Наука та інновації. 2013. Т. 9. № 1. С. 80—95

Г.О. Андрощук

НДІ інтелектуальної власності НАПрН України, Київ

ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В США: ПРОТИДІЯ ЕКОНОМІЧНОМУ ШПИГУНСТВУ

Розглянуто економіко-правові аспекти захисту комерційної таємниці. Дається визначення понять економічна розвідка, промислове шпигунство, аналіз Закону про економічне шпигунство (Economic Espionage Act), економіко-статистичні показники стану, виявлення, розслідування справ і покарання за економічне шпигунство. Наводяться рекомендації ФБР щодо захисту бізнесу від економічного шпигунства. Робиться висновок, що захист комерційної таємниці здійснюється також з метою забезпечення конкурентоспроможності національної економіки.

Ключові слова: економічне шпигунство, комерційна таємниця, правова охорона, промислове шпигунство, розвідка.

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 [1].

Термін «*промислове шпигунство*» вперше був сформульований на початку 60-х років минулого століття на семінарі з методики збору інформації для керівного складу фірми Manadgement Investigation Services. Успішно здійснені акції промислового шпигунства дають суттєві переваги над конкурентами, яким іноді доводиться витрачати мільйони на подолання наслідків таких акцій.

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. Її сфера – всі галузі ринкової економіки. За визначенням Інтерполу, економічна розвідка – це «*одержання облудним шляхом інтелектуальної власності, яка належить якій-небудь юридичній особі, що була створена чи законно придбана цією юридичною особою з метою виробити щось, що має або може мати промислову цінність і (в більш широкому плані) цінність для національної економіки*».

Найчастіше економічне і промислове шпигунство вживаються як синоніми. Проте промислове шпигунство – це частина економічного. Вони відрізняються в такій же мірі, як промисловість і економіка.

Вікіпедія визначає промислове шпигунство як «*форму недобросовісної конкуренції, при якій здійснюється незаконне отримання, використання, розголошення інформації, що становить комерційну, службову чи іншу охоронювану законом таємницю з метою отримання переваг при здійсненні підприємницької діяльності, а*

так само отримання матеріальної вигоди»; військовий словник США (US Military Dictionary) – як *«дії, спрямовані на отримання інформації про виробничі потужності промисловості, техніки, або можливості через таємні операції»*; енциклопедія Британіка (Britannica Concise Encyclopedia) – як *«придбання торгових секретів від бізнесу конкурентів. Промислове шпигунство є реакцією на зусилля багатьох підприємств тримати в таємниці свої проекти, формули, процеси виробництва, дослідження та плани на майбутнє. Промислові секрети можуть стати відомими у відкритому ринку через нелояльних працівників або за допомогою інших засобів. Заходи покарання осіб, визнаних винними, – в діапазоні від заборони на подальше використання знань до відшкодування збитку»*.

Якщо звернутися 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. Білл Клінтон дав вказівку керівництву розвідувального співтовариства США про поглиблення досліджень у сфері економічної розвідки [1]. Було виділено три пріоритетних напрямки:

- макроекономічна розвідка — збір стратегічної інформації про глобальні процеси в економіках інших держав;
- мікроекономічна розвідка — збір тактичної й оперативної інформації з тієї ж проблематики;
- економічна контррозвідка — протидія спробам іноземних державних спецслужб і комерційних фірм здобути американські торгово-економічні й технологічні секрети.

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 [2]. США виходять з того, що проти американської економіки регулярне шпигунство ведуть розвідки 23-х країн, у т.ч. провідні європейські держави [3].

ПРАВОВА ОХОРОНА КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Правова охорона комерційної таємниці в Сполучених Штатах Америки ґрунтується, головним чином, на законодавстві кожного штату окремо. Єдиним видом правової охорони комерційної таємниці, що існує в даний час на федеральному рівні, є встановлення кримінальної відповідальності за крадіжку та незаконне присвоєння відомостей, які становлять комерційну таємницю, а також за «економічне шпигунство». Закон, котрий часто називається як «Акт про економічне шпигунство» (*Economic Espionage Act*), міститься в частині 18, § 1831 – 1839 Кодексу законів США [4]. У цілому, законодавство штатів забороняє незаконне присвоєння секретних відомостей, що становлять комерційну таємницю. Визначення комерційної таємниці, наведене в Законі, включає нові технології, за допомогою яких здійснюється створення і зберігання комерційної таємниці. Так, до комерційної таємниці відносяться всі види і форми фінансової, комерційної, наукової, технічної та економічної інформації, включаючи моделі, креслення, програми, формули, ідеї, прототипи, методики, технології, процедури або коди, що зберігаються будь-яким способом, за умови, що власник вжив розумних зусиль для збереження секретності, а інформація має самостійну економічну цінність завдяки відсутності до неї доступу з боку інших осіб.

Для того щоб кваліфікуватися як комерційна таємниця, відповідні відомості повинні мати самостійну економічну цінність, оскіль-

ки вони невідомі іншим. Цінність може бути або фактичною (тому, що комерційна таємниця використовувалася та продовжує використовуватися), або потенційною (тому, що комерційна таємниця була виявлена, але не використовувалася, або тому, що її цінність нелегко виявити). Наявність ознаки самостійності економічної цінності інформації, зазначеної у визначенні комерційної таємниці, може бути встановлена різними способами. Так, оцінка вартості комерційної таємниці може бути заснована на ринковій ціні угод з передачі аналогічної або схожої інформації. У розрахунок можуть бути також прийняті витрати, понесені власником комерційної таємниці під час відповідних розробок і досліджень. Якщо ж інформація, що становить комерційну таємницю, була вкрадена і продана третім особам, в судовому засіданні буде врахована і та ціна, яку за неї заплатили правопорушники. Особливо відзначимо, що суди не завжди відносять до комерційної таємниці інформацію, яка вважається компанією (і дійсно є) цінною для здійснення підприємницької діяльності. Так, клієнтська база компанії може бути визнана такою, що становить комерційну таємницю, тільки в тому випадку, якщо клієнти, що містяться в цій базі, не відомі у відповідній галузі промисловості або торгівлі і можуть бути знайдені тільки із застосуванням значних організаційних і фінансових ресурсів, а на створення бази знадобилося значна кількість часу. У цьому випадку економічна цінність клієнтської бази буде полягати саме у відсутності аналогічної інформації у конкурентів.

З метою правової охорони конфіденційні відомості повинні також бути об'єктом *«розумних зусиль»* з підтримки їх таємності. Розумність цих зусиль визначається відповідно до конкретних обставин тієї чи іншої справи. На практиці під *«розумними зусиллями»* розуміються, наприклад, повідомлення працівників про необхідність дотримання конфіденційності, підписання працівниками угод про нерозголошення комерційної таємниці, зберігання секретних документів *«під замком»* і т. ін. Як правило, при звільненні співробітник письмово повідомляє організацію про взяті на себе зобов'язання щодо збереження комерційної таємниці. Керівник організації, звідки звільнився працівник, може повідомити нового роботодавця про інформованість працівника в області комерційних секретів. Попереджаючи можливі правопорушення з боку найманого персоналу, роботодавець може самостійно запропонувати працівникові сповістити його про наявність зобов'язань щодо нерозголошення комерційної таємниці. Власник комерційної таємниці зобов'язаний визначити цінність охоронюваних матеріалів і оцінити ризик їх можливої втрати. Слід зазначити, що заходи, прийняті з метою забезпечення секретності інформації, повинні бути відповідні її цінності. У ході судового розгляду оцінюються технічні засоби, використані для захисту інформації, а також спільна політика компанії у сфері інформаційного обміну з третіми особами. Дані відомості можуть послужити підставою для відмови в судовому захисті інтересів особи, яка не проявила належної передбачливості у сфері охорони власних секретів. Інформація вважається комерційною таємницею і в тому випадку, якщо власник розкриває її своїм контрагентам в рамках ліцензійного договору, договору комісії або інших угод, які передбачають використання інформації в строго певних цілях. У цьому випадку власник комерційної таємниці повинен забезпечити належні заходи забезпечення секретності і, зокрема, укласти з усіма одержувачами інформації договори про нерозголошення переданих відомостей.

Крім того, у ряді штатів в США вимагається, щоб комерційна таємниця легко не розкривалася шляхом зворотного інжинірингу (*reverse engineering*).

Відповідно до законодавства США будь-яка особа, яка незаконно привласнює або загрожує незаконно привласнити комерційну таємницю, права на яку належать іншій особі, порушує права власника прав на комерційну

таємницю. Незаконне присвоєння (*misappropriation*) визначається зазвичай як придбання, розголошення або використання комерційної таємниці іншою особою за допомогою *«неналежних засобів»*. У цілому, під *«неналежними засобами»* розуміється крадіжка, дача хабара, введення в оману, порушення або підбурювання до порушення зобов'язання зберігати комерційну таємницю, а також шпигунство із використанням електронних або інших засобів. Обов'язок зберігати комерційну таємницю в секреті може встановлюватися контрактом, наприклад, угодою про конфіденційність, або передбаченим законом зобов'язанням зберігати відомості, що становлять комерційну таємницю, в секреті у зв'язку із зайняттям відповідальної посади. Крім прямих правопорушень суди приймають до розгляду позови про співучасть (*vicarious infringement*) і відповідальність за дії інших осіб.

Таким чином, особа, яка підбурює іншу особу порушити чиїсь права, або особа, яка надає допомогу в такому правопорушенні, несуть однакову відповідальність.

Американська судова практика не дає однозначної відповіді на питання, чи втрачає інформація статус комерційної таємниці в разі її анонімного опублікування в мережі Internet. Так, у ряді судових рішень вказувалося, що відмова у юридичному захисті в цьому випадку лише стимулює порушників законодавства публікувати неправомірно отриману інформацію в Internet з метою руйнування інституту комерційної таємниці. Розкриття інформації, що є комерційною таємницею, органами державної влади в ході попереднього слідства чи іншого розслідування не впливає на її правовий статус. Надання інформації необхідне для здійснення державних повноважень, причому законодавство встановлює достатні гарантії належного захисту комерційної таємниці. Крім спеціально передбаченої норми про забезпечення конфіденційності інформації, що розкривається в ході судового засідання, закон встановлює додаткові обмеження на отримання інформації органами державної влади без згоди її власника.

Правова охорона комерційної таємниці здійснюється доти, доки вона відповідає, в цілому, вимогам набуття правової охорони – має цінність і таємність. Правова охорона припиняється у разі, якщо правовласник не здійснює розумних заходів щодо забезпечення секретності відомостей або якщо секретні відомості стають відомими завдяки використанню належних засобів (наприклад, зворотного інжинірингу).

ДОВЕДЕННЯ ПОРУШЕННЯ ПРАВ НА КОМЕРЦІЙНУ ТАЄМНИЦЮ

Критерієм незаконного присвоєння відомостей, що становлять комерційну таємницю, тобто здійснення правопорушення за законодавством США є придбання, використання або розголошення зазначених відомостей іншою особою неналежними засобами. Таке придбання комерційної таємниці може оспорюватися шляхом подання позову до суду у разі, якщо відповідач купує зазначені вище відомості неналежними засобами, або якщо він їх купує в іншої особи і знає або має підстави вважати, що ці відомості були отримані неналежними засобами. Власник прав на комерційну таємницю повинен продемонструвати свої права на зазначені відомості, а також доказати, що такі відомості становлять комерційну таємницю. Правова охорона комерційної таємниці виникає автоматично у разі, якщо відомості, що мають цінність для правовласника, тримаються в секреті з використанням розумних заходів (*reasonable measures*). Розумність заходів, що використовуються для захисту конфіденційності відповідних відомостей, визначається в кожному конкретному випадку. Невикористання розумних заходів щодо захисту відомостей, таких, як угода про конфіденційність, призводить до втрати прав на комерційну таємницю. Серед типів відомостей, що, як правило, мають правову охорону, є формули, зразки, компіляції, програми,

пристрої, інструкції, способи та технології. Відповідно, списки клієнтів, інструкції, виробничі процеси, методи розробки програмного забезпечення (включаючи його коди), а також винаходи, які не були запатентовані, часто отримують правову охорону за законодавством США про комерційну таємницю. Особи, які подають заявки про реєстрацію прав на винаходи, часто використовують положення законодавства про комерційну таємницю з метою правової охорони своїх винаходів під час їх розробки та протягом процесу розгляду заявки до того часу, поки заявка не буде опублікована і відомості, що містяться в такій заявці, не втратять статусу конфіденційності.

Незаконне присвоєння необхідно доводити в кожному конкретному випадку. Незаконне присвоєння нерідко можна довести за допомогою прямих доказів того, що відповідач одержав відомості, які становлять комерційну таємницю, за допомогою хабара, крадіжки або шпигунства. Для доведення незаконного присвоєння не потрібно фізичного отримання документів, що містять комерційну таємницю, хоча це може бути корисним. Несанкціоноване використання чи розголошення можна також довести, встановивши, що відповідач не був уповноважений правовласником використовувати комерційну таємницю, а також що він знав або мав підстави вважати, що його знання про комерційну таємницю походять від особи, яка використала незаконні засоби для її набуття, або що він одержав такі знання від особи, яка повинна була зберігати комерційну таємницю чи то обмежувати її використання у відповідності зі своїми службовими обов'язками. Найчастіше справи, пов'язані з комерційною таємницею, стосуються крадіжки конфіденційних відомостей, що становлять комерційну таємницю, колишніми працівниками, економічного шпигунства за допомогою незаконних методів спостереження, а також несанкціонованої цифрової передачі програмних кодів і майстер-файлів.

У зв'язку з необхідністю захищати конфіденційні відомості від несанкціонованого розголошення суди, як правило, видають охоронні накази, що обмежують розкриття таких відомостей тільки певним спеціально зазначеним особам, які несуть зобов'язання зберігати надані ним відомості в секреті. Суди також часто проводять закриті слухання та вводять обмежений режим доступу до матеріалів справ з метою подальшого забезпечення секретності комерційної таємниці.

СПОСОБИ ЗАХИСТУ ПРАВ ТА ВІДШКОДУВАННЯ ЗБИТКІВ

Оскільки в результаті несанкціонованого використання або розголошення відомості, що становлять комерційну таємницю, можуть втратити свою цінність, найважливішими способами збереження таємниці за законодавством США є судові заборони з метою запобігання потенційного або фактичного незаконного присвоєння комерційної таємниці. Способи захисту прав на комерційну таємницю, що містяться в законодавстві США, включають мінімальні стандарти захисту прав, передбачені Угодою про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС), серед яких – судові заборони, відшкодування збитків, відшкодування витрат на послуги адвоката та судові витрати, вилучення товарів, з якими пов'язані правопорушення, або їх знищення [4].

Судові заборони (Injunctions). Тимчасові, попередні або остаточні заборони можуть бути видані судом на тих умовах, які він вважатиме виправданими, для запобігання або припинення фактичного чи потенційного незаконного присвоєння відомостей, що становлять комерційну таємницю. Видання судових заборон є звичайною практикою у справах про порушення прав на комерційну таємницю. Судові заборони «*ex parte*» (тобто накази про заборону, видані без повідомлення відповідача) можливі на тимчасовій основі та, як правило, виносяться у випадку фактичного або потенційного незаконного присвоєння. Такі судові заборони діють доти, доки не втрачається таємничість відомостей, а в деяких випадках судові заборо-

ни можуть продовжувати діяти протягом певного додаткового періоду часу з метою усунення можливості одержання комерційної вигоди від незаконного присвоєння. Наприклад, у тих випадках, коли використання відомостей, які становлять комерційну таємницю, може сприяти скороченню періоду часу на створення товару, судова заборона триває не менше ніж період часу, що був зекономлений за рахунок незаконного використання зазначених відомостей. На додаток до судової заборони щодо незаконного присвоєння цінної інформації у деяких справах суд може зобов'язати відповідача вжити адекватних заходів щодо захисту від розголошення відомостей, що становлять комерційну таємницю, додатково до припинення несанкціонованого доступу до них або їх використання.

Відшкодування збитків у грошовій формі (Money Damages). Відповідач може відповідати за фактичні збитки власника прав на комерційну таємницю у зв'язку з незаконним присвоєнням відомостей, що її становлять, а також за одержання прибутків або економічної переваги в результаті такого незаконного присвоєння, які не були враховані при розрахунку збитків власника прав на комерційну таємницю. У випадку умисного або злочинного незаконного присвоєння відомостей, що становлять комерційну таємницю, суди присуджують виплату штрафних санкцій у сумі, яка не перевищує подвійної суми фактичних збитків.

Гонорар адвокатів і судові витрати. У виняткових випадках суд може також винести рішення про відшкодування стороні, на користь якої винесено рішення, судових витрат, а також витрат на послуги адвоката. Під «винятковими» випадками зазвичай маються на увазі умисні або злочинні правопорушення. У справах про недобросовісне присвоєння відомостей, що становлять комерційну таємницю, також присуджується, як правило, відшкодування витрат на послуги адвоката.

Вилучення предметів, що порушують права. Суд може розпорядитися про вилучення всіх предметів, які, як стверджується, порушують права на комерційну таємницю. До числа таких предметів відносяться матеріальні носії, які містять відомості, а також майстер-файли, товари тощо, що містять комерційну таємницю або вироблені з її використанням.

Знищення. Суд може також винести рішення про знищення всіх предметів, що порушують права на комерційну таємницю, та/або повернення матеріальних носіїв, які містять відомості, що становлять комерційну таємницю, відповідачу або під його контроль.

Відповідальність за дії інших осіб (vicarious liability) та співучасть (contributory infringement). Особи, які свідомо і навмисно сприяють правопорушенням або заохочують до їх вчинення, несуть відповідальність нарівні з безпосереднім правопорушником і підпадають під такі ж самі покарання. Такі особи відповідають за сприяння у правопорушенні (якщо вони знали про правопорушення або мали підстави знати про набуття відомостей, що становлять комерційну таємницю, неналежними засобами), а також спонукання, заохочення або матеріальну підтримку такої діяльності. Особи несуть відповідальність за дії інших осіб, якщо вони мають право і можливість контролювати сторони, які займаються протиправною діяльністю, а також мають безпосередній фінансовий інтерес у використанні товарів, що створені за допомогою комерційної таємниці або містять таку комерційну таємницю.

Застава і гарантії. За законодавством США суд може вимагати від правовласника внести заставу в розумних розмірах, щоб гарантувати компенсацію відповідачу у випадку, коли арешт буде визнаний неправомірним.

АКТ ПРО ЕКОНОМІЧНЕ ШПИГУНСТВО

Захист прав на комерційну таємницю (кримінальні справи). Навмисна крадіжка відомостей, що становлять комерційну таємницю, може бути визнана в США злочином відповідно як до федерального законодавства,

так і до законодавства штатів. Найважливішим законом США, що стосується крадіжки відомостей, які становлять комерційну таємницю, є *Акт про економічне шпигунство 1996 р.* (*Economic Espionage Act of 1996*). Це — єдиний федеральний закон про комерційну таємницю в Сполучених Штатах, який передбачає виключно кримінальну відповідальність за порушення прав на комерційну таємницю [4, 5]. В Акті передбачається кримінальне покарання за економічне шпигунство і за навмисну крадіжку, відтворення, одержання або володіння відомостями, що становлять комерційну таємницю. Для того щоб незаконне присвоєння відомостей, що становлять комерційну таємницю, можна було оскаржити в суді, воно повинно бути здійснене з метою одержання комерційної або економічної вигоди та повинно використовуватися стосовно товарів, які перебуватимуть у цивільному обороті між штатами.

Для отримання обвинувального вироку суду прокурор зобов'язаний довести поза всяким сумнівом, що:

1) обвинувачуваний украв або одержав, знищив чи передав секретні відомості без дозволу правовласника;

2) обвинувачуваний знав або мав підстави знати, що ці відомості становлять комерційну таємницю;

3) відомості насправді становлять комерційну таємницю, що має правову охорону.

Для того щоб комерційна таємниця кваліфікувалася як така, що має правову охорону, відомості повинні стосуватися або бути включеними до товару, який виробляється чи перебуває в цивільному обороті між штатами або в міжнародній торгівлі. Термін «*комерційна таємниця*» відповідно до Акту про економічне шпигунство охоплює всі форми і види фінансових, ділових, наукових, технічних, економічних та інженерних відомостей, включаючи, наприклад, схеми, плани, компіляції, програмні пристрої, формули, конструкції, прототипи, методи, способи, процеси, процедури, програми та коди як у матеріальній, так і в нематеріальній формі, незалежно від того, яким чином зберігаються, компілюються і запам'ятовуються відомості — у фізичній, електронній, графічній формі, на фотознімках або в письмовій формі.

Для того щоб відомості становили охороноздатну комерційну таємницю, власник прав на неї повинен вжити розумних заходів з метою забезпечення таємності таких відомостей. Крім того, відомості повинні «*мати самостійну економічну цінність, фактичну або потенційну, у зв'язку з тим, що вони не є відомими іншим особам і не можуть бути легко визначеними за допомогою належних засобів такими іншими особами*». Інакше кажучи, комерційна таємниця має містити певний елемент, який невідомий у відповідній галузі промисловості або торгівлі, але водночас не потрібно, щоб він був настільки унікальним, аби претендувати на новизну у розумінні прав на винаходи. Відомості не обов'язково повинні бути секретними за всіма параметрами для того, щоб являти собою комерційну таємницю. Комерційною таємницею може бути й сполучення елементів, які публічно відомі, у разі, коли таке сполучення є саме по собі унікальним.

Немає потреби точно доводити фактичну або потенційну цінність відомостей, що становлять комерційну таємницю. Суди, як правило, користуються різними методами доведення цінності комерційної таємниці, включаючи суму за продаж аналогічної комерційної таємниці на відкритому ринку, якщо такі випадки мали місце. Або коли обґрунтовані розрахунки суми, яку покупець, котрий бажає купити, заплатив би продавцю за технологію при укладенні угоди на звичайних комерційних умовах. Оцінка суми витрат на науково-дослідні та дослідно-конструкторські розробки, що поніс власник прав на комерційну таємницю і, як останній засіб, ціна на чорному ринку, котру правопорушник фактично отримав або сплатив в обмін на технологію.

В Акті про економічне шпигунство загалом визначені види заборонених дій, які включа-

ють звичайні випадки крадіжки, коли певний об'єкт фізично відбирається у правовласника. Актом також передбачаються менш традиційні випадки незаконного присвоєння або знищення, об'єктів без дозволу правовласника (наприклад, копіювання, дублювання, схематичне зображення, змальовування, фотографування, завантаження, скачування, зміна, знищення, фотокопіювання, репродукування, передача, відправлення, вручення, відправлення поштою, повідомлення або розголошення відомостей, що становлять комерційну таємницю). Не обов'язково, щоб оригінал відомостей, які становлять комерційну таємницю, виходив за рамки нагляду або контролю з боку правовласника. Навіть якщо власник прав на комерційну таємницю все ще здатен її використовувати, одного факту незаконного присвоєння достатньо для того, щоб знизити або зруйнувати фактичну або потенційну цінність комерційної таємниці. Одержання, купівля або володіння відомостями, що становлять комерційну таємницю, в тих випадках, коли відомо, що вони були викрадені, отримані або перетворені без дозволу правовласника, також забороняється.

Хоча за законодавством вимагається, щоб правопорушник мав певне знання про секретний характер відомостей, що становлять комерційну таємницю, однак він не зобов'язаний мати знання про існування законодавства або навіть знати про те, що відомості можуть становити комерційну таємницю. Замість цього достатньо того, що обвинувачуваний знав про те, що відомості, які становлять комерційну таємницю, мають правову охорону, здійснюються захисні заходи навколо цих відомостей, або знав про використання угоди про конфіденційність та інші засоби захисту таємності цих відомостей, а також, що обвинувачуваний знав, що відомості являють цінність для власника прав на комерційну таємницю і не є широко відомими. Оскільки більшість обвинувачуваних знають про потенційну цінність незаконно привласнених відомостей, що становлять комерційну таємницю, а також про те, що вони підлягають захисту від розголошення (звідки й виникає необхідність незаконного відтворення або передачі), обов'язок тягаря доведення неважко виконати.

Прокурор повинен також довести, що обвинувачуваний мав намір *«заподіяти шкоду»* власнику прав на комерційну таємницю. Це не вимагає доведення умислу або злого наміру. Досить того, що обвинувачуваний знав або усвідомлював те, що його поведінка зачепить інтереси законного правовласника.

Акт про економічне шпигунство поширюється не тільки на крадіжки відомостей, які становлять комерційну таємницю (акти незаконного присвоєння), які вчинені на території США, але й на випадки, що мають місце за межами США, якщо обвинувачуваний є громадянином США або це — американська корпорація, а також якщо будь-який акт у зв'язку із реалізацією крадіжки (незаконного присвоєння) вчинявся в США.

У багатьох штатах також діють закони, які забороняють незаконне придбання, розголошення або використання відомостей, що становлять комерційну таємницю. Хоча закони відрізняються один від одного, законодавством більшості штатів передбачено доведення свідомої або навмисної крадіжки або незаконного присвоєння зазначених відомостей. Визначення поняття комерційної таємниці, як правило, відповідає тому поняттю, яке використовується в цивільному судочинстві, із застосуванням тих самих вимог до доведення цінності відомостей та вживання правовласником розумних заходів щодо захисту їх конфіденційності. Так, наприклад, за законодавством штату Каліфорнія, набуття, розголошення або використання відомостей, що становлять комерційну таємницю, без дозволу правовласника вважається злочином. Обвинувачувані можуть бути оштрафовані на 5 000 дол. США або засуджені до позбавлення волі строком до 1 року, або можуть бути піддані обом видам покарання одночасно.

Умисел. Принципова різниця між цивільною та кримінальною відповідальністю полягає в тому, що в рамках провадження у цивільній справі про захист прав на комерційну таємницю не потрібно демонструвати «умисел». Обвинувачуваний не зобов'язаний знати, що його дії незаконні. Досить того, що він вчинив відповідні дії. За кримінальним законодавством, навпаки, підлягають покаранню тільки навмисні правопорушення.

Відповідно до Акту про економічне шпигунство прокурор повинен довести, що обвинувачуваний «свідомо» украв (незаконно привласнив) відомості, які становлять комерційну таємницю. Наявність умислу допускає, що обвинувачуваний знав або був суттєво упевнений, що він набуває, розголошує або використовує відомості, які становлять комерційну таємницю. Він може й не знати, що дані відомості є комерційною таємницею. Він всього лише повинен усвідомлювати, що зазначені відомості мають цінність завдяки своїй секретній природі, а також що він не має права використовувати, набувати або розголошувати такі відомості. Особа, яка одержала доступ до комерційної таємниці через незнання, помилку або випадково, не може бути притягнена до відповідальності відповідно до Акту про економічне шпигунство.

Порогові вимоги. Акт про економічне шпигунство не передбачає порогових вимог для порушення кримінальної справи про крадіжку (незаконне присвоєння) відомостей, що становлять комерційну таємницю. Якщо обвинувачуваний свідомо украв або без дозволу правовласника отримав, знищив чи передав секретні відомості, до нього можуть бути застосовані кримінальні покарання.

Покарання, штрафи та позбавлення волі. Покарання за правопорушення дуже суворі через характер збитків, що наносяться крадіжкою (незаконним присвоєнням) відомостей, які становлять комерційну таємницю. Фізичні особи можуть бути оштрафовані на суму до 500 тис. дол. США, а юридичні особи – до 5 млн. дол. США [4,5]. Обвинувачуваний може бути також позбавлений волі строком до 10 років. Крім того, майно, яке використовувалося для скоєння злочину, а також отримані злочинним способом доходи можуть бути конфісковані.

Оскільки відповідно до Акту про економічне шпигунство крадіжка (незаконне присвоєння) відомостей, що становлять комерційну таємницю, розглядається як вид крадіжки майна, законодавством США вимагається не тільки фізичне повернення украденої комерційної таємниці, але й відновлення власнику прав на комерційну таємницю цінності секретних відомостей, що її становлять. Цінність включає збитки, понесені власником прав на комерційну таємницю. Відновлення цінності присуджується додатково до грошових штрафів.

Акт про економічне шпигунство також надає прокуророві повноваження подати цивільний позов для видачі судової заборони у зв'язку з потенційним або фактичним порушенням законодавства. Така судова заборона відіграє важливу роль у захисті відомостей, що становлять комерційну таємницю, від наступного розголошення або використання, що спричиняють шкоду та збитки.

Повторні правопорушення (рецидиви). При винесенні вироку в кримінальній справі про захист прав на комерційну таємницю, як правило, до уваги приймається фактор рецидивізму, що може збільшити як суму грошового штрафу, так і строк ув'язнення. Через те, що Акт про економічне шпигунство є відносно новим законодавчим актом, він передбачає досить суворе покарання для первинних обвинувачуваних, і питання рецидивізму ще не піднімалося.

Конфіскація. Крім штрафів і позбавлення волі Акт про економічне шпигунство передбачає винесення судом наказу про конфіскацію будь-яких доходів або майна, що отримані прямо або опосередковано від порушень норм Акту про економічне шпигунство. Суд може також винести наказ про конфіскацію будь-якого майна, що використовувалося при скоєнні злочину або вживалося для сприяння у

скоєнні злочину. Таке майно вилучається і конфіскується без компенсації обвинувачуваному. При розгляді питання про конфіскацію засобів, що використовувалися або призначалися для використання при скоєнні крадіжки відомостей, які становлять комерційну таємницю, або сприянні у скоєнні крадіжки (незаконного присвоєння), суд може врахувати *«характер, обсяг і ступінь використання майна при скоєнні злочину»*.

ОБ'ЄКТИ ПОСЯГАННЯ ТА ПОКАРАННЯ ЗА УЧАСТЬ В ЕКОНОМІЧНОМУ ШПИГУНСТВІ

Крім визначення крадіжки відомостей, що становлять комерційну таємницю, як злочину (незаконне присвоєння), Акт про економічне шпигунство передбачає кримінальне покарання за умисну крадіжку цих відомостей, що вчинена на користь іноземної держави, іноземної організації або агента (що також називається «економічним шпигунством»). Покарання за участь в економічному шпигунстві, як правило, є суворішими, ніж за крадіжку відомостей, що становлять комерційну таємницю. Максимальний грошовий штраф, що накладається на особу, яка вчинила подібні дії, становить 500 тис. дол. США, а максимальний строк позбавлення волі збільшується до 15 (п'ятнадцяти) років. Для юридичних осіб, які беруть участь в іноземному економічному шпигунстві, сума грошового штрафу зростає до 10 млн. дол. США.

Найбільший інтерес розвідки різних країн виявляють до інформаційних систем – 21,8 % від загального числа підозрілих контактів. На другому місці стоять лазери і оптика (10,7 %), далі — аеронавтика (9,7 %) і різні датчики та сенсори (9,5 %). Крім цього, розвідки інших країн різною мірою цікавляться озброєнням і енергетичними матеріалами (9,2 %), електронікою (6,6 %), космічними системами (6,5 %), морськими системами (4,8 %), матеріалами та їх обробкою (4 %), а в 3,6 % випадків проявляють зацікавленість процесом контролю підписів на документах. Лідером серед способів одержання американських секретів став простий «запит інформації» (34,2 %). Покупка секретів стоїть на другому місці (32,2 %). Інші способи, такі, як використання особистих відносин, спроби добування інформації через Інтернет, робота на конференціях і семінарах, культурний обмін і наполегливі звернення до маркетингової служби виявилися не такими затребуваними, і частота

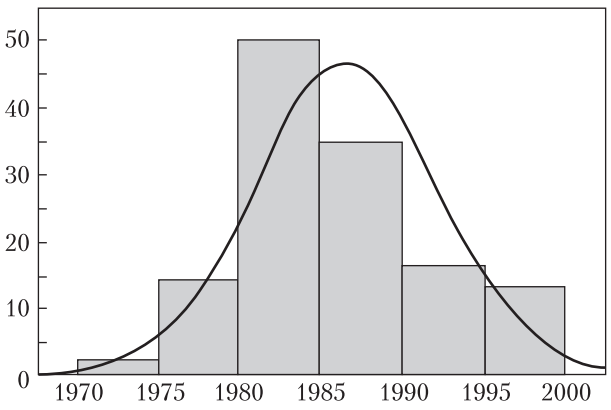

Рис. 1. Офіційна статистика розкриття ФБР справ про шпигунство в США за 30 років

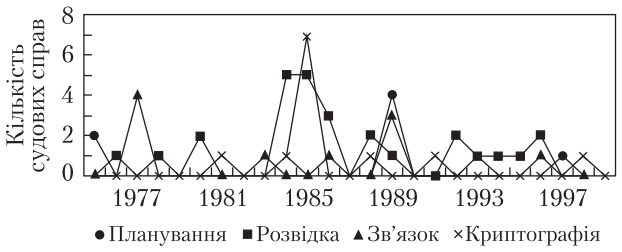

Рис. 2. Вибіркова динаміка областей шпигунства по роках

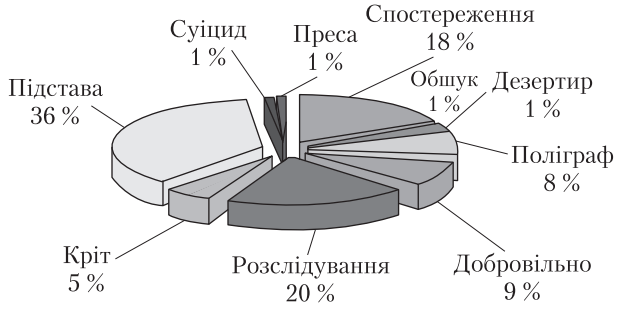

Рис. 3. Спосіб викриття шпигуна

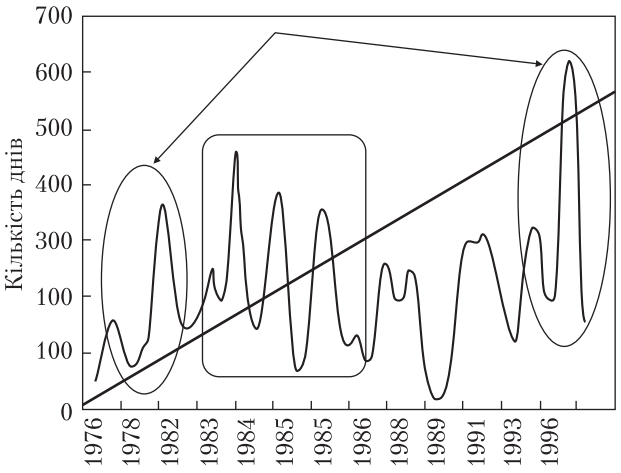

Рис. 4. Тривалість розслідування справ про шпигунство

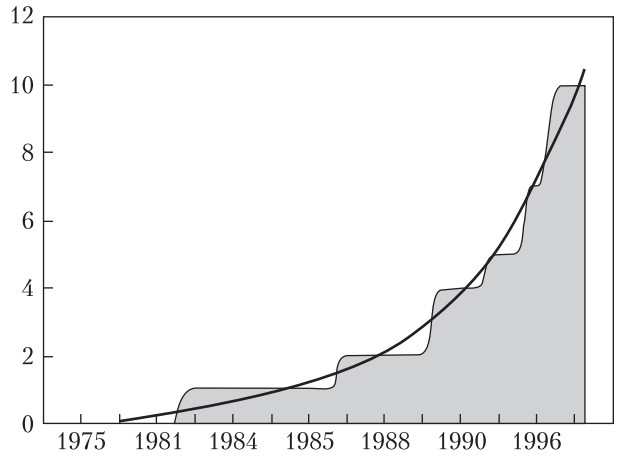

Рис. 5. Динаміка розкриття справ ФБР про шпигунство в області інформаційних технологій

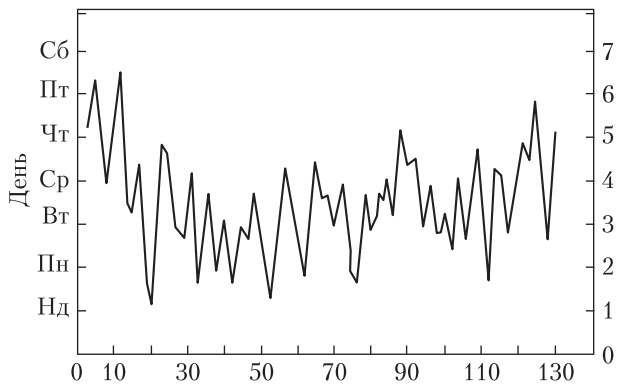

Рис. 6. Розподіл кількості арештів ФБР по днях тижня за 30 років

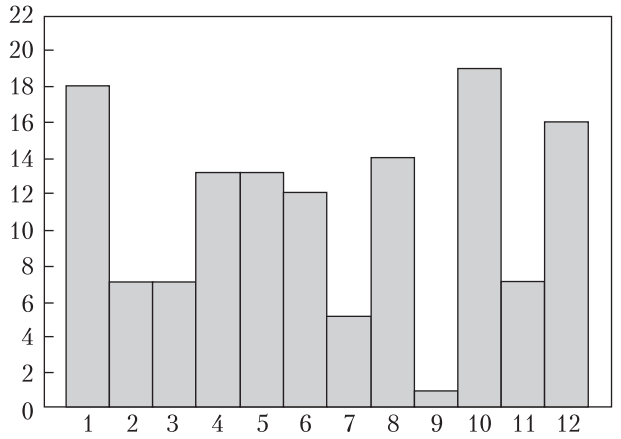

Рис. 7. Гістограма розподілу кількості арештів ФБР по місяцях

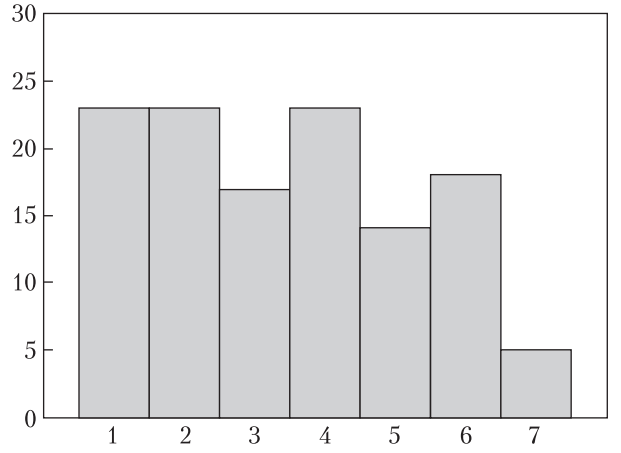

Рис. 8. Гістограма розподіл кількості арештів ФБР по днях тижня

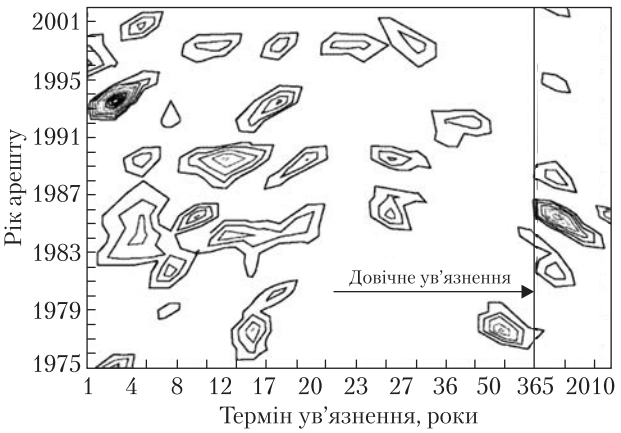

Рис. 9. Розподіл терміну ув'язнення за присудами суду

використання кожного такого способу не перевищує десяти на сотню. Євразія посіла перше місце щодо зацікавленості в області озброєнь і енергетичних матеріалів, а також військових технологій морського призначення. Військова контррозвідка встановила, що на країни цього регіону припадає 31,60 % від загального числа спроб отримання інформації про американське озброєння та енергетичні матеріали і 35,45 % у сфері військових технологій морського призначення [11].

Детальний економіко-статистичний аналіз стану, виявлення, розслідування справ і покарання за економічне шпигунство в ФБР США подано на діаграмах і графіках: офіційна статистика розкриття справ про шпигунство за 30 років (рис. 1); вибіркова динаміка галузей шпигунства по роках (рис. 2); спосіб виявлення шпигуна (рис. 3); тривалість розслідування справ про шпигунство (рис. 4); динаміка розкриття справ про шпигунство в галузі інформаційних технологій (рис. 5); розподіл кількості арештів по днях тижня за 30 років (рис. 6); розподіл кількості арештів по місяцях (рис. 7); розподіл кількості арештів по днях тижня (рис. 8); розподіл терміну ув'язнення за вироком суду (рис. 9); залежність кількості пунктів звинувачення шпигуна від розміру отриманого ним гонорару (рис. 10).

Приклад. *У червні 1997 р. за спробу продати дискети, креслення та інші матеріали з конфіденційною інформацією компанії, яка сама повідомила зацікавлену сторону про підготовку до протиправної дії, до 15 місяців тюремного ув'язнення було засуджено колишнього співробітника компанії «PPG Industries». ФБР затримало також двох американців китайського походження, які намагалися нелегально придбати матеріали американської фірми «Bristol-Myers Squibb» про виробництво біопрепарату для лікування ракових захворювань. Покупцем цієї біотехнології виступав тайванський мультинаціональний конгломерат «Yuen Foong Paper Manufacturing Company». Якби викрадення вдалося, потенційні втрати американської фір-*

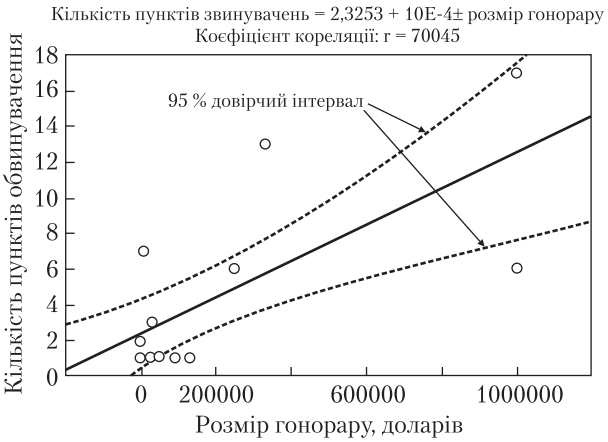

Рис. 10. Регресія кількості висунутих судом пунктів звинувачення шпигуна на розмір отриманого ним гонорару

ми могли б скласти мільярди доларів. До одного року тюремного ув'язнення і 30 тис. дол. штрафу був засуджений Гарольд Ворді, колишній службовець «Eastman Kodak Corporation», який при звільненні з фірми «прихопив» тисячі конфіденційних документів і почав надавати «консультаційні послуги» іншим фірмам, у т. ч. закордонним. І в цьому випадку втрати від розголошення секретної технологічної інформації могли б скласти мільярди доларів [6].

Економічне шпигунство в цілому вимагає таких самих доказів, що й крадіжка відомостей, які становлять комерційну таємницю (незаконне присвоєння). Прокурор повинен довести, що обвинувачуваний украв або без дозволу правовласника одержав, знищив чи передав відомості, які становлять комерційну таємницю. Він повинен також довести, що той знав або мав підстави вважати, що ці відомості є комерційною таємницею, і ці відомості дійсно є комерційною таємницею.

Крім цього, для доведення факту іноземного економічного шпигунства (відповідно до визначення, яке міститься у розділі 1831 Акту про економічне шпигунство) прокурор повинен також доказати, що обвинувачуваний знав про те, що злочин принесе вигоду або був скоєний із наміром принести вигоду іноземній державі, іноземній організації або іноземн-

ному агенту. Термін *«іноземна структура»* (*foreign instrumentality*) означає *«будь-яке відомство, бюро, відділ, установу, асоціацію або будь-яку юридичну, комерційну організацію або підприємство, фірму чи організацію, які в значній мірі належать іноземній державі, нею контролюються, спонсоруються, управляються або перебувають під її впливом»*. Термін *«іноземний агент»* означає *«будь-яка посадова особа, співробітник, довірена особа, державний службовець, делегат або представник іноземної країни»*.

Таким чином, прокурор повинен продемонструвати, що обвинувачуваний знав або мав тверде переконання про те, що незаконне присвоєння принесе вигоду іноземній структурі. Якщо ця *«структура»* не є сама по собі державною структурою (наприклад, якщо це компанія), то повинні бути представлені докази наявності фінансової підтримки з боку іноземної держави або *«скоординованої розвідувальної діяльності»*.

ДОКАЗИ У КРИМІНАЛЬНИХ СПРАВАХ ПРО ПОРУШЕННЯ ПРАВ НА КОМЕРЦІЙНУ ТАЄМНИЦЮ

Доказом дійсно існуючої комерційної таємниці, яка має правову охорону, є зазвичай свідчення про те, що відповідні відомості невідомі широкій громадськості, мають цінність завдяки своєму секретному характеру, а також що власник прав на комерційну таємницю вжив розумних заходів з метою захисту таємності цих відомостей. Докази, які використовуються при розгляді цивільних справ, можуть використовуватися і в кримінальних справах. Це можуть бути документальні докази у вигляді наклейок-попереджень про конфіденційність відомостей та інші обмеження, що розміщуються на матеріальних носіях, які містять відомості, що становлять комерційну таємницю; попереджувальні знаки про обмеження доступу в місцях зберігання чи використання цих відомостей або укладені угоди про їх конфіденційність. Відсутність загальних знань про відомості в рамках відповідної галузі може бути встановлена безпосередньо за допомогою показань свідків або опосередковано шляхом оцінки комерційної таємниці (відомості, що є відомими широкому загалу, матимуть невелику цінність або ж взагалі не матимуть цінності).

Приклади. *У справі «PepsiCo v Redmond» найбільш складним виявилося встановлення наявності ділового секрету як такого. При цьому суд брав до уваги ступінь поінформованості про секрет за межами компанії-позивача; міру знайомства співробітників компанії «PepsiCo» та інших залучених до її діяльності осіб; строгість застосовуваних заходів інформаційної безпеки; цінність конфіденційної інформації як для позивача, так і для конкурентів; обсяги витрат, і, нарешті, можливість отримання або відтворення цієї інформації іншими особами. Хоча для ділових секретів вимога новизни не є обов'язковою умовою, вони повинні представляти собою недоступну для громадськості інформацію або комбінацію елементів інформації, кожен з яких окремо не складає секрету. При цьому власник інформації зобов'язаний вжити розумні заходи збереження конфіденційності. Після розгляду справи «PepsiCo v Redmond» поняття загрози незаконного привласнення ділового секрету включило доктрину так званого «неминучого розкриття». Через 6 днів після того, як ознайомлений в деталях розвитку виробництва віце-президент Північно-американського відділення «PepsiCo» звільнився з нього і збирався перейти на роботу в конкуруючу компанію «Quaker», компанія «PepsiCo» подала позов до суду, вимагаючи заборонити цей перехід, оскільки це пов'язано із ризиком «неминучого розкриття» надзвичайно важливих питань цінової і маркетингової політики. Суд першої інстанції задовольнив позов «PepsiCo» і зобов'язав відповідача не приступати до роботи в компанії «Quaker» протягом 6 місяців. Апеляційний суд підтримав рішення суду першої інстанції.*

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 нерозкриття 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 [7].

Для доказу злочинного умислу необхідно довести, що обвинувачуваний свідомо брав участь у крадіжці або спробі украсти відомості, що становлять комерційну таємницю (тобто, скоїв злочинне присвоєння). Таке злочинне присвоєння включає набуття, перетворення, використання або розголошення відомостей, що становлять комерційну таємницю. Необхідно показати, що крадіжка (незаконне присвоєння) була здійснена обвинувачуваним свідомо, тобто він діяв з умислом або «навмисно». Обвинувачуваний повинен також усвідомлювати, що відомості, які він краде або перетворює, є відомостями, права на які належать іншій особі, і він не мав права їх набувати, використовувати або розголошувати. Знання обвинувачуваним про такий статус відомостей часто доводиться завдяки позначенням, які наносить правовласник на матеріальних носіях, що містять відомості, які становлять комерційну таємницю, існуванню угоди про нерозголошення цих відомостей між обвинувачуваним і власником прав на комерційну таємницю або навіть завдяки високій ціні, яку інша особа готова заплатити за одержання доступу до таких відомостей.

Приклад. *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 передав вкрадені матеріали, захотів їх реалізувати, у того був проведений обшук. У листопаді 2010 р. Кесюе Хуана офіційно звинуватили у викраденні інформації у Cargill Inc. [8].*

Як наголошується в опублікованій в жовтні 2011р. доповіді американської контррозвідки про економічне кібершпигунство, завдання шпигунів значно полегшує поширення оцифрування даних та їх електронних носіїв.

Приклад. *Громадянин США Донгфан Чан працював інженером у корпорації Boeing на таких проектах, як бомбардувальник B-1 та космічні човники. На початку 2011 року він був засуджений до 15 років ув'язнення за економічне шпигунство на користь китайських авіакомпаній. При обшуку в нього вдома було вилучено 250 тис. сторінок секретних документів. Раніше вони б*

зайняли кілька ящиків, а сьогодні вмістилися в одному диску вартістю 75 центів.

Як підкреслюється в доповіді, кібершпигунство нині представляє для США значно серйознішу небезпеку, ніж його традиційні різновиди [9].

Серед особливостей американського законодавства про захист комерційної таємниці слід виділити заходи кримінальної відповідальності як найбільш ефективні засоби забезпечення прав та інтересів власника комерційної таємниці. Вважається, що передбачена законом цивільна відповідальність (відшкодування збитків) недостатня для запобігання інформаційних злочинів.

Директор ФБР Роберт Мюллер 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 [10].

Таким чином, з метою забезпечення конкурентоспроможності національної економіки захист комерційної таємниці здійснюється не тільки в приватних, а й у публічних інтересах.

ЛІТЕРАТУРА

1. *Івченко О.* Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка // Юридичний журнал. – 2003. – № 7. – [Електронний ресурс] / Режим доступу: http://justinian.com.ua/magazines.php.
2. *Китай* і Росія: «агресивні» спонсори кібер-шпигунства – контррозвідка США // The Epoch Times Україна 15.11.2011. [Електронний ресурс] / Режим доступу: http://www.epochtimes.com.ua/world/conflicts/kitay-i-rosiya-agresivni-sponsori-kiber-shpigunstva-kontrrozvidka-ssha-99960.html.
3. *Экономический* шпионаж. [Електронний ресурс] / Режим доступу: http://www.agentura.ru/library/hirschmann/part4/.
4. *Андрощук Г.А. Крайнев П.П.* Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Ин Юре. – 2000 с.
5. *Андрощук Г.А., Крайнев П.П.* Правовое регулирование защиты коммерческой тайны за рубежом. // Экономическая безопасность, разведка и контрразведка. – 2002. – № 1. – С. 18–45.
6. *Фрих Л.* США в борьбе с экономическим шпионажем. [Електронний ресурс] / Режим доступу: http://corruption.rsuh.ru/magazine/5-2/n5-11.html.
7. *Практика* защиты коммерческой тайны и интеллектуальной собственности в США. – К.: Хрещатик, 1992. – 168 с.
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] / Режим 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. *Козловский В.* США: Россия и Китай – лидеры кибершпионажа. [Електронний ресурс] / Режим доступу: http://www.bbc.co.uk/russian/international/2011 / 11/111105_russia_cyberespionage.shtml.
10. *Economic* Espionage.[Електронний ресурс] / Режим доступу: http://www.fbi.gov/about-us/investigate/coun te rintelligence/economic-espionage.
11. *В США* резко возросла активность иностранной разведки. [Електронний ресурс] / Режим доступу: http://news.liga.net/news/world/324831-v-ssha-rezko-vozrosla-aktivnost-inostrannoy-razvedki.htm.

Г.А. Андрощук

ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ В США: ПРОТИВОДЕЙСТВИЕ ЭКОНОМИЧЕСКОМУ ШПИОНАЖУ

Рассмотрены экономико-правовые аспекты защиты коммерческой тайны. Дается определение понятий экономическая разведка, промышленный шпионаж, анализ Закона об экономическом шпионаже (*Economic Espionage Act*), экономико-статистические показатели состояния, выявления, расследования дел и наказания за экономический шпионаж. Приводятся рекомендации ФБР по защите бизнеса от экономического шпионажа. Делается вывод, что защита коммерческой тайны осуществляется также с целью обеспечения конкурентоспособности национальной экономики.

Ключевые слова: экономический шпионаж, коммерческая тайна, правовая охрана, промышленный шпионаж, разведка.

G.A. Androshchuk

PROTECTION OF TRADE SECRETS IN THE U.S.A: COMBATING ECONOMIC ESPIONAGE

The economic and legal aspects of the protection of trade secrets are considered. The definition of the concepts of economic intelligence, industrial espionage, analysis of the law on economic espionage (Economic Espionage Act), economic and statistical indicators of the state, detection, investigation and punishment cases in economic espionage are given. Recommendations of FBI to protect business from economic espionage are presented. It is concluded that protection of trade secrets is also carried out to ensure the competitiveness of the national economy.

Key words: economic espionage, trade secrets, legal protection, industrial espionage, intelligence.

Стаття надійшла до редакції 20.02.12