УДК 339.9

Г. О. АНДРОЩУК, канд. екон. наук, доцент

ЕКОНОМІЧНЕ ШПИГУНСТВО: ЗРОСТАННЯ МАСШТАБІВ І АГРЕСИВНОСТІ* (Частина І)

Все таємне стає явним
(Біблія. Євангелії від Марка (гл. 4, ст. 22)
та від Луки (гл. 8, ст. 17))

Резюме. *Здійснено економіко-правовий аналіз стану та тенденцій розвитку економічного шпигунства й захисту об'єктів ІВ у процесі міжнародного науково-технічного співробітництва та трансферу технологій. Показано (на прикладі США) роль держави, спецслужб і керівництва підприємств у протидії економічному шпигунству. Розглянуто роль комерційної таємниці в міжнародній конкуренції як інтелектуального капіталу, базису збереження результатів інноваційної діяльності та конкурентних переваг на ринку. Наведено приклади розслідування гучних справ з економічного шпигунства за останні роки. Робиться висновок про те, що більшість розкрадань комерційної таємниці (понад 90% випадків) здійснюється інсайдерами. Запропоновано низку превентивних заходів з охорони комерційної таємниці.*

Ключові слова: *економічне шпигунство, інтелектуальна власність, комерційна таємниця, кібершпигунство, недобросовісна конкуренція, промислове шпигунство, національна безпека, інсайдер.*

ВСТУП

Економічне шпигунство є одним із супутників ринкової економіки, причому внаслідок посилення конкурентної боротьби як на національних, так і міжнародних ринках, його масштаби значно зростають. Експерти американського Національного контррозвідувального центру (структурного підрозділу ФБР) щорічно за завданням Конгресу готують аналітичну доповідь із проблем економічного шпигунства в США. На їхню думку, економічне шпигунство є зростаючою загрозою для національної безпеки країни, послаблює її лідируючі позиції в науково-технічній сфері [1].

За даними американської контррозвідки, з початку 90-х років минулого століття усе чіткіше стала виявлятися переорієнтація іноземних спецслужб, які працюють проти США, на добування секретної інформації про новітні американські розробки у сфері критичних технологій.

Інтелектуальна власність (ІВ) — це не тільки правова, а також і складна економічна категорія. Вона бере участь у створенні доданої вартості, особливо у високотехнологічних галузях, робить свій внесок у вартість сукупних активів господарюючих суб'єктів і збільшує ринкову капіталізацію бізнесу. Виключні майнові права на результати інтелектуальної діяльності є "четвертим кошиком" у світовій торгівлі, разом із товарами, роботами і послугами. Нова роль ІВ як самостійного товару на ринку почала даватися взнаки наприкінці XX століття. У країнах, де сформований цивілізований ринок ІВ, обсяги торгівлі правами досить значні. Продаж ІВ у світовій торгівлі в рамках СОТ становить до 10% від ВВП країн, що входять до СОТ [2, с. 55].

Інститут ІВ є системоутворюючим ядром сучасної глобальної економіки. Поява нових результатів інтелектуальної, творчої діяльності, їх правова охорона на зовнішніх ринках передують матеріальному руху товарів і послуг. Самі об'єкти права також є товаром — ринок ІВ зростає темпами, що перевищують темпи зростання "матеріальних" ринків — понад 10% в рік (Китай — 23%, США — 5%, Франція — 2%, Росія — 5%). Від того, які результати інтелектуальної діяльності залучені в економічний оборот, яка їхня вартість і швидкість обороту, залежить динаміка зростання ВВП і глобальних індексів конкурентоспроможності національних економік.

На горизонті 2025 р. роль ІВ та цифрової інфраструктури обороту прав ІВ стане ключовим чинником, що визначатиме зростання національних економік і, як результат — вплив країни в світі. Передумови для цього створені розвитком глобальних цифрових мереж, понад 70% трафіку яких становить рух об'єктів ІВ [3, с. 7].

* Статтю підготовлено в рамках виконання НДІ інтелектуальної власності НАПрН України теми фундаментального дослідження «Інтелектуальна власність як складова системи забезпечення національної безпеки».

У процесі розвитку міжнародного науково-технічного співробітництва з промислово розвинутими країнами питання, пов'язані з купівлею-продажем технології, що включає передачу знань, науково-технічного, комерційного та управлінського досвіду (ноу-хау), набувають особливої актуальності та вимагають комплексного врегулювання, перш за все, на національному рівні. Тому необхідний ефективний захист майнових інтересів власників комерційної таємниці, ноу-хау не тільки в процесі співробітництва із зарубіжними країнами, а й усередині країни, оскільки ліцензійні договори, договори про передачу ноу-хау між партнерами стають тим реальним інструментом, на основі якого будуються відносини в сфері обміну науково-технічними досягненнями.

Економічне та промислове шпигунство є найбільшою загрозою науково-технічній діяльності та інноваційному розвитку держав. Але воно ведеться на всіх рівнях, їм займаються держави, міжнародні організації, спеціалізовані установи і окремі особи. Основне призначення економічного шпигунства — економія коштів і часу, які необхідно затратити, щоб наздогнати конкурента, що займає лідируюче положення, або не допустити в майбутньому відставання від нього, якщо той розробив або розробляє нову перспективну технологію, а також щоб вийти на нові для підприємства і держави ринки. Це справедливо і щодо міждержавної конкуренції, де до питань економічної конкурентоспроможності додаються і проблеми національної безпеки.

Економічне шпигунство перетворилося на важливий фактор науково-технічного прогресу і політики багатьох розвинутих держав, таких як Китай, Росія, Японія, Німеччина, Індія, Іран, Бразилія, Аргентина. Наприклад, зростання індустріальної потужності Країни Сонячного Сходу пов'язують зі збільшенням числа промислових шпигунів до значної цифри — 10 тисяч. Як зазначають автори дослідження "*Китайське промислове шпигунство: придбання технологій і військова модернізація*" Китайська Народна Республіка (КНР) реалізує "навмисний проект, фінансований державою, щоб обійти витрати на дослідження, подолати культурні недоліки і "перескочити" на перший план, використовуючи креативність інших народів", тим самим досягаючи "найбільшої передачі багатства в історії" [4].

ПОСТАНОВКА ПРОБЛЕМИ

Аналіз наукових публікацій і ЗМІ свідчить про зростаючу увагу керівництва держав, міжнародних організацій, спеціалізованих установ, корпорацій, науковців і практиків до питань, пов'язаних з протидією економічному і промисловому шпигунству. Серед іноземних фахівців, які досліджували проблеми економічного, промислового шпигунства та захисту комерційної таємниці в процесі міжнародного науково-технічного співробітництва і трансферу технологій, можна назвати таких, як: Ж. Бержье, Ю. Бобилов, Р. Гасанов, К. Лайтон, К. Мелтон, Д. Найт, Д. Пулі, Ф. Рустман, Г. Штумпф, В. Черняк, Г. Яковлев, В. Ярочкін тощо. В Україні цю проблематику вивчають Г. Андрощук, І. Дахно, І. Галиця, Я. Жаліло, А. Жарінова, І. Ревак, Ю. Капіца, Т. Лічман, Б. Маліцький, Ю. Макогон, А. Марущак, С. Мосов, В. Мунтіян, І. Мігус, В. Соловйов, В. Сідак, А. Сухоруков, Л. Федулова, Ю. Якубівська та інші науковці.

Але багатогранність і комплексний, міждисциплінарний характер проблематики, динамічність змін, що відбуваються у світі в цій сфері, зокрема в США, вимагають подальших наукових досліджень.

Метою статті є економіко-правовий аналіз стану та тенденцій розвитку економічного шпигунства та захисту об'єктів ІВ, зокрема, комерційної таємниці в процесі міжнародного науково-технічного співробітництва та трансферу технологій, визначення (на прикладі США) ролі держави, спецслужб і керівництва підприємств у протидії економічному шпигунству, виявлення існуючих проблем і вироблення пропозицій щодо їх розв'язання.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

США — найпотужніша країна, їх ВВП становить чверть від світового. Показник вкладу доданої вартості, яка утворюється від обороту ІВ, становить 12%. США є найбільшим власником результатів ІВ. Уже багато років США отримує за різні відрахування від використання прав на неї величезні кошти: відповідні показники перевищують доходи від експорту сільськогосподарської продукції. Окреме питання — експорт, а також дотримання прав і законних інтересів правовласників за кордоном: найбільше джерело доходу в американському бюджеті — це надходження від експорту ІВ: ліцензій на використання, авторських прав, товарних знаків, винаходів та ін.

Уточнення понятійного апарату дослідження. Предметом обговорення на державному, регіональному та міжнародному рівнях усе частіше стають конкурентна, комерційна, ділова, корпоративна і бізнес-розвідка та властиві їм методи недобросовісної конкуренції. Замість терміна "розвідка" як синонім або антонім іноді використовується термін "шпигунство".

При аналізі сутності публікацій виникають сумніви, а чи однаковий зміст вкладають автори в ці терміни? Майже усі, хто пише на цю тему, згодні з тим, що термін "шпигунство" (часто в поєднанні з прикметниками: "промислове", "економічне", "комерційне", "корпоративне", "науково-технічне") означає в загальному вигляді **активні протиправні дії, спрямовані на збір або розкрадання цінної інформації, закритої для доступу сторонніх осіб**. Але спектр трактування терміна, використовуваного з цими прикметниками, досить широкий: від твердження, що це майже тотожні поняття, до вибудовування ієрархічної схеми взаємозв'язку цих понять (типу "економічне шпигунство" — ширше поняття, яке охоплює і такі його підвиди, як промислове, виробниче, науково-технічне, комерційне шпигунство тощо).

Відзначимо, що в США і деяких інших державах ці поняття визначені законодавчо. Так, відповідно до прийнятого в США в 1996 р. Закону "Про економічне шпигунство" (The Economic Espionage Act, EEA) і коментарів до нього *під економічним шпигунством (Economic espionage) розуміють здійснення суб'єктом зловмисних дій, пов'язаних з: (1) крадіжкою, незаконним присвоєнням, а також отриманням шляхом обману або шахрайства інформації, що становить комерційну таємницю (секрет виробництва); (2) копіюванням, відтворенням, знищенням, скачуванням і передачею (зокрема, через мережу) інформації, що становить комерційну таємницю (секрет виробництва); (3) отриманням інформації, що становить комерційну таємницю (секрет виробництва) з усвідомленням того, що вона була присвоєна або перетворена без відповідного на те дозволу, з метою надання вигоди (переваги) іноземному уряду, державному органові чи агенту*.

Відповідно *під промисловим шпигунством (Industrial espionage or Theft of trade secrets) розуміють ті самі дії, але з метою нанесення шкоди власникові інформації, що становить комерційну таємницю, пов'язану з виробництвом продукту, котрий поставляється на внутрішній і міжнародний ринок шляхом надання економічної вигоди суб'єкту, який не є власником інформації, що становить комерційну таємницю.*

Залежно від того, чи трапилось економічне (крадіжка промислових секретів на користь іноземних держав) або промислове шпигунство (крадіжка промислових секретів з комерційною метою), законодавство США визначає відповідні міри покарання.

Отже, це не тотожні поняття. Якщо йдеться про діяльність спецслужб і державних структур на зовнішньому ринку — це економічна розвідка. Коли крадіжкою технологій за кордоном займаються приватні фірми — це промислове шпигунство. А в разі, коли крадуть один у одного компанії однієї країни, прийнято говорити про ділову (конкурентну) розвідку, яка може використовувати як незаконні способи промислового шпигунства, так і легальні методи конкурентної розвідки.

Шпигуном може бути **громадянин, який перебуває на службі в розвідці іншої держави, або особа, просто завербована вороже налаштованої країною для отримання необхідних даних, що доступні йому завдяки виконанню службових обов'язків або зайняття певної посади.**

У цього злочину є різні види, які відрізняються за об'єктом правопорушення.

Так, у Кримінальному кодексі РФ існує кілька статей, пов'язаних зі шпигунством. У науці кримінального права Росії розрізняють такі види: 1) шпигунство як відокремлений злочин (ст. 276); 2) шпигунство як один із видів державної зради (ст. 275); 3) промислове шпигунство (ст. 183). Різниця між двома першими досить значна, незважаючи на те, що вони здаються схожими за своєю суттю. У першому випадку несуть відповідальність тільки іноземні громадяни або особи без будь-якого громадянства, тобто громадяни РФ не можуть відповідати за цією статтею. Вони будуть відповідати вже за ст. 275, оскільки вважається, що вони зрадили свою країну.

Промислове (або економічне) шпигунство представляє собою зовсім інший різновид подібного правопорушення. Воно характеризується тим, що тут відправляються дані, які не становлять державної таємниці, але можуть використовуватися для отримання економічних переваг. Цим видом шпигунства можуть займатися як приватні, так і державні організації. Важливо довести саме протиправність дій, щоб класифікувати їх як правопорушення, інакше буде йтися про конкурентну розвідку. Якщо комерційне шпигунство — це злочин, спрямований на отримання відомостей, що становлять інтерес з комерційною метою, то шпигунство має за мету передачу даних щодо державної таємниці або іншої інформації, яка може навіть перебувати в необмеженому доступі.

У статті 276 КК РФ йдеться про те, що будь-які дії з обробки або відправлення даних, які можуть загрожувати безпеці РФ, караються позбавленням волі на строк від 10 до 20 років. Також уточнюється обов'язкова умова для застосування цієї статті: вчинити правопорушення повинна людина з громадянством іншої країни або взагалі без нього.

Варто зазначити, що у в законодавстві нашого сусіда Білорусі також існує таке поняття, як "комерційне шпигунство". Під цим терміном розуміється викрадення або збирання незаконним способом відомостей, що становлять комерційну або банківську таємницю, з метою їх розголошення або незаконного використання. КК Республіки Білорусь (ст. 254) передбачено санкції у вигляді штрафу або арешту.

У законодавстві України до 2004 р. також існувало поняття "комерційне шпигунство". Згідно зі статтею 231 КК України, присвяченій захисту комерційної таємниці, комерційне шпигунство розумілось, як "умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення, або іншого використання цих відомостей". Але після внесення змін до статті від 16.12.2004 р. в зв'язку з розширенням складу злочину, до якого, крім комерційної таємниці, стала відноситись і банківська таємниця, законодавець вилучив поняття "комерційного шпигунства". А як казали древні китайці: "те, що не названо, не існує".

Зазначимо, що в більшості пострадянських країн уже давно зроблені кроки до становлення та розвитку інституту комерційної таємниці. Спеціальні закони про охорону комерційної таємниці діють сьогодні в Молдові (1994 р.), Киргизстані (1998 р), Туркменістані (2000 р.), Азербайджані (2001 р.), Російській Федерації (2004 р.), Таджикистані (2008 р), Білорусі (2013 р.). **В Україні спеціального закону про охорону комерційної таємниці і досі не має.**

Зростання ролі спецслужб. Із завершенням холодної війни протиборство систем не закінчилось. Воно перейшло з політичної площини в економічну. Тепер виникають уже не політичні війни за панування тієї чи іншої системи, а суто економічні. Вони перейшли від зернових, сталевих, автомобільних, нафтових до інтелектуальних — спроб заволодіти критичними технологіями четвертої промислової революції. В сучасних умовах воюють уже не корпорації, а держави. Це добре продемонстровано фразою "Що добре для Боїнга — добре для Америки".

Президент США Дж. Буш-ст. ще у 1990 р. оголосив економічну розвідку новим пріоритетом у діяльності спецслужб. Адміністрація Клінтона також підтримувала ідею посилення економічного напряму в роботі розвідки [5]. У Стратегії національної безпеки зазначалося: "збір та аналіз розвідувальної інформації, що стосується економічного розвитку, буде відігравати все більш важливу роль для розуміння світових економічних тенденцій, допоможе підвищити конкурентоспроможність американської економіки, виявивши загрози національним компаніям з боку іноземних розвідок і нечесної торгової практики" [6].

Відповідно до досліджень, проведених Американським товариством промислової безпеки, найчастіше викривають у промисловому шпигунстві громадян Великої Британії, Індії, Канади, Китаю, Мексики, Росії, Сінгапуру, Тайваню, Швеції та США. На державному рівні лідерами економічної розвідки проти США були Ізраїль, Китай, Росія і Тайвань (країни вказані в алфавітному порядку) [5].

Директор ЦРУ Роберт М. Гейтс відзначав, що запити на економічні матеріали з ЦРУ за кількістю перевищують усі інші. Майже половина всіх завдань розвідці, що надходять від 20 головних державних установ, "економічні за своїм характером". Варто зазначити, що видатки на державну економічну розвідку в США становлять майже 40% видатків спецслужб.

У 1980-ті роки економічною розвідкою, крім ЦРУ, активно почали займатися й інші відомства — Федеральна резервна система, а також міністерства фінансів і торгівлі США, які створили у себе структури, що займаються збиранням інформації і аналізом розвитку окремих держав, порушивши тим самим монополію ЦРУ на ведення цього виду діяльності. У підсумку, до початку 1990-х рр. в американській економічній розвідці сформувались такі рівні:

1) макроекономічна розвідка, закріплена наказом президента США Р. Рейгана № 12333 "Про розвідувальну діяльність Сполучених Штатів" від 4 грудня 1981 р.): діяльність зі збору розвідувальної інформації про тенденції розвитку економіки іноземних держав, включаючи відомості про сировинні ресурси, розвиток критичних технологій, фінансові системи, а також міжнародні валютні, сировинні ринки тощо;

2) економічна контррозвідка: діяльність із припинення спроб іноземних конкурентів і спецслужб з одержання торговельно-економічної, наукової і технологічної інформації американського бізнесу;

3) мікроекономічна розвідка: збирання комерційних і промислових секретів іноземних конкурентів. Мікроекономічне шпигунство в рамках роботи спецслужб у багатьох випадках було і залишається непідконтрольним керівництву в умовах ієрархічної структури відомств. Майже неможливо відслідковувати, на користь кого повсякденно працює конкретний оперативний співробітник.

Варто підкреслити, що зміна адміністрації Білого дому, нові кадрові призначення як у розвідтоваристві, так і в дипломатичному відомстві, зроблені Б. Обамою в 2009 р., нічого принципово не змінили в контексті розглянутих

проблем і тенденцій. Єднання розвідки і бізнесу — об'єктивний процес, зупинити який не владна ніяка адміністрація.

Значно більш прозорою була і є економічна контррозвідка і розвідка на макроекономічному рівні. Контррозвідка в економічній сфері є важливим пріоритетом забезпечення національної безпеки. У Стратегії національної контррозвідки США йдеться про необхідність захисту економічних переваг країни, комерційних таємниць і ноу-хау від спроб проникнення суперника. Вперше в доктринальних документах, присвячених діяльності державних спецслужб, відкрито говориться про тісну взаємодію розвідки і бізнесу.

У серпні 2017 р. адміністрація Трампа відкрила офіційне розслідування порушення прав ІВ США і їхніх союзників. Тільки в США збитки були оцінені на 600 млрд доларів на рік.

При економічному шпигунстві, яким займаються державні служби, увага приділяється не окремому продукту, а загальній картині економіки держави-конкурента. Якою структурою характеризується її господарство, в яких галузях має перевагу ("ключові технології"), що і де можна використовувати для власних досліджень і розробок, яким шляхом можна перейняти сучасні технологічні процеси виробництва. Після отримання таких основних даних конкурент розвиває свою стратегію, щоб цілеспрямовано "орієнтуватися" на окремі продукти. Всі країни світу, за деякими винятками, мають у своєму розпорядженні спецслужби, які "секретним шляхом" отримують за кордоном інформацію і аналізують її в інтересах своїх країн. Чим вагоміша геополітична роль держави, тим більше сила і обсяг її розвідувальних відомств.

Аналіз, проведений американською контррозвідкою, показує, що в 58% випадків економічне і промислове шпигунство здійснювалось за завданнями зарубіжних компаній, в 22% — в інтересах іноземних урядів і в 20% — приватних і державних зарубіжних наукових центрів і лабораторій [1]. При цьому менш розвинуті країни, як правило, прагнуть до вивезення технологій, доступних на комерційному ринку, хоча для цього нерідко доводиться порушувати правила експортного контролю. Розвинуті держави, зі свого боку, мають на меті отримання секретних розробок, здатних підвищити міць їх збройних сил.

Останнім часом також спостерігається тенденція до збільшення числа розкрадань окремих ультрасучасних компонентів і вузлів, які можуть використовуватися для модернізації застарілих збройових, розвідувальних та інформаційних систем.

Експерти особливо виділяють діяльність на території США спецслужб КНР, Японії, Ізраїлю, Франції, Південної Кореї і Тайваню. Іноземні розвідники прагнуть також добути закриті відомості про виробничу і маркетингову політику американських корпорацій, діяльність яких, перш за все, стосується оборонного комплексу, про укладені ними з урядовими відомствами США контракти, а також заходи з нарощування експорту високотехнологічної продукції.

Еволюція методів економічного шпигунства передбачає розвиток адекватних заходів протидії. Тому **економічна контррозвідка є невід'ємною складовою системи служби безпеки — як на державному, так і на корпоративному рівні.** В її завдання входить контроль за інформаційними потоками і можливими шляхами витоку

Бернар Бенсон — винахідник нових видів зброї, мільйонер, який розбагатів на реалізації патентів із різних видів озброєнь (система телеуправління для торпед, принцип польоту ракет з самонавідними головками, крило "Дельта" для надзвукових літаків, системи комп'ютерів та інше — всього понад 100 патентів), виступаючи на конференції ЮНЕСКО заявив, що накопичення секретів у запам'ятовуючих пристроях становить небезпеку, яка може обернутися катастрофою, і закликав негайно їй запобігти. Витік майже 80% даних пов'язаний із елементарною необачністю або халатністю. Йдеться також про особисте листування, саме воно є одним з каналів витоку важливих промислових секретів через необережність. У зв'язку з цим органи військової розвідки і безпеки США завели мінідосьє на більш ніж на 25 мільйонів американців, які вважалися потенційно небезпечними.

Французький дослідник Моріс Денюзьер зазначає: "Сучасна наукова, промислова та економічна інформація здебільшого легкодоступна. 95% даних, що вас цікавлять, можна отримати зі спеціальних журналів і наукових праць, звітів компаній, внутрішніх видань підприємств, брошур і проспектів, які роздають на ярмарках і виставках. Мета шпигуна — роздобути ті 5% інформації, що залишилися, в якій і криється фірмовий секрет, таємниця майстерності" [7].

Здійснення транснаціональними корпораціями екномічної розвідки призвело до плинності кадрів у спецслужбах і пов'язаних з цим втрат потенціалу. Так, склад співробітників розвідки (не тільки ЦРУ, а й інших відомств співтовариства, котрі працюють на економічному напрямі) щорічно оновлюється приблизно на 20%, оскільки багато професіоналів переходять на більш високооплачувану роботу в приватні компанії.

У США існує асоціація колишніх агентів Федерального бюро розслідувань (ФБР). Вона налічує близько 4500 членів, які пропонують промисловості свої послуги для боротьби зі шпигунами. Асоціація видає довідник про вільних детективів, а також публікує список уже працюючих. Тільки в одній компанії "Форд" працює 39 колишніх агентів ФБР, захищаючи її промислові секрети [7].

Комерційна таємниця як об'єкт інтелектуальної власності і посягань. Найбільш поширеною формою охорони ІВ є комерційна таємниця (конфіденційність) [8]. Комерційна таємниця віками використовувалася в бізнесі. Наприклад, Китай століттями реалізовував комерційну перевагу від збереження в таємниці секрету виробництва шовку з ниток тутового шовкопряда. Таємниця технології виробництва скла майстрів острова Мурано (Венеція) досі зберігається в найсуворішому секреті та передається тільки у спадок. А чого варте полювання за секретом китайського фарфору, який вкрали французи, а запатентували англійці, попередньо запозичивши його у сусідів. Або викрадення американцями креслень прядильних машин, які працювали на англійських фабриках у Ланкаширі, що стало відправною точкою для створення і розвитку бавовняної промисловості в Новому Світі.

Комерційній таємниці початково приписувалось дві переваги над патентами: низька вартість набуття прав і необмежена тривалість користування ними. Прийнята в більшості штатів судова практика, яка визнає безліч патентів недійсними і робить інформацію, що міститься в них, доступною для конкурентів, надає комерційній таємниці додаткові переваги. Чинне законодавство, наприклад, вважає, що для визнання порушення комерційної таємниці вже не потрібне підтвердження використання всіх елементів секрету, що міститься в ній. Досить довести наявність в продукції конкурента істотної подібності. Рівень новизни, необхідний для визнання наявності комерційної таємниці, нижче того, що потрібний для підтвердження патентоспроможності. Факту виявлення розкриття для громадськості хоча б деякої частини винаходу може бути достатньо для анулювання патенту, але не комерційної таємниці.

Водночас комерційна таємниця рідше привертає увагу громадськості та фахівців, ніж інші види інтелектуальної власності. Причин тому кілька. *По-перше*, конфіденційність не пов'язана з процесом державної реєстрації; вона використовується в повсякденній практиці кожним підприємцем. *По-друге*, хоча загальні положення національних законів про комерційну таємницю (секрети виробництва) мають схожість, принципи правозастосування в різних країнах різні. *По-третє*, суперечки щодо комерційної таємниці зазвичай позбавлені широкого розголосу і тому не є предметом публічного обговорення.

Економічне значення комерційної таємниці. Комерційна таємниця є специфічним об'єктом ІВ і основною складовою нематеріальних активів підприємства. Володіння нею є базисом для збереження конкурентних переваг на ринку (особливо при міжнародній конкуренції), необхідною умовою залучення інвестицій і збереження результатів інноваційної діяльності.

У популярному фільмі "Соціальна мережа" (The Social Network), що отримав безліч нагород, розповідається про те, як засновник і власник інтернет-мережі Facebook Марк Цукерберг привласнив конфіденційний бізнес-план студентів Гарварда, які найняли його для завершення роботи над їх сайтом ConnectU. Проти мережі Facebook дійсно було порушено судову справу, в тому числі в зв'язку з привласненням. У результаті спір було вирішено за багато мільйонів доларів [9].

За оцінками експертів, сукупна вартість комерційної таємниці міжнародних компаній сфери торгівлі становить п'ять трлн доларів. Щорічно вони втрачають близько 250 млрд доларів у результаті втрати комерційної таємниці [10]. За останнє десятиліття ризики втрати комерційної таємниці значно зросли. Ці тенденції актуальні й для пострадянських країн.

У зв'язку з розвитком інформаційних технологій і диференційованих технічних можливостей проблеми, пов'язані з економічним шпигунством, набувають особливої актуальності. Сьогодні засоби промислового та економічного шпигунства для деяких компаній і держав стали ефективним інструментом випередження конкурентів і становлення конкурентоспроможності на вищому рівні. Існують відпрацьовані прийоми проникнення в таємниці. Так, згідно з недавнім звітом фірми Mandiant, що займається комп'ютерною безпекою, у розпорядженні Китаю є тисячі таких фахівців — хакерів. Ніхто не знає, скільки секретів зберігається у компаніях і їх вартість. Однак основним аргументом на користь секретності в порівнянні з патентами є забезпечення безпеки. Водночас багато компаній навіть не усвідомлює рівень витоку своїх секретів. Так, 90% компаній, які обслуговує фірма Mandiant, не помітили фактів проникнення в їхні файли китайських хакерів [11].

Китайська влада не змогли б здійснити економічні перетворення "без дешевого і необ-

меженого доступу до технологій інших країн". Такий же висновок зроблено і Агентством із запобігання загрозам національній безпеці США у спеціальній доповіді 2010 р., де йдеться про те, що модернізація китайської армії "сильно залежить від інвестицій у китайську науку і технологічну інфраструктуру і від отримання новітньої зброї з-за кордону". Так само відзначається, що китайська система крадіжки технологій унікальна тим, що вона дає свободу дій "дослідним інститутам, корпораціям та іншим організаціям, які розробляють власні схеми зі збору інформації, виходячи зі своїх потреб".

За даними доповіді Центру стратегічних і міжнародних досліджень (CSIS) США світова економіка щорічно втрачає до 445 млн доларів через злочини в мережі. Останніми роками бурхливо зростає кібершпигунство, від якого страждають торгівля, конкурентоспроможність та інновації. Збиток від нього, за найскромнішими підрахунками, оцінюється в 375 млн доларів, а за найсміливішими — в 575 млн. Про це йдеться у доповіді, спонсором якої є компанія McAfee, що займається розробками в сфері антивірусного програмного забезпечення. Кібершпигунство знижує рівень прибутків винахідників та інвесторів, має серйозні наслідки і для ринку праці розвинутих країн. Найзначніші втрати несуть найбільші економіки світу — США, Китай, Японія і Німеччина. Автори доповіді оцінюють їх збитки в 200 млн доларів щороку [11].

Згідно з розрахунками фірми промислової безпеки ASIS International річна вартість вкраденої у компаній ІВ у США становила 300 млрд доларів. Екстрапольована на весь світ ця цифра становить понад один трлн доларів. За 16 років після прийняття в США Закону "Про економічне шпигунство" (EEA), яким крадіжка економічних секретів була зведена в ранг федеральних злочинів, у третині проведених згідно з цим законом розслідувань були замішані вихідці з Китаю або особи, які працювали на цю країну. Після 2008 р. вже 44% справ мали відношення до Китаю. Відповідачі викрадали секрети, які стосуються військового літакобудування та створення космічного човна, комерційну таємницю компаній as Ford, GM, Dow Chemical, Motorola і DuPont [12].

Заперечуючи висунуті звинувачення, китайська влада відзначала, що їх компанії також є жертвами промислового шпигунства. Посилаючись на глобальне дослідження фірми McAfee, яка займається безпекою інформаційних технологій, представники китайського бізнесу повідомили про найбільш високий середній рівень збитку від крадіжки ІВ, що припадає на кожну з їх компаній: 7,2 млн доларів у Китаї і тільки 375 тис. доларів у Великій Британії [12].

З практики протидії економічному шпигунству. У світовій практиці є чимало випадків порушення права на комерційну таємницю та промислового шпигунства — одного з найдавніших методів недобросовісної конкуренції. Як правило, вони мають латентний (прихований) характер і лише іноді висвітлюються у судових рішеннях, ЗМІ та спеціальній літературі.

Найбільш доступною є інформація про випадки економічного шпигунства в США. Аналізуючи інформацію з сайту Федерального бюро розслідувань (ФБР) та судову практику, можна скласти відповідне досьє та виявити певні закономірності щодо об'єктів і суб'єктів економічного шпигунства [13]. Найбільш резонансні справи: косметичні компанії — Avon проти Mary Kay Cosmetics (1991 р.); IT-компанії — Microsoft проти Oracle (2000 р.), спір з участю Apple і Samsung (триває). До речі, остання справа в 2014 р. набула дещо інших обрисів, залучаючи до суперечки ще й компанію Google за використання операційної системи, подібної до Apple.

Наведемо кілька прикладів гучних справ з економічного шпигунства в США за останні роки. У штаті Мічиган 30 квітня 2013 р. була засуджена подружня пара — колишній інженер General Motors та її чоловік — до ув'язнення і штрафу 25 тис. доларів. Згідно зі звинуваченням, вони намагалися викрасти гібридну технологію, що стосувалася комерційної таємниці General Motors з наміром використовувати її в рамках спільного підприємства з автомобільним конкурентом General Motors у Китаї (Chery Automobile). Технологія була скопійована переписуванням секретних інформаційних матеріалів на жорсткий диск, знайдений у підсудних. За попередніми підрахунками General Motors вартість викрадених документів становила понад 40 млн доларів [14].

Нещодавно компанія Dupont, що володіє великою часткою світового ринку в сфері діоксиду титану, що оцінюється щорічно в мільярди доларів, була близькою до ризику крадіжки комерційного секрету закордонним конкурентом — компанією Pangang Group Co. У червні 2013 р. китайському виробникові вітряних турбін Sinovel було пред'явлено звинувачення в незаконному привласненні комерційних секретів компанії AMSC (США), оцінених в один млрд доларів [8]. У штаті Кентуккі 16 квітня 2014 р. був засуджений колишній співробітник компанії White Drive Products Inc за розкрадання комерційної таємниці. Як і в попередньому випадку, документи без дозволу були скопійовані на портативний USB-диск. Після цього обви-

нувачений Гроус почав роботу з прямими конкурентами компанії White Drive Products Inc. Крім ув'язнення, Гроус також повинен сплатити штраф у розмірі один млн доларів.

У Каліфорнії 24 квітня 2013 р. було пред'явлено звинувачення Девіду Носалю відразу за кількома випадками викрадення комерційної таємниці комп'ютерної фірми-роботодавця Девіда. Зокрема, він здійснив три вторгнення в комп'ютерну систему компанії Korn/Ferry International, а також двічі був звинувачений у викраденні комерційної таємниці для свого нового бізнесу. Отримавши несанкціонований доступ до комп'ютера компанії, він скопіював документи, що містять торгові секрети.

Недавній випадок (судове засідання відбулося 9 червня 2014 р.) стосувався справи за обвинуваченням інженера-хіміка Матіаса Тезока у використанні комерційної таємниці. За 25 років своєї діяльності компанія Voltaix LLC розробила провідний у галузі секретний науковий метод для застосування в своїй діяльності, а саме — особливий таємний і конфіденційний рецепт виробництва в сфері виготовлення хімікатів для напівпровідникової і сонячної енергетики. При прийомі на роботу (на пуско-налагоджувальні роботи) Матіас Тезок, як і інші співробітники, підписав угоду про нерозголошення таємниці, яку згодом порушив. Після звільнення з Voltaix LLC він відкрив власну фірму Metaloid Precursors Inc, яка почала використовувати технологію виробництва Voltaix LLC для своєї економічної вигоди [17].

Грег Чунг (Greg Chung) шпигував для Китаю майже 30 років (з 1979 по 2006 рр.). Він працював на компанію Boeing і Rockwell International як спеціаліст з розрахунку напруги (stress analyst). Чунг викрав секретні відомості про конструкції космічного шаттла, ракети Delta IV і вантажного військового літака С-17 в інтересах китайського уряду [18]. За словами Чунга, його мотивом виступала "відданість своїй Батьківщині". Він викрав сотні тисяч документів у свого американського роботодавця і передав їх китайському уряду під час подорожей до Китаю під виглядом читання лекцій, таємно зустрічаючись з китайськими агентами. Чунг співпрацював також із іншим китайським шпигуном Чи Маком (Chi Mak), щоб передавати цінну інформацію в Китай.

Слідчі дійшли висновку, що Чунг почав шпигувати для китайців ще наприкінці 1970-х, відразу після того, як став громадянином США і був найнятий Rockwell International. Він працював у компанії Rockwell, поки вона в 1996 р. не була куплена Boeing і аж до звільнення в 2002 р. Через рік, компанія знову найняла його як консультанта. Він був звільнений лише після того, як ФБР почало розслідування його діяльності. Незаконну діяльність Чунга слідчі виявили, розслідуючи в 2006 р. справу з економічного шпигунства іншого китайського шпигуна. Розслідування привело їх в будинок Чунга, де була виявлена схованка конфіденційних документів. Ці документи включали, зокрема, інформацію про паливну систему для ракети-носія на шаттлі, тобто ті документи, які інженеру було суворо наказано "закривати" наприкінці кожного дня. Компанія Boeing інвестувала в розробку цих технологій 50 млн доларів протягом п'яти років [19].

Американський інженер Грег Чунг був визнаний винним у веденні 30-річної діяльності економічного шпигунства, після того, як поліція виявила в його будинку 300 тисяч сторінок секретних матеріалів. Він був визнаний винним за шістьма пунктами в економічному шпигунстві; по одному пункту, що діяв як іноземний агент; за звинуваченням у змові; а також за статтею, що він повідомляв неправдиву інформацію федеральним агентам.

Адвокати Чунга намагалися довести, що їхній клієнт був усього лише злодієм документів, знайдених у нього в будинку, і наполягали, що він не був шпигуном. Вони стверджували також, що Чунг порушив тільки політику конфіденційності компанії Boeing, принісши документи до себе додому, але не порушував ніяких законів, і уряд США не може довести, що він передавав секретну інформацію Китаю. Однак суддя Кормак Дж. Карні відхилив припущення про те, що Чунг був злодієм, як "сміховинне". У судовій постанові окружний суддя Кормак Дж. Карні зазначив: "Довіра, яку висловила компанія Boeing містеру Чунгу, щоб захистити свою власність і комерційну таємницю, очевидно, значила для містера Чунга дуже мало. Він знехтував цим, щоб служити КНР (Китайській Народній Республіці), яку він з гордістю проголосив своєю батьківщиною". У лютому 2010 р. Грег Чунг був засуджений до більш ніж 15 років позбавлення волі. Суд над Грегом Чунгом був першою справою у рамках Закону "Про економічне шпигунство" (Economic Espionage Act) 1996 р. Китайський уряд у цій справі не зробив ніяких коментарів.

Інший китайський шпигун — Лі Мак, який також фігурував у цій справі, зізнався, що ще в 1978 р. він був відправлений у США, щоб отримати роботу в оборонній промисловості з метою здійснення промислового шпигунства. Більше 20 років він передавав інформацію про конструкцію тихих електричних силових установок для підводних човнів США, відомості про радіолокаційні системи Aegis, а також інформацію про стелс-літаки, що розробляються ВМС

США. Китайський уряд також доручив Макові шукати інформацію про будь-які інші технології. Макові допомагали члени його сім'ї під час зашифровування і таємної передачі інформації в Китай. У травні 2007 р. Лі Мак був визнаний винним у змові, відсутності реєстрації як агента іноземної уряду, а також в інших порушеннях. Він був засуджений до більш ніж 24 років позбавлення волі [20].

Колишній науковий співробітник компанії Dow Chemical Вень Чю Лю (Wen Chyu Liu) в січні 2012 р. був засуджений до 60 місяців в'язниці за двома звинуваченнями, штрафу в 25000 доларів і вилученню 600000 доларів. У лютому 2011 р. він був звинувачений у крадіжці торгових секретів у свого колишнього роботодавця і продажу їх компанії в Китаї. Лю вступив у змову не менше ніж з чотирма діючими і колишніми співробітниками. Він подорожував Китаєм, щоб продати отриману інформацію, заплатити залученим співробітникам за матеріали та інформацію. Одного зі співробітників він підкупив за 50 тис. доларів готівкою, щоб отримати керівництво з виробничого процесу та іншу необхідну інформацію, пов'язану з хлорвмісним поліетиленом (CPE).

Вень Чю Лю, він же Девід В. Лю, в 1960-ті роки приїхав у США з Китаю як аспірант. У 1965 р. Лю став працювати науковим співробітником в Dow Chemical Company's — у відділі, розташованому в Плакемінсі штату Луїзіана (Plaquemine, LA). Він був зайнятий на різних етапах розробки і виробництва еластомерів, зокрема хлорованого поліетилену.

Хімічна компанія The Dow Chemical Company (Dow) — провідний виробник хлормісткого поліетилену ("CPE"), що є еластомірним полімером, який вона продає по всьому світу під назвою "Тірин CPE". CPE — це біла, порошкоподібна речовина, стійка до екстремальних тисків і температур. CPE використовується у гідравлічних, автомобільних і промислових шлангах, електричних оболонках кабелів, а також будівельних і конструкційних матеріалах — таких, як вінілова обшивка. Компанія Dow виробляє CPE на двох підприємствах: у Плакемінсі і в Стаді (Німеччина). Свідки уряду показали, що компанія Dow вклала мільйони доларів у розробку і вдосконалення процесу виробництва CPE та його кінцевий продукт. Вони стверджували, що інвестиції і дослідження корпорації привели до розвитку важливих уточнень за умовами експлуатації і виготовлення CPE, а також до поліпшення проектних технічних специфікацій деяких апаратів і обладнання, що використовуються у процесі. Уряд заявив, що Лю змовився вкрасти комерційну таємницю компанії Dow і продавав цю інформацію китайським виробникам для власного збагачення.

Компанія Dow 1 липня 1999 р. подала цивільний позов проти Лю, звинувачуючи його в крадіжці комерційних секретів, які використовувалися у виробництві своєї CPE [21; 22].

Термін "комерційна таємниця", як це визначено в законодавстві США, означає: всі форми і види фінансової, ділової, наукової, технічної, економічної або технічної інформації, зокрема, моделі, плани, збірники, програмні пристрої, формули, конструкції, прототипи, методи, методики, процеси, процедури, програми, або коди, матеріальні чи нематеріальні, незалежно від форми зберігання (в фізичному, електронному вигляді, наочно, фотографічно або в письмовій формі), якщо її власник прийняв розумні заходи, щоб тримати таку інформацію в таємниці, і якщо інформація має економічну цінність, фактичну або потенційну, не будучи загальновідомою і легко встановленою.

За словами свідків уряду, компанія Dow вважає виробничий процес і обладнання, призначене для процесу, комерційною таємницею, яка надає їй конкурентну перевагу. Компанія вживає відповідних заходів фізичної та юридичної безпеки для захисту своєї технології і процесів, які використовуються у виробництві CPE. Такі заходи включають обмеження доступу до об'єктів компанії Dow і угоди про конфіденційність і нерозголошення інформації з працівниками, зокрема з Лю.

Лю (Liou) працював у Dow з 1965 р. аж до свого виходу на пенсію в 1992 р. Він працював у відділі досліджень і розробок з різних аспектів виробництва виробів компанії Dow, зокрема CPE. Приступаючи до роботи, Лю підписав угоду про конфіденційність, в якій зобов'язувався не розголошувати конфіденційну інформацію та комерційну таємницю третім особам. Після виходу Лю на пенсію компанія Dow відправила йому лист, нагадуючи про відповідну угоду. На початку 1990-х, до виходу на пенсію, Лю і його дружина створили компанію Pacific Richland у Батон-Руж (штат Луїзіана). Незабаром після цього китайські компанії висловили зацікавленість у створенні хлорованого полівінілхлориду (CSM або CPVC). Хоча Dow ніколи не виробляла CSM, CPE використовується як інгредієнт у виробництві CSM. Лю найняв на роботу деяких колишніх і тоді нинішніх співробітників компанії Dow, щоб допомогти йому в налагодженні процесу виробництва CPE. Серед співробітників були: Джон Уілер — інженер, колишній керівник проекту з модернізації заводу з виробництва CPE в Плакемінсі та консультант компанії Dow, коли Лю завербував його; Хейн

Мейер — інженер, який допоміг побудувати завод Dow у Стаді та працював до 1997 р. на Dow у Німеччині; Кот Стокер — старший інженер, відповідальний за координацію щоденного виробництва CPE, який працював на компанію Dow у 1999 р. і був автором значної частини керівництва з виробництва CPE компанії Dow. Під час розслідування справи всі троє співпрацювали з урядом і давали свідчення проти Лю у ході судового розгляду. Так, свідки уряду показали, що після створення Pacific Richland, Лю попросив Уілера забезпечити процес проектування виробництва CPE, щоб Pacific Richland міг продати його китайським компаніям. Уілер показав, що він створив схему інженерного потоку для процесу виробництва CPE, заснованого на знанні фабрик Dow із виробництва CPE. Лю і Уілер потім зробили кілька поїздок до Китаю для продажу процесу CPE для китайських клієнтів і Лю фінансував ці поїздки. Китайські компанії Qingdao Chemical Works ("Qingdao") and Hubei Shaunghuang Chemical Group Company ("Hubei") висловили зацікавленість у будівництві заводів у Китаї. Згідно зі свідченнями, компанії були спеціально зацікавлені в отриманні "технології Dow". Лю підписав контракти про продаж обом компаніям інженерного пакета CPE і наполіг на тому, щоб отримати від цих контрактів майже два млн доларів. Згодом Стокер створив для Лю керівництво з виробництва CPE. Стокер показав, що велика частина розділів цього керівництва була плагіатом із керівництва по виробництву CPE компанії Dow. Лю поставляє це керівництво з процесу виробництва CPE та інженерний пакет, в який увійшли численні інженерні документи, технологічні схеми, схеми і діаграми трубопроводів і приладів, у Хубей. Технологічні схеми зображували весь процес виготовлення CPE. Уілер підтвердив, що Лю найняв його, аби вкрасти інформацію Dow, щоб побудувати завод CPE в Китаї. Він особисто вкрав комерційну таємницю CPE Dow разом зі Стокером, Мейером і Лю, який заплатив йому близько 196 тис. доларів протягом двох з половиною років. Він також заявив, що Хубей був зацікавлений у технології Dow. Уілер розглянув і зіставив креслення сушарки Dow зі Стад і сушарки з псевдозрідженим шаром, який Лю надав китайцям, і свідчив про те, що вони були по суті ідентичні, адже "проект по Стаду був використаний, щоб зробити інший проект, проданий китайцям". Він стверджував, що розробка процесу зайняла у них лише кілька місяців, щоб завершити китайські пакети, оскільки вони вже "мали пакет Dow CPE в своїх руках". Нарешті, Уілер показав, що після того, як Dow подала цивільний позов, він став свідком того, як Лю викинув кілька коробок документів на стоянці у смітник перед зустріччю зі своїм адвокатом. Стокер, співробітник Dow у той час, коли Лю направив матеріали для китайських компаній, показав, що Лю спеціально "хотів технології Dow" і погодився виплатити йому 50 тис. доларів готівкою за допомогу. Він показав, що в керівництві представлений огляд хімічного процесу, опис апаратів і ємностей, їх розмірів, і те, що кожен з них виконує в процесі експлуатації. Лю вимагав це керівництво процесом для китайського проекту, бо він мав зобов'язання надати його в рамках свого договору з китайцями.

Стокер, який є автором значної частини керівництва процесом Dow, показав, що він займався плагіатом більшої частини керівництва Dow, розробляючи керівництво процесу для Pacific Richland. Лю обіцяв заплатити Стокеру 50 тис. доларів. Дізнавшись про те, що Dow збирався подати цивільний позов проти них, Стокер і Уілер вилучили файли з їх комп'ютерів у Pacific Richland. Лю знав, що вони видалили файл. Стокер також зазначив, що після початку цивільного позову компанії Dow він і Лю домовилися, що будуть оскаржувати позов і брехати. Нарешті, Стокер показав, що Лю пізніше переїхав у Канаду, щоб поставити себе поза досяжністю закону США. Мейер зізнався, що він особисто надав секретну технологію Dow з виробництва CPE, щоб Лю продав китайським компаніям. Мейер свідчив, що він звернувся до Лю зі своїми побоюваннями щодо використання технологій CPE, але той заспокоїв його, сказавши, що все законно.

Обвинувачення. Федеральне велике журі 24 березня 2005 р. висунуло звинувачення Лю по 15 пунктам, які інкримінували йому змову, отримання та володіння вкраденими торговими секретами, шахрайство, незаконні грошові операції і лжесвідчення. Лю був заарештований 22 серпня 2006 р. в Сіетлі (штат Вашингтон) на міжконтинентальному рейсі з Тайбей, Тайвань. Якби його визнали повністю винним за всіма пунктами звинувачення, він був би засуджений до 300 років в'язниці та майже 10 млн доларів штрафів або вдвічі більше його валового прибутку від шахрайства (залежно від того, що більше). Згідно з обвинувальним актом, Лю вступив у змову мінімум з чотирма діючими і колишніми співробітниками установ Dow у Плакемінсі і Стаді (Німеччина), які працювали там на виробництві CPE. Мета цієї змови полягала в тому, щоб привласнити комерційну таємницю, а потім продати технологію виробництва CPE різним китайським компаніям. Як представник своєї кампанії Лю подорожував по всьому Китаю, продаючи вкрадену інформацію. Він пла-

тив нинішнім і колишнім співробітникам Dow за отримані матеріали та інформацію, пов'язану з виробництвом CPE в Dow. В одному випадку Лю підкупив тодішнього співробітника підприємства в Плакемінсі за 50 тис. доларів готівкою, щоб отримати керівництво з виробничого процесу та іншу інформацію, пов'язану з CPE.

Лжесвідчення. Коли компанія Dow подала проти Лю федеральний цивільний позов, він помилково заперечував під присягою, що укладав угоди зі спільниками, подорожуючи Китаєм, щоб зустрітися із представниками китайської компанії, зацікавленої в проектуванні та будівництві нового заводу з виробництва CPE. Після цього йому пред'явили федеральні кримінальні звинувачення.

Засудження. 7 лютого 2011 р., після тритижневого судового процесу, федеральне журі в Батон-Руж, штат Луїзіана визнала Лю, якому було 74 роки, винним у змові та крадіжці з метою торгівлі секретною інформацією і в лжесвідченні в зв'язку з крадіжкою ним комерційної таємниці компанії Dow Chemical і продажу її компанії в КНР. Йому загрожувало до 10 років позбавлення волі за змову і розкрадання комерційної таємниці, і не більше п'яти років у в'язниці за лжесвідчення журі присяжних. Кожен пункт звинувачення тягне також максимальний штраф в розмірі 250 тис. доларів. У результаті Лю був засуджений за змову з метою крадіжки комерційної таємниці і лжесвідчення. Він подав апеляцію, але суд йому в ній відмовив. Районний суд засудив Лю до позбавлення волі до 60 місяців по кожному обвинуваченню.

Резюме. Більшість розкрадань комерційної таємниці здійснюється "інсайдерами" (власними службовцями компанії або особами, які працюють з ними за контрактом). За даними розслідувань, пов'язаних з порушенням закону, в ЕЕА на них припадає понад 90% випадків [23]. Зазвичай ці особи записують інформацію на флеш-диски або передають її через мобільний телефон чи електронною поштою. Респонденти дослідження фірми McAfee вважають, що рейтинг збитку від інсайдерів вищий, ніж від уразливості програмного забезпечення або від кібершпіонажу.

(Продовження статті читайте у наступному номері)

H. O. Androshchuk, PhD in Economics, Associate Professor

ECONOMIC ESPIONAGE: GROWTH AND AGGRESSIVITY (PART I)

Abstract. *Economic and legal analysis of the state and trends in the development of economic espionage and protection of IP objects in the process of international scientific and technical cooperation and technology transfer are carried out. The role of the state, intelligence services and enterprise management in countering economic espionage is shown (by the example of the USA). The role of trade secrets in international competition as intellectual capital, the basis for preserving the results of innovation activity and competitive advantages in the market are considered. The examples of investigation of high-profile cases on economic espionage in recent years are given. It is concluded that most of the theft of commercial secrets (more than 90% of cases) is carried out by insiders. A number of preventive measures to protect commercial secrets are proposed.*

Keywords: *economic espionage, intellectual property, commercial secret, cyber espionage, unfair competition, industrial espionage, national security, insider.*

Г. А. Андрощук, канд. экон. наук, доцент

ЭКОНОМИЧЕСКИЙ ШПИОНАЖ: РОСТ МАСШТАБОВ И АГРЕССИВНОСТИ (ЧАСТЬ I)

Резюме. *Осуществлен экономико-правовой анализ состояния и тенденций развития экономического шпионажа и защиты объектов ИС в процессе международного научно-технического сотрудничества и трансфера технологий. Показана (на примере США) роль государства, спецслужб и руководства предприятий в противодействии экономическому шпионажу. Рассмотрены роль коммерческой тайны в международной конкуренции как интеллектуального капитала, базиса сохранения результатов инновационной деятельности и конкурентных преимуществ на рынке. Приведенные примеры расследования громких дел по экономическому шпионажу за последние годы. Делается вывод о том, что большинство хищений коммерческой тайны (более 90% случаев) осуществляется инсайдерами. Предложен ряд превентивных мер по охране коммерческой тайны.*

Ключевые слова: *экономический шпионаж, интеллектуальная собственность, коммерческая тайна, кибершпионаж, недобросовестная конкуренция, промышленный шпионаж, национальная безопасность, инсайдер.*