УДК 339.9

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

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

(Закінчення. Початок у журналі "Наука, технології, інновації" № 3 (7) 2018 року)

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.*

Кібершпигунство. Практичні проблеми охорони комерційної таємниці розв'язати важче, ніж правові. Стрімке зростання інноваційних технологій, що зробили величезний внесок у світову економіку, полегшило можливість скоєння крадіжок цінної комерційної інформації, наприклад за допомогою фішинг-шахрайства. Комерційні шпигуни відправляють електронною поштою листи, використовуючи особисті дані, отримані з соціальних мереж; одержувачі листів не усвідомлюють, що повідомлення фальшиве. Після натискання на введене в повідомлення посилання шкідлива програма проникає в комп'ютер одержувача, а через нього — в комп'ютерну мережу компанії, де вона може залишатися місяцями і навіть роками. Цей "тихий інтервент" відшукує конфіденційні файли і паролі та відправляє їх назад хакеру, який використовує або продає отриману інформацію. Є низка превентивних заходів, включаючи наймання експертів із комп'ютерної безпеки, відсутність USB-портів на корпоративних комп'ютерах, введення політики використання співробітниками власних комп'ютерів у робочих цілях і вимоги, щоб у відрядженнях співробітники використовували "чисті" орендовані ноутбуки [23]. Ідентифікувати кібершпигунів складно, якщо врахувати масштаби і анонімність, властиві Інтернету. Оцінити збиток, нанесений бізнесу, також непросто. Багато підприємств не здогадується про те, що їхні комп'ютерні системи наражаються на небезпеку, а деякі не люблять зізнаватися у випадках крадіжки у них інформації. Але дослідження показують, що проблема загострюється, і органи влади шукають шляхи її розв'язання.

Російський слід. За останні роки інформаційні новини про хакерів і кібератаки вже стали буденністю. Найчастіше авторство зломів приписується трьом групам хакерів, яких пов'язують із російськими спецслужбами: Cozy Bear, Fancy Bear і Energetic Bear [24]. Нині у причетності російської розвідки до цих атак уже ніхто не сумнівається. Директор Національної розвідки США заявив, що російські хакери готують нову масштабну кібератаку проти Штатів і тільки чекають команди Кремля. ФБР, Міністерство внутрішньої безпеки США і Британський центр національної комп'ютерної безпеки 16 квітня 2018 р. заявили, що російські хакери атакували держструктури і приватні компанії у спробі заволодіти інтелектуальною власністю і отримати доступ до мереж своїх жертв. Аналогічні звинувачення в той же день озвучила міністр оборони Австралії Маріс Пейн.

Крадіжка мільйонів. У лютому 2017 р. Мін'юст США висунув звинувачення в крадіжці даних понад 500 млн акаунтів в Yahoo проти

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

двох офіцерів ФСБ — Дмитра Докучаєва та Ігоря Сущина. Кібератака відбулася наприкінці 2014 р. За версією звинувачення, співробітники ФСБ найняли для цього двох хакерів. Серед жертв злому виявилися і російські журналісти, і урядовці з США [24].

Енергійний ведмідь. Російські хакери з групи Energetic Bear створили програму Crash Override, за допомогою якої в 2017 р. змогли вимкнути комп'ютери, що відповідають за енергосистеми міст США. Вони легко зламали мережі малих комунальних підприємств, а потім проникли в мережі постачальників, які, в свою чергу, працюють з великими компаніями. Жертвами атаки стали сотні підприємств [24].

Червоний код. Директор Національної розвідки США Ден Коутс заявив, що російські хакери готують нову масштабну кібератаку проти США. Він підкреслив, що "система знову блимає червоним кольором", як це було напередодні терактів 11 вересня 2001 р. Коутс зазначив, що підконтрольні Кремлю кіберзлочинці частіше за інших нападають на цифрову інфраструктуру США.

На грані. Згідно з інформацією американської розвідки, нині ситуація буквально "в парі кліків" від тієї, що сталася в ході президентської кампанії 2015–2016 рр. Тоді хакери атакували Демократичний національний комітет і систему кампанії Хілларі Клінтон. У цій справі США раніше висунули звинувачення 12 російським розвідникам. Американські спецслужби і IT-компанії встановили, що влітку 2015 р. діяли представники Cozy Bear, а навесні 2016 р. — Fancy Bear. На думку розвідслужб США, кібератаки були санкціоновані високопоставленими російськими чиновниками.

Кремль готовий атакувати. Коутс підкреслив, що Вашингтон знає про задум російських хакерів, і натякнув, що зараз "вибір за Путіним". Міністерство внутрішньої безпеки США попереджає про зломи інфраструктури США російськими групами з 2014 р., проте до цих пір рівень загрози не був такий високий. За словами Коутса, Кремль готовий атакувати, а світ знаходиться на порозі нової — цифрової війни [24].

Широкомасштабне економічне шпигунство в кіберпросторі. Апарат директора національної розвідки США нещодавно опублікував доповідь, в якій Росія звинувачується в "широкомасштабному" економічному шпигунстві на кіберпросторі. Доповідь опубліковано на сайті відомства. Відзначається, що Росія, Китай і Іран представляють у кіберпросторі найбільшу загрозу, будучи найбільш успішними "гравцями" з найбільшою кількістю можливостей. За даними розвідки, Росія робить атаки для розкрадання ІВ США. Розробки потім використовуються для модернізації економіки в технологічній сфері [24].

Законодавчі зміни. Конгрес США 11 травня 2016 р. прийняв Defend Trade Secrets Act of 2016 (DTSA) — Закон "Про комерційну таємницю" (далі — Закон), який передбачає можливість притягнення до відповідальності співробітників і підрядників за розголошення комерційної таємниці компанії [25]. Звертаємо увагу: якщо раніше кожен штат встановлював правила охорони комерційної таємниці окремо, то тепер це питання врегульоване і на федеральному рівні. Дія Закону поширюється на комерційні таємниці, пов'язані з продуктами і (або) послугами, які використовуються, або ж призначені для використання в торгівлі між штатами, а також у зовнішній торгівлі. Закон передбачає такі засоби захисту комерційної таємниці:

- компанії можуть звернутися до суду з метою накладення арешту на незаконно привласнені предмети (носії інформації, які містять комерційну таємницю), що перебувають у володінні співробітників/підрядників;
- можливості накладення судової заборони з метою запобігання загрози або припинення незаконного привласнення комерційної таємниці працівником/підрядником.

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

Відповідно до Закону не вважатиметься незаконним розголошенням комерційної таємниці розкриття співробітником/підрядником такої інформації в державних органах або у судовому порядку. Однак таке розкриття буде вважатися правомірним тільки в разі наявності підозр про порушення компанією норм законодавства. Кожен співробітник і підрядник компанії повинні бути поінформовані про можливість отримання такого імунітету в порядку, передбаченому законодавством.

Зазначимо, що дія норм цього Закону поширюється не тільки на громадян і компанії США, а й на фізичних і юридичних осіб інших країн, зокрема України. Тому, якщо ви працюєте в США, плануєте здійснити вихід на американський ринок або ж співпрацюєте з місцевими компаніями, варто взяти до уваги імплементацію нових механізмів захисту.

Інформаційно-аналітичне забезпечення. Важливим засобом протидії економічному шпи-

гунству є на лише контррозвідка, а і суд. Аналітична компанія Lex Machina 18 липня 2018 р. оприлюднила перший в історії США звіт про судові суперечки у сфері комерційної таємниці. У доповіді проаналізовано показники і основні тенденції, що відбуваються протягом дев'ятирічного періоду з більш ніж 9800 справ, порушених відповідно до законів штатів "Про комерційну таємницю" і федерального Закону "Про захист комерційної таємниці" (DTSA) від 2016 р. [26]. Так, судовий розгляд справ у сфері комерційної таємниці збільшився в окружних судах США в той час, що минув з моменту проходження DTSA. У період між 2009 і 2016 рр. подача позовів про захист прав на комерційну таємницю зазвичай була у межах 860–930 випадків на рік. Проте у 2017 р. у справах, пов'язаних із комерційною таємницею, відбулось збільшення до 1334 справ. У першій половині 2018 р. уже було подано 581 позов, тобто в цьому році темпи зростання дещо перевищують кількість справ порівняно з 2017 р. Судові позови, пов'язані з комерційною таємницею, як правило, переплітаються з іншими претензіями, особливо з комерційними претензіями, такими як порушення контракту або ділового делікту. Так, з 8849 позовів щодо порушення комерційної таємниці, поданих у період між 2009 р. і другим кварталом 2018 р., тільки 2723 випадки (30,7%) стосувалися претензій щодо комерційних таємниць. Загалом 5192 випадки стосувалися претензій щодо комерційних таємниць, які збігалися з комерційними претензіями, що становить близько 60% від усіх випадків комерційної таємниці.

Lex Machina розширила свою платформу Legal Analytics до судових розглядів із комерційної таємниці, її десятої сфери практики. Цей новий модуль, як вже зазначалося, охоплює майже 10 тис. справ, пов'язаних із судовими розглядами у сфері захисту прав на комерційну таємницю, що очікували розгляду в федеральному суді з 2009 р. Аналітичний модуль надає дані і тенденції, пов'язані з незаконним привласненням комерційної таємниці відповідно до законодавства штатів, у справах, відкритих в окружному суді США з 2009 р. по теперішній час. Він також висвітлює рекорди відповідних адвокатів і сторін, досвід і поведінку суддів, резолюції, розміри збитку, приписи і багато іншого. Аналіз цих показників дає можливість виявити нові дані, наприклад, окружний суд США по Центральному району Каліфорнії розглядає більшість випадків справ щодо комерційної таємниці (71%), які позитивно вирішуються в ході судового розгляду, тоді як 29% справ виграють підсудні. До провідних юридичних фірм, що розглядають справи з комерційних таємниць, включають фірми, котрі спеціалізуються на трудовому праві, оскільки багато таких порушень пов'язано з колишніми співробітниками.

Коментуючи розширення платформи, Карл Харріс, президент і головний операційний директор Lex Machina, зазначив: "*Комерційна таємна аналітика була одним із найбільш затребуваних доповнень до платформи Legal Analytics, бо досі пошук і аналіз конкретних справ, пов'язаних з судовими розглядами в сфері комерційної таємниці, був надзвичайно складним, дорогим і трудомістким. Новий модуль судового розгляду з питань комерційної таємниці надає адвокатам доступ до найбільшого, найбільш повного і точного набору даних, доступному для аналізу випадків незаконного привласнення комерційної таємниці*" [27].

ВИСНОВКИ

Вартість і конкурентна перевага компанії сьогодні багато в чому залежать від інтелектуального капіталу в формі комерційної таємниці. Швидкий розвиток технологій і комп'ютеризації зробили більш легким копіювання і викрадення секретної інформації, а зростаюча мобільність службовців збільшила ризики її власників.

Економічне шпигунство залишається і буде лишатися потужним інструментом державних розвідок, призначення яких — пряме порушення законів іноземних держав в інтересах і за дорученням своєї країни. На рівні підприємств останнім часом усе частіше робиться вибір на користь конкурентної розвідки, оскільки підприємство не має повноважень державних розвідок. Тому в разі провалу операції економічного шпигунства підприємство ризикує бути притягнутим до кримінальної відповідальності, а також понести репутаційні ризики.

На думку дослідників, у багатьох випадках підприємства малого і середнього бізнесу до промислового шпигунства вдаються тому, що не навчені методам конкурентної розвідки, а часто і взагалі не знають про їх існування. У ситуації, коли необхідність виживання або підвищення конкурентоспроможності є об'єктивною, а про законні методи досягнення результату підприємство не інформовано, частина компаній встає на шлях промислового шпигунства. Тому товариства професіоналів конкурентної розвідки всього світу включають в свої завдання просвітницькі функції.

Нещодавно Європейський парламент закликав припинити використання антивірусного програмного забезпечення "Лабораторії Касперського". У резолюції ця продукція названа "шкідливою". Британський Національний центр кібербезпеки при Центрі урядового зв'язку Спо-

лученого Королівства направив в усі урядові установи приписи не використовувати це програмне забезпечення в системах, пов'язаних з національною безпекою [28]. Аналогічні приписи з'явилися у США. Таку ж рекомендацію довели до відома всього населення країни.

Рекомендується: періодично перевіряти адекватність систем охорони; строго обмежити доступ і розподіл секретних відомостей; використовувати найсучасніші охоронні технології; не залучати нових співробітників до робіт з високими ризиками; укладати з працівниками, партнерами, клієнтами ретельно розроблені угоди про охорону конфіденційної інформації як умову нового або триваючого співробітництва; ознайомлювати персонал з цілями і значущістю зобов'язань і політики в галузі охорони комерційної таємниці та попереджати тих, хто звільняється, про продовження дії зобов'язань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Демин В.А*. Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности [Электронный ресурс]. — Режим доступа: http://www.cprspb.ru/bibl/economi/2.html.
2. *Перепечко Л.Н*. Особенности развития рынка интеллектуальной собственности в мире и России / Перепечко Л.Н., Ягольницер М.А., Рахманова А.Р. // Экономика и предпринимательство. — 2017. — № 3; Ч. 1. — С. 54–64.
3. Эффективное использование интеллектуальной собственности : доклад. — Центр стратегических разработок. — М., 2017. — 57 с. [Электронный ресурс]. — Режим доступа: https://csr.ru/wp-content/uploads/2017/10/Intellektualnaya_sobstvennost_doklad.pdf.
4. Chinese Industrial Espionage: Technology Acquisition and Military Modernization / William C. Hannas, James Mulvenon, and Anna B. Puglisi. — Routledge, 2013. — 378 p.
5. *Сёмин Н.Л*. Спецслужбы и крупный бизнес США // Россия и Америка в XXI веке // Электронный научный журнал. — 2011. — №1 [Электронный ресурс]. — Режим доступа: http://www.rusus.ru/?act=read&id=230.
6. National Security Strategy of Engagement and Enlargement. The White House, GPO, February. — 1995. — P. 17.
7. *Яковлев Григорий* Шпионаж по науке // Военно-промышленный курьер № 28 (643) за 27 июля 2016 года [Электронный ресурс]. — Режим доступа: https://vpk-news.ru/articles/31576.
8. *Pooley J*. Trade secrets: the other IP right / J. Pooley // WIPO Magazine. — 2013. — № 3. — P. 2–4.
9. *Darwin R*. Protecting your business from trade secret theft / R. Darwin // Intellectual Property Magazine. — 2011. — № 4. — P. 48–49.
10. Can you keep a secret? To patent an idea, you must publish it. Many firms prefer secrecy Mar 16th 2013 / SEATTLE / From the print edition Intellectual property / Economist — World News, Politics, Economics [electronic resource]. — Access: www.economist.com/topics/intellectual-property.
11. Хакеры ежегодно выкачивают из мировой экономики полмиллиарда долларов [Электронный ресурс]. — Режим доступа: http://kp.ua/life/457249-khakery-ezhehodno-vykachyvauit-yz-myrovoi-ekonomyky-polmyllyarda-dollarov.
12. Two Convicted in Conspiracy to Steal GM Trade Secrets Sentenced to Prison [electronic resource]. — Access: http://www.fbi.gov/detroit/press-releases/2013/two-convicted-in-conspiracy-to-steal-gm-trade-secrets-sentenced-to-prison.
13. *Андрощук Г.О*. Захист комерційної таємниці в США: протидія економічному шпигунству / Г.О. Андрощук // Наука та інновації. — 2013. — Т. 9, № 1. — С. 80—95. [Електронний ресурс]. — Режим доступу: ftp://nas.gov.ua/akademperiodyka/Downloads/Archive%20SI%20Journal/SI_ukr/2013/N1/Androshchuk.pdf.
14. *Ciardullo J.-P*. Trade Secret Litigation / J.-P. Ciardullo // IP Litigator. — 2014. — March/April. — P. 30–31.
15. Jury Convicts Christian County Man for Stealing Trade Secrets from His Former Employer [electronic resource]. — Access: http://www.fbi.gov/louisville/press-releases/2014/jury-convicts-christian-county-man-forstealing-trade-secrets-from-his-former-employer.
16. Executive Recruiter David Nosal Convicted of Computer Intrusion and Trade Secret Charges [electronic resource]. — Access: http://www.fbi.gov/sanfrancisco/press-releases/2013/executive-recruiter-david-nosal-convicted-of-computer-intrusion-and-trade-secret-charges.
17. Local Chemical Engineer Indicted on Federal Charges in Trade Secrets Case [electronic resource]. — Access: http://www.fbi.gov/dallas/press-releases/2014/local-chemical-engineer-indicted-on-federal-charges-in-trade-secrets-case.
18. The Insider Threat. An introduction to detecting and deterring an insider spy // The Federal Bureau of Investigation [electronic resource]. — Access: http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.
19. How Boeing engineer spied for Chinese for 30 years... and stole secret space shuttle designs // Daily Mail, 17 July 2009 [electronic resource]. — Access: http://www.dailymail.co.uk/news/article-1200339/How-Boeing-engineer-spied-Chinese-30-years--stole-secrets-space-shuttle.html#ixzz3H9ctSOOu
20. *Bhattacharjee Yudhijit* A New Kind of Spy. How China obtains American technological secrets // The New Yorker, May 5 2014 [electronic resource]. — Access: http://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy.
21. *Singer Bill* Industrial Espionage at Dow Chemical // Forbes, 2/08/2011. [electronic resource]. — Access: http://www.forbes.com/sites/billsinger/2011/02/08/industrial-espionage-dow.
22. United States v. Wen Chyu Liu. [electronic resource]. — Access: http://caselaw.findlaw.com/us-5th-circuit/1630519.html.
23. *Passman P*. Trade secret theft: increases in global pressure, protection for companies / P. Passman // WIPR. — 2014. — Vol. 28. — № 4. — P. 43 –44.
24. США обвинили Россию в широкомасштабном экономическом кибершпионаже [Электронный ресурс]. — Режим доступа: http://goodnews.ua/technologies/ssha-obvinili-rossiyu-v-shirokomasshtabnom-ekonomicheskom-kibershpionazhe.
25. Defend Trade Secret Act of 2016 [electronic resource]. — Access: https://www.congress.gov/bill/114th-congress/senate-bill/1890/text.
26. *Brachmann Steve* Reports Shows Significant Increase in Trade Secret Litigation Since Passage of DTSA [electronic resource]. — Access: http://www.

ipwatchdog.com/2018/07/27/reports-increase-trade-secret-litigation-dtsa/id=99646.
27. IPPro Patents. Lex Machina launches trade secrets Legal Analytics [electronic resource]. — Access: http://www.ippropatents.com/ippropatentsnews/technologyarticle.php?article_id=5855.
28. Европарламент призвал отказаться от использования антивируса Касперского [Электронный ресурс]. — Режим доступа: https://vesti-ukr.com/mir/292423-evroparlament-prizval-otkazatsja-ot-ispolzovanija-antivirusa-kasperskoho?utm_source=traqli&utm_medium=email&utm_campaign=394&tqid=3OewYXk0X0QBmW72C9j9xN9x_VrPA85XpEe85Glx.

REFERENCES

1. Demin V.A. *Ekonomicheskij i promyshlennyj shpionazh: rasshirenie masshtabov i rost agressivnosti* [Economic and industrial espionage: scaling up and aggressiveness]. Available at: http://www.cprspb.ru/bibl/economi/2.html.
2. Perepechko L.N., Yagolnitser M.A., Rakhmanova A.R. (2017) *Osobennosti razvitiya rynka intellektual'noj sobstvennosti v mire i Rossii* [Features of the Intellectual Property Market Development in the World and Russia]. *Ehkonomika i predprinimatel'stvo* [Economy and Entrepreneurship], No. 3 (part 1), pp. 54–64.
3. *Effektivnoe ispol'zovanie intellektual'noj sobstvennosti : doklad. — Centr strategicheskih razrabotok* (2017) [Effective Use of Intellectual Property. Report. Center for Strategic Development]. Moscow (in Russ.), 57 p. Available at: https://csr.ru/wp-content/uploads/2017/10/Intellektualnaya_sobstvennost_doklad.pdf.
4. Chinese Industrial Espionage: Technology Acquisition and Military Modernization by William C. Hann, James Mulvenon, and Anna B. Puglis (Routledge, 2013), 378 p.
5. Soimin N.L. (2011) *Specsluzhby i krupnyj biznes SSHA* [Special services and large business of the USA]. *Rossiya i Amerika v XXI veke* [Russia and America in the XXI century electronic scientific journal], no. 1. Available at: http: //www.rusus.ru/? Act = read & id = 230.
6. National Security Strategy of Engagement and Enlargement. The White House, GPO, February 1995, p. 17.
7. Yakovlev Grigory (2016) *Shpionazh po nauke* [Espionage in science]. *Voenno-promyshlennyj kur'er* [Military industrial courier] no. 28 (643) for July 27. Available at: https://vpk-news.ru/articles/31576.
8. Pooley J. (2013) Trade secrets: the other IP right. WIPO Magazine, no. 3, pp. 2–4.
9. Darwin R. (2011) Protecting your business from trade secret theft. Intellectual Property Magazine, no. 4, pp. 48–49.
10. Can you keep a secret? It's patent an idea, you have to publish it. Many companies prefer secrecy Mar 16th 2013. SEATTLE. From the print edition Intellectual property. Economist — World News, Politics, Economics. Available at: www.economist.com/topics/intellectual-property.
11. *Hakery ezhegodno vykachivayut iz mirovoj ehkonomiki polmilliarda dollarov* [Hackers annually pump half a billion dollars from the world economy]. Available at: http://kp.ua/life/457249-khakery-ezhehodno-vykachyvauit-yz-myrovoi-ekonomyky-polmyllyarda-dollarov.
12. Two Convicted in Conspiracy to Steal GM Trade Secrets Sentenced to Prison. Available at: http://www.fbi.gov/detroit/press-releases/2013/two-convicted-in-conspiracy-to- steal-gm-trade-secrets-sentenced-to-prison.
13. Androschuk G.O. *Zakhyst komertsiinoi taiemnytsi v SShA: protydiia ekonomichnomu shpyhunstvu* [Protection of commercial secrets in the USA: counteraction to economic espionage]. *Nauka ta innovatsii* [Science and innovations]. T. 9, no. 1. pp. 80-95. Available at: ftp://nas.gov.ua/akademperiodyka/Downloads/Archive%20SI%20Journal/SI_ukr/2013/N1/Androshchuk.pdf.
14. Ciardullo J.-P. (2014) Trade Secret Litigation. IP Litigator, March/April, pp. 30-31.
15. Jury Convicts Christian County Man for Stealing Trade Secrets from His Former Employer. Available at: http://www.fbi.gov/louisville/press-releases/2014/jury-convicts-christian-county-man-forstealing-trade-secrets-from-his-former-employer.
16. Executive Recruiter David Nosal Convicted of Computer Intrusion and Trade Secret Charges. Available at: http://www.fbi.gov/sanfrancisco/press-releases/2013/executive-recruiter-david-nosal-convicted-of-computer-intrusion-and-trade-secret-charges.
17. Local Chemical Engineer Indicted for Federal Charges in Trade Secrets Case. Available at: http://www.fbi.gov/dallas/press-releases/2014/local-chemical-engineer-indicted-on-federal-charges-in-trade-secrets-case.
18. The Insider Threat. An introduction to detecting and deterring an insider spy. The Federal Bureau of Investigation. Available at: http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.
19. How Boeing engineer spied for Chinese for 30 years... and stole secret space shuttle designs. Daily Mail, 17 July 2009. Available at: http://www.dailymail.co.uk/news/article-1200339/How-Boeing-engineer-spied-Chinese-30-years--stole-secrets-space-shuttle.html#ixzz3H9ctSOOu.
20. Bhattacharjee Yudhijit (2014) A New Kind of Spy. How China obtains American technological secrets. The New Yorker, May 5. Available at: http://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy.
21. Singer Bill. Industrial Espionage at Dow Chemical. Forbes, 08/02/2011. Available at: http://www.forbes.com/sites/billsinger/2011/02/08/industrial-espionage-dow.
22. United States v. Wen Chyu Liu. Available at: http://caselaw.findlaw.com/us-5th-circuit/1630519.html.
23. Passman P. (2014) Trade secret theft: increases in global pressure, protection for companies. WIPR, Vol. 28, no. 4, pp. 43-44.
24. *SSHA obvinili Rossiyu v shirokomasshtabnom ehkonomicheskom kibershpionazhe* [US accused Russia of large-scale economic cyber-espionage]. Available at: http://goodnews.ua/technologies/ssha-obvinili-rossiyu-v-shirokomasshtabnom-ekonomicheskom-kibershpionazhe.
25. Defend Trade Secret Act of 2016. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/1890/text.
26. Brachmann Steve. Reports Shows Significant Increase in Trade Litigation Since the Passage of DTSA. Available at: http://www.ipwatchdog.com/2018/07/27/reports-increase-trade-secret-litigation -dtsa/id=99646.
27. IPPro Patents. Lex Machina launches business secrets Legal Analytics. Available at: http://www.

ippropatents.com/ippropatentsnews/technologyarticle.php?article_id=5855.
28. *Evroparlament prizval otkazat'sya ot ispol'zovaniya antivirusa Kasperskogo* [The European Parliament called for refusal to use Kaspersky Anti-Virus]. Available at: https://vesti-ukr.com/mir/292423-evroparlament-prizval-otkazatsja-ot-ispolzovanija-antivirusa-kasperskoho?utm_source=traqli&utm_medium=email&utm_campaign=394&tqid=3OewYXk0X0QBmW72C9j9xN9x_VrPA85XpEe85Glx.

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

ECONOMIC ESPIONAGE: GROWTH AND AGGRESSIVITY (PART II)

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 II)

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.*

ІНФОРМАЦІЯ ПРО АВТОРА

Андрощук Геннадій Олександрович — канд. экон. наук, доцент, головний науковий співробітник, завідувач лабораторії правового забезпечення розвитку науки і технологій, НДІ інтелектуальної власності НАПрН України, вул. Казиміра Малевича, 11, корп. 4, м. Київ, Україна, 03680; +38 (044) 200-08-76; genandro1@gmail.com

INFORMATION ABOUT THE AUTHOR

Androshchuk H.O. — PhD in Economics, Associate Professor, Chief Senior Researcher, Head of Laboratory of Legal Support of Science and Technology Research, Institute of the National Academy of Legal Sciences of Ukraine Intellectual Property, 11, Kazymira Malevycha Str., Bldg. 4, Kyiv, Ukraine, 03680; +38 (044) 200-08-76; genandro1@gmail.com

ИНФОРМАЦИЯ ОБ АВТОРЕ

Андрощук Г.А. — канд. экон. наук, доцент, главный научный сотрудник, заведующий лаборатории правового обеспечення развития науки и технологий, НИИ интеллектуальной собственности НАПрН Украины, ул. Казимира Малевича, 11, корп. 4, г. Киев, Украина, 03680, МСП; +38 (044) 200-08-76; genandro1@gmail.com