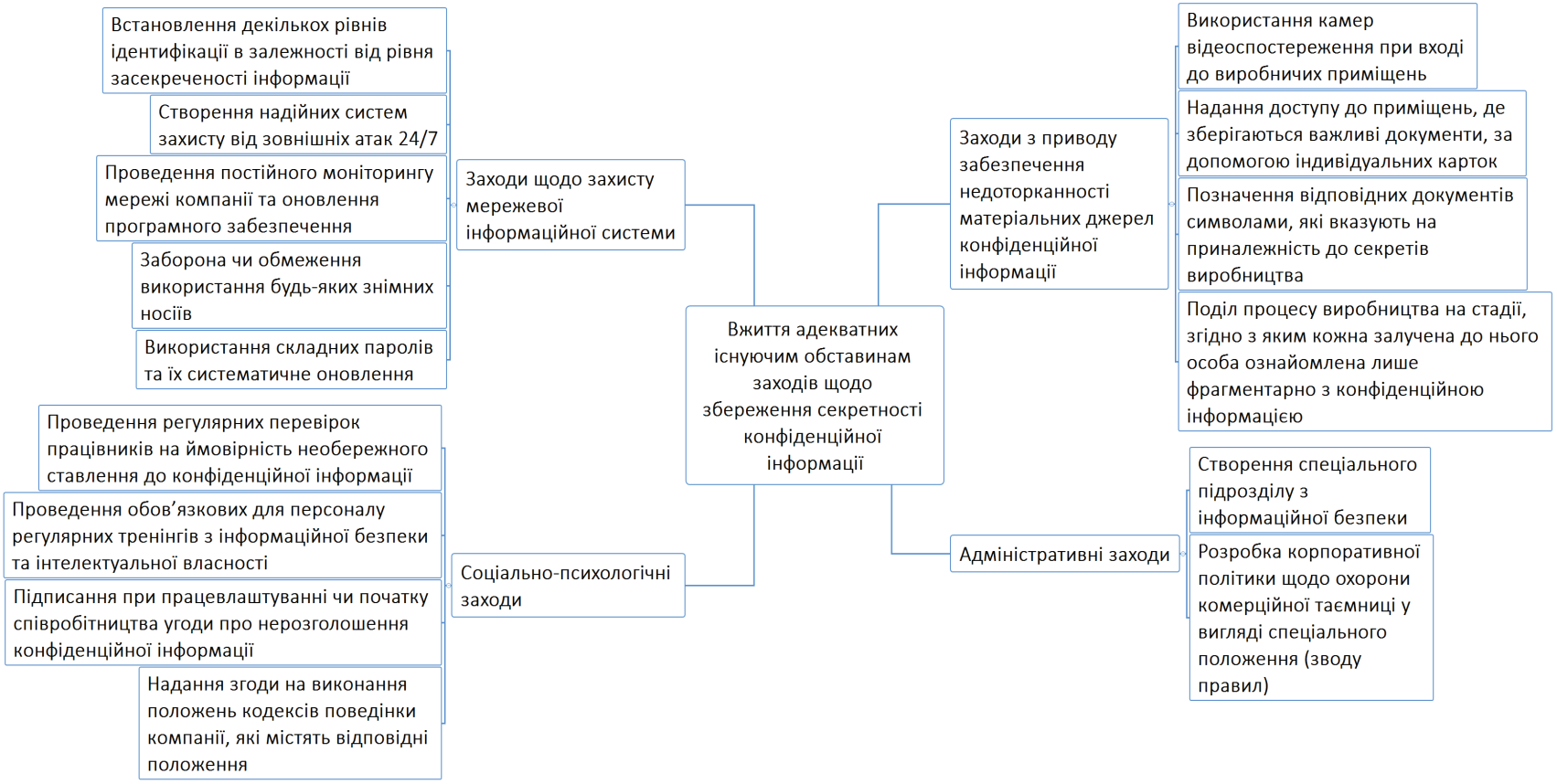
Дослідивши обставини судових справ щодо економічного шпигунства, які порушувалися перед судами США впродовж останніх десяти років, можемо узагальнити та систематизувати заходи, що підлягають реалізації по відношенню до інформації, щоб та отримала правову охорону як комерційна таємниця, відповідаючи ознаці «розумних заходів» у термінології Акту 1996 р. По-перше, слід виділити категорію адміністративних заходів, призначення яких полягає в тому, щоб запровадити на рівні цілої компанії такі організаційно-управлінські інновації, котрі здатні мінімізувати ризики небажаних інформаційних витоків. На нашу думку, серед них заслуговує на особливу увагу створення спеціального підрозділу з інформаційної безпеки, а також розробка корпоративної політики щодо охорони комерційної таємниці у вигляді спеціального положення (зводу правил). По-друге, необхідно запроваджувати заходи з приводу забезпечення

недоторканності матеріальних джерел конфіденційної інформації: надання доступу до приміщень, де зберігаються важливі документи, за допомогою індивідуальних карток; використання камер відеоспостереження при вході до виробничих приміщень; поділ процесу виробництва на стадії, згідно з яким кожна залучена до нього особа ознайомлена лише фрагментарно з конфіденційною інформацією; позначення відповідних документів символами, які вказують на приналежність до секретів виробництва. По-третє, охороні комерційної таємниці сприяють заходи щодо захисту мережевої інформаційної системи, такі як: використання складних паролів та їх систематичне оновлення; створення надійних систем захисту від зовнішніх атак 24/7; встановлення декількох рівнів ідентифікації в залежності від рівня засекреченості інформації; заборона чи обмеження використання будь-яких знімних носіїв; проведення постійного моніторингу мережі компанії та оновлення програмного забезпечення. По-четверте, соціально-психологічні заходи, кожен з яких спрямований на те, щоб сформувати у свідомості працівника компанії чи будь-якої іншої особи, яка має доступ до її конфіденційної інформації, переконання, відповідно до якого вона не підлягає розголошенню (підписання при працевлаштуванні чи початку співробітництва угоди про нерозголошення конфіденційної інформації, а також надання згоди на виконання положень кодексів поведінки компанії, які містять відповідні положення; проведення обов'язкових для персоналу регулярних тренінгів з інформаційної безпеки та інтелектуальної власності, в рамках яких пояснюється необхідність збереження секретності комерційної таємниці для успішності компанії, а також обов'язок нести правову відповідальність за розголошення конфіденційної інформації як законодавча вимога; проведення регулярних перевірок працівників на ймовірність необережного ставлення до конфіденційної інформації).

Для того, щоб показати перелік «адекватних існуючим обставинам заходів щодо збереження її секретності», які необхідно вжити по відношенню до конфіденційної інформації українським підприємством з метою надання їй статусу комерційної таємниці, а також взаємозв'язки між ними, зважаючи на аналіз практики США, було підготовлено когнітивну карту (див. додаток 1).

Висновки. Таким чином, хоча й нормативно-правова база США з питань охорони комерційної таємниці охоплює федеральне право та право штатів, а також поєднує норми різної галузевої приналежності, була розроблена єдина концепція комерційної таємниці, яка ґрунтується на виділенні двох ключових ознак: відсутність загальнодоступності відповідної інформації, внаслідок чого компанія отримує переваги над конкурентами на ринку, а також вжиття нею ряду заходів з метою охорони засекреченості такої інформації. В судовій практиці США в період 2009-2018 рр. федеральними судами було розглянуто низку справ на основі обвинувачень в економічному шпигунстві шляхом викрадення та незаконного заволодіння комерційними таємницями, кримінальна відповідальність за яке була передбачена Актом 1996 р. Під час вивчення їхніх обставин було представлено аргументацію з приводу того, чому відомості, які оприлюднювалися протиправно різними способами, являють собою комерційну таємницю. Важливе значення мало пояснення того, що компанія, працівником якої був підсудний, вжила розумні заходи для збереження секретності таких відомостей, насамперед у справі ««США проти Х. Джин» (фізична безпека; комп'ютерна та мережева безпека; Кодекс поведінки та політика комп'ютерних ресурсів). З урахуванням досвіду США було розроблено рекомендації з приводу вжиття українським підприємством адекватних заходів у світлі вимог ст. 505 Цивільного кодексу України, перелік яких складається з наступних видів: адміністративних, щодо забезпечення недоторканності матеріальних джерел конфіденційної інформації, щодо захисту мережевої інформаційної системи, соціально-психологічних. Досвід США свідчить про те, що універсальної формули «розумних заходів» не існує, а оцінку того, чи були вони достатніми для надання певній інформації статусу комерційної таємниці, здійснює суд, виходячи з конкретних обставин.

Додаток 1


Вжиття адекватних існуючим обставинам заходів щодо збереження секретності конфіденційної інформації
Заходи щодо захисту мережевої інформаційної системи
Встановлення декількох рівнів ідентифікації в залежності від рівня засекреченості інформації
Створення надійних систем захисту від зовнішніх атак 24/7
Проведення постійного моніторингу мережі компанії та оновлення програмного забезпечення
Заборона чи обмеження використання будь-яких знімних носіїв
Використання складних паролів та їх систематичне оновлення
Соціально-психологічні заходи
Проведення регулярних перевірок працівників на ймовірність необережного ставлення до конфіденційної інформації
Проведення обов'язкових для персоналу регулярних тренінгів з інформаційної безпеки та інтелектуальної власності
Підписання при працевлаштуванні чи початку співробітництва угоди про нерозголошення конфіденційної інформації
Надання згоди на виконання положень кодексів поведінки компанії, які містять відповідні положення
Заходи з приводу забезпечення недоторканності матеріальних джерел конфіденційної інформації
Використання камер відеоспостереження при вході до виробничих приміщень
Надання доступу до приміщень, де зберігаються важливі документи, за допомогою індивідуальних карток
Позначення відповідних документів символами, які вказують на приналежність до секретів виробництва
Поділ процесу виробництва на стадії, згідно з яким кожна залучена до нього особа ознайомлена лише фрагментарно з конфіденційною інформацією
Адміністративні заходи
Створення спеціального підрозділу з інформаційної безпеки
Розробка корпоративної політики щодо охорони комерційної таємниці у вигляді спеціального положення (зводу правил)

Список літератури

1. Grimes S., Murphy S. 'Reasonable Measures' For Protecting Trade Secrets: A Primer [Електронний ресурс] // Winston & Strawn LLP. – Режим доступу: https://www.winston.com/en/thought-leadership/reasonable-measures-for-protecting-trade-secrets-a-primer.html.
2. Андрощук Г. О. Захист комерційної таємниці в США: протидія економічному шпигунству / Г. О. Андрощук // Наука та інновації. – 2013. – Т. 9, № 1. – С. 80-95.
3. Інформаційний лист Вищого господарського суду України №01-8/184 «Про деякі питання практики застосування господарськими судами законодавства про інформацію» від 28.03.2007 [Електронний ресурс] // Офіційний портал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v_184600-07.
4. Code of Federal Regulations. Part 1910. Revised as of July 1, 1998. – Washington: US Government Printing Office, 1998. – 584 p.
5. Uniform Trade Secrets Act with 1985 Amendments [Електронний ресурс] // World Intellectual Property Organization. – Режим доступу: https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf.
6. Economic Espionage Act of 1996 [Електронний ресурс] // U.S. Government Publishing Office. – Режим доступу: https://www.govinfo.gov/content/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf.
7. Penal Code. Title 7. Offences against property. Chapter 31. Theft [Електронний ресурс] // Texas Constitution and Statutes. – Режим доступу: https://statutes.capitol.texas.gov/Docs/PE/pdf/PE.31.pdf.
8. Opinion by Judge Graber. United States Court of Appeals for the Ninth Circuit. United States of America (Plaintiff-Appellee) vs. Dongfan «Greg» Chung (Defendant-Appellant) [Електронний ресурс] // The Trade Secrets Institute at Brooklyn Law School. – Режим доступу: http://tsi.brooklaw.edu/sites/tsi.brooklaw.edu/files/filings/united-states-v-chung/20110926ninth-circuit-appellate-decision.pdf.
9. United States v. Liew [Електронний ресурс] // Internet portal of the United States Courts for the Ninth Circuit. – Режим доступу: http://cdn.ca9.uscourts.gov/datastore/opinions/2017/05/05/14-10367.pdf.
10. D.Q. Wilber. How a corporate spy swiped plans for DuPont's billion-dollar color formula [Електронний ресурс] // Official Bloomberg Website. – Режим доступу: https://www.bloomberg.com/features/2016-stealing-dupont-white.
11. United States of America, Plaintiff Appellee, v. Huanjuan Jin, Defendant Appellant [Електронний ресурс] // The Trade Secrets Institute at Brooklyn Law School. – Режим доступу: http://tsi.brooklaw.edu/sites/tsi.brooklaw.edu/files/filings/united-states-v-hanjuan-jin/20130926final-order.pdf.
12. United States v. Hanjuan Jin, 833 F. Supp. 2d 977, 1000 (N.D. Ill. 2012) [Електронний ресурс] // Casetext Inc. – Режим доступу: https://casetext.com/case/united-states-v-hanjuan-jin.

Стаття надійшла 25.05.2019 р.

А. О. Гачкевич, канд. юрид. наук, старший преподаватель
Национальный университет «Львовская политехника»
Кафедра международной информации
ул. Степана Бандеры, 12, Львов, 79013, Украина

Т. Р. Казарян, магистрант-исследователь по международным отношениям, общественных коммуникаций и региональных студий
Национальный университет «Львовская политехника»
ул. Степана Бандеры, 12, Львов, 79013, Украина

ПРИНЯТИЕ АДЕКВАТНЫХ МЕР КАК ПРИЗНАК КОММЕРЧЕСКОЙ ТАЙНЫ: АНАЛИЗ ОПЫТА США

Резюме

Статья посвящается изучению вопроса мер, которые необходимо предпринять в отношении конфиденциальной информации предприятием для того, чтобы она была признана коммерческой тайной. В основе исследования лежит анализ особенностей правовой системы США, государства с богатыми традициями в сфере охраны прав на коммерческие тайны. Поставленный вопрос рассматривается в контексте изучения судебных дел: «США против Чанга», «США против Лью», «США против Джин». На основании анализа судебных решений и учитывая практические подходы, конкретизируются теоретические положения относительно перечня «разумных мер» как признака коммерческой тайны.

Ключевые слова: коммерческая тайна, разумные меры, судебная практика, экономический шпионаж, информационная безопасность.

A. O. Hachkevych, PhD in Law, Senior Lecturer
Lviv Polytechnic National University
the Department of International Information
Stepana Bandery Street, 12, Lviv, 79013, Ukraine

T. R. Kazarian, Master's degree student in international relations,
public communications and regional studies
Lviv Polytechnic National University
Stepana Bandery Street, 12, Lviv, 79013, Ukraine

UNDERTAKING OF ADEQUATE MEASURES AS A FEATURE OF A TRADE SECRET: ANALYSIS OF U.S. EXPERIENCE

Summary

This article examines the question of undertaking adequate measures by an enterprise with respect to confidential information aiming at recognizing it as a trade secret. The present study is based on the analysis of U.S. legal system peculiarities, which has deep traditions in the sphere of trade secrets protection. Consideration of the question posed is carried out by studying the judgements of three cases: «US vs. Chung», «US vs. Liew» and «US vs Jin». Theoretical provisions of «adequate measures» list related to the features of a trade secret are specified based on judicial decisions investigation and regarding practical approaches.

Key words: trade secret, reasonable measures, jurisprudence, economic espionage, information security.