http://doi.org/10.35668/2520-6524-2022-3-02
УДК 330.47:004

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

КОМЕРЦІЙНА ТАЄМНИЦЯ ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ: ПРАКТИКА КИТАЮ ТА США (Частина 2)

Резюме. *У статті досліджено глобальний економічний та інноваційний вплив комерційної таємниці. Комерційні таємниці мають широке охоплення та підтримують інноваційну екосистему, захищаючи технологічні, продуктові, ринкові та організаційні інновації, а також забезпечуючи ключове доповнення та підтримку іншої інтелектуальної власності (ІВ). Показано, що незаконне присвоєння або крадіжка комерційної таємниці з країн ОЕСР становить 1–3 % ВВП. Вартість крадіжок комерційної таємниці досягла 1,7 трлн дол. США на рік. На прикладі економік Китаю і США показано зростання важливості нематеріальних активів, комерційної таємниці та посилення загроз їх викрадення. У США понад 80 % усіх справ з економічного шпигунства та 60 % справ щодо комерційної таємниці пов'язані з Китаєм. Враховуючи їхній негативний вплив на національну безпеку, США застосовують нові законодавчі механізми захисту ІВ і комерційної таємниці. Проаналізовано виклики та ризики, що пов'язані зі співпрацею України з Китаєм. Надано рекомендації щодо їх мінімізації та протидії загрозам.*

Ключові слова: *інтелектуальна власність, інновації, комерційна таємниця, кібербезпека, національна безпека, економічне шпигунство.*

Із судової практики розгляду спорів щодо захисту комерційної таємниці в Китаї [1; 2]. Цікавою є справа, що демонструє використання доказів, отриманих у судовому процесі за кордоном. Справа SI Group v. Sino Legend Chemical (2013) стосувалася комерційної таємниці американського виробника. Китайська фірма виготовляла аналогічні продукти. У 2010 р. SI Group звинуватила в Шанхайському проміжному суді N 2 Sino Legend Chemical, стверджуючи, що вона незаконно привласнила її комерційну таємницю, що стосується технології. SI Group заявила, що конкурентна продукція Sino Legend Chemical була випущена незабаром після того, як колишній заводський менеджер SI Group почав працювати в Sino Legend Chemical головним менеджером. Проте SI Group не обмежилася судовою справою в Китаї. У травні 2012 р. SI Group звернулася до Комісії з міжнародної торгівлі США (International Trade Commission; далі — ITC) з приводу імпорту продукції Sino Legend Chemical у США. У червні 2013 р. Шанхайський проміжний суд № 2 припинив справу на підставі того, що технологічний процес, який застосовується Sino Legend Chemical, відрізняється від процесу SI Group, що містить комерційну таємницю. Рішення в жовтні 2013 р. було підтримане Шанхайським вищим народним судом. Однак у січні 2014 р. ITC обґрунтувала те, що Sino Legend Chemical незаконно привласнила комерційну таємницю американської компанії та наклала заборону на імпорт до США певних продуктів цієї компанії. Рішення ITC стало підставою для скарги Sino Legend Chemical до Федерального апеляційного суду. Варто зазначити, що для успіху в справі має значення стратегія використання паралельних процедур у закордонних судових справах. Юрисдикції загального права мають тенденцію вимагати ширших виступів адвокатів та показів свідків. Документи, представлені в судовому процесі США, потенційно можуть бути використані для сприяння в китайському судовому процесі після того, як стануть відкритими. Правовласники мають також розглянути можливість дій, що можуть бути здійснені в інших країнах: наприклад, отримання записів від митниці для доказу обсягу експорту. У згаданій справі Шанхайський суд рекомендував SI Group відкласти розгляд справи в китайському суді, можливо, у спробі очікувати на рішення в США. Особливість китайської правової системи полягає у використанні висновків судової експертизи в технічних питаннях, що становлять предмет спору. Адже більшість китайських суддів не мають науково-технічної освіти й зазнають труднощів через обмежений

час для розуміння складних технічних питань, що підлягають вирішенню в суді. Якщо до судової суперечки, що пов'язана з комерційною таємницею, залучається технічне ноу-хау, судді (або Народне бюро безпеки, або Народна прокуратура — Public Security Bureau (далі — PSB), People's Procuratorate) звертатимуться до органу судової експертизи для аналізу того, чи відома технічна інформація громадськості чи інформація, використана відповідачем, аналогічна інкримінованій комерційній таємниці. Проте експертиза може бути різною. Окрім того, процедурні гарантії залежать від того, як визначено обсяг експертизи та яким чином його було передано. Тому сторони спору мають передавати свої технічні висновки та активно співпрацювати із закладом судової експертизи, коли той готує звіт. Так, у справі Hengxiang v. Zhang, Xu and Shen (2009 р.) під час розгляду було зроблено чотири звіти експертизи з суперечливими висновками від трьох різних юридичних експертних установ. Перший звіт було подано Народним бюро безпеки після отримання справи для кримінального розслідування. У висновку експертизи йшлося про те, що комерційна таємниця невідома громадськості, і зроблено її на основі результатів, отриманих під час дослідження новизни, здійсненому у Відомстві з інтелектуальної власності (State Intellectual Property Office (SIPO)). Потім PSB передало справу до Народної прокуратури, а відповідач представив публікацію як доказ того, що інформація, яка стосується комерційної таємниці, була раніше розкрита. Після цього аналогічний експертний орган змінив висновок, що ґрунтується на публікації. Коли справа перейшла в цивільний процес, суд вчинив дії вже з іншим експертним звітом. Другий орган судової експертизи встановив, що комерційна таємниця була розкрита в зазначеній публікації. Під час перехресної перевірки позивач спростував висновки цього звіту, аргументуючи, що публікація розкрила лише експериментальні дані, тоді як комерційна таємниця належить до даних виробництва. Багато таких параметрів, як температура реакції, процедура очищення, тиск, що використовуються для промислового очищення продукту (або при його виробництві), не були розкриті в публікації. У результаті четвертого експертного звіту від третього органу експертизи містився висновок, що комерційна таємниця була невідома громадськості. Щоб уникнути подібних ситуацій, сторонам важливо готувати власні технічні звіти в обсязі питань експертизи та заздалегідь надавати матеріали чи дані, що можуть допомогти експертним установам зробити правильні науково обґрунтовані висновки. Сторони також мають уважно аналізувати обсяг питань експертизи, щоб бути впевненими, що туди входять лише технічні, а не правові питання, і що обраний експерт, який має досвід у відповідній галузі техніки.

Іншою проблемою є те, що в Китаї в судових справах, що стосуються питань охорони ІВ, сума збитків, які нараховуються, у середньому низька. Частково це викликано труднощами в приведенні доказу, що стосується втрат позивача чи прибутку відповідача, за відсутності процедури розкриття та ефективної системи зберігання документів. Водночас існує низка справ, у яких було визначено суттєву шкоду: Xian Intermediate Court визначив збиток у 2,8 млн дол. США у цивільній справі Xian Heavy Machinery v. CCTEC (2006 р.) та Zuhai Intermediate Court наклав кримінальний штраф у 5,94 млн дол. США у справі People's Procuratorate v. Jiangxi Yibo (2013). У справі Xian Heavy Machinery колишній найманий працівник скопіював певні конструкторські креслення машин для лиття сталі, а потім перейшов на роботу до конкурента. Пізніше позивач програв два тендери цій конкурентній компанії. Після виявлення порушення позивач визначив прибуток відповідача на основі розрахунку збитків з урахуванням двох відповідних контрактів на конструювання та виробництво, що дорівнювало 23,82 млн дол. США. Оскільки відповідач відмовився визнавати ці фінансові дані, позивач отримав експертний висновок від китайської Асоціації важкого машинобудування, щоб показати, що середній рівень прибутку в галузі конструювання та виробництва машини для лиття сталі становить 12 % від загального доходу. Суд призначив суму збитків у 12 % від 23,82 млн дол. США, що становило 2,86 млн дол. США.

Справа Jianxi Yibo — кримінальна судова справа 2013 р., що стосується крадіжки комерційної таємниці даних про ціни. Декілька колишніх найманих працівників компанії Zhuhai Saina Printing Technology організували конкурентний бізнес, заснувавши дві нові компанії Jiangxi Yibo та Zhongshan Wode. Вони мали можливість продавати продукцію за нижчими цінами в порівнянні з Zhuhai Saina під час укладання угод, використовуючи конфіденційну цінову структуру, яку отримали на попередній роботі. Після встановлення відповідальності Guangzhou Province Zhuhai Intermediate Court (Проміжний суд Чжухай провінції Гуанчжоу) наклав на обидві компанії відповідачів кримінальний штраф у розмірі 5,94 млн дол. США. Розмір штрафу був розрахований на основі перевірки фінансового прибутку двох компаній і звітів митниці, що показують продаж ідентичних продуктів одинадцяти

колишнім покупцям компанії Zhuhai Saina. Високий рівень кримінального штрафу в справі Jianxi Yibo Вищий народний суд (Supreme People's Court) розглядав як ілюстрацію вирішення спору щодо злочину у сфері ІВ.

Справа про комерційну таємницю виробництва ваніліну 2021 р. (увійшла до десяти найкращих справ китайського народного суду) [3]. Верховний народний суд Китаю 26 лютого 2021 р. оголосив вирок щодо Wanglong Group Co., Ltd., який присудив Jiaxing Zhonghua Chemical Co., Ltd. та Shanghai Xinchen New Technology Co., Ltd. компенсацію 159 млн юанів (~ 24,5 млн дол. США) у справі про комерційну таємницю, що стосується виробництва ваніліну — харчового ароматизатора. Це був найбільший розмір компенсації за крадіжку комерційної таємниці, що присуджено в Китаї. Позивачі в цій справі, Чжунхуа і Сіньчень, спільно розробили новий процес виробництва ваніліну та захистили його як комерційну таємницю. До крадіжки комерційної таємниці Zhonghua була найбільшим у світі виробником ваніліну, займаючи приблизно 60 % світового ринку. У 2010 р. колишній співробітник Zhonghua та відповідач Фу Сянген отримав винагороду від відповідача Wanglong Group, він розкрив комерційну таємницю виробництва ваніліну керівнику Wanglong Group та Ningbo Wanglong Technology Co., Ltd. З червня 2011 р. Wanglong почала виробляти ванілін, ставши за короткий час третім за величиною виробником у світі. Фактичний річний обсяг виробництва ваніліну становить щонайменше 2000 т (10 % частки світового ринку). Ванілінові продукти, вироблені відповідачами з порушенням комерційної таємниці, що фігурує в справі, продаються на основних ринках світу і конкурують з Zhonghua за клієнтів та ринки. Оскільки Wanglong незаконно отримала технічні секрети, що пов'язані з цією справою, у них не було значних витрат на дослідження та розробки, і вони могли продавати ванілінові продукти за нижчими цінами (демпінг), що вплинуло на початкові міжнародні та внутрішні ринки Zhonghua. У результаті, частка Zhonghua на світовому ринку ваніліну впала з 60 % до 50 %. У 2018 р. Zhonghua та Xinchen подали позов до Вищого народного суду Чжецзяна, стверджуючи, що Wanglong Group Company, Wanglong Technology Company, Xifu Lion King Dragon Company, Fu Xianggen та Wang Guojun порушили комерційну таємницю виробництва ваніліну. Позивачі просили суд зобов'язати відповідача припинити порушення та компенсувати 502 млн юанів. Суд першої інстанції встановив, що Wanglong Group Company, Wanglong Technology Company, Xifu Lion Wanglong Company та Fu Xianggen викрали комерційну таємницю, що пов'язана зі справою, і наказав їм припинити порушення та компенсувати 3 млн юанів за економічні збитки та 500 тисяч юанів — витрати, пов'язані з припиненням порушення (судові витрати). За винятком підсудного Ван Гоцзюня, усі сторони в цій справі відмовилися ухвалити рішення суду першої інстанції та звернулися до Верховного народного суду. У другому випадку Zhonghua та Xinchen зменшили свої вимоги щодо компенсації до 177 млн юанів (включаючи розумні витрати).

Суд з ІВ Верховного народного суду ухвалив у другій інстанції, що вищезгадані компанії порушили всі комерційні таємниці, що пов'язані з цією справою. Згідно з даними про економічні втрати, надані правовласником, беручи до уваги серйозні обставини порушення, велику комерційну цінність відповідних комерційних секретів і відмову порушників (таких, як Wanglong) припинити використання ними вкрадених комерційних секретів відповідно до судової заборони, рішення суду першої інстанції було скасовано, а рішення змінено. Тепер порушники мають спільно відшкодувати правовласнику комерційної таємниці 159 млн юанів (зокрема 3,49 млн юанів на розумні витрати на захист прав). Причому сума відшкодування збитків, що заявлена правовласниками, була розрахована лише до кінця 2017 р., а закон на той момент не передбачав штрафних санкцій. Отже, штрафні санкції в цьому випадку не застосовні. Проте Верховний народний суд зазначив правовласникам, що кожен відповідач продовжував правопорушення після 2018 р. і позивачі можуть вимагати додаткового захисту відповідно до закону (49 млн юанів на розумні витрати на захист прав). Окрім того, оскільки порушення комерційної таємниці, що пов'язане зі справою, має погані обставини та серйозні наслідки та може бути запідозрене в скоєнні кримінальних злочинів, Верховний народний суд передав відповідні підозрювані кримінальні докази до відділу громадської безпеки для судового переслідування.

Роль ІВ і цифрової інфраструктури обороту прав ІВ стає ключовим чинником, що визначатиме зростання національних економік і, як результат — вплив країни у світі. Передумови для цього створені розвитком глобальних цифрових мереж, понад 70 % трафіку яких становить рух об'єктів ІВ [4].

Зростання важливості нематеріальних активів, комерційної таємниці та посилення загроз їх викрадення. Ці тенденції підтверджують результати останніх міжнародних досліджень. The Economist Intelligence Unit 9 червня 2021 р. опублікувала результати дослідження

“Відкрити секрети? Охоронна вартість нематеріальної економіки” (Open secrets? Guarding value in the intangible economy). У звіті наголошено, що вартість крадіжок комерційної таємниці досягла 1,7 трлн дол. США на рік і що керівники корпорацій очікують, що ризик розкрадання комерційної таємниці ще більше зросте в наступні п’ять років. Дослідження базується на аналізі відповідей 314 керівників вищої ланки компаній із Китаю, Франції, Німеччини, Сінгапуру, Великої Британії та США в шести секторах економіки: споживчі товари та роздрібна торгівля; фінанси; енергія та природні ресурси. Згідно з результатами дослідження, 45 % керівників не володіють основами комерційної таємниці, 55 % респондентів підтвердили, що в них був обмежений цифровий і фізичний доступ до конфіденційної інформації. Опитані визначили три найбільш цінні типи ІВ нині: бази даних клієнтів (42 %), технології продуктів (40 %) та інформація про дослідження і розробки (23 %). Через зростаючу вартість таких нематеріальних активів керівники вищої ланки розглядають свої найсерйозніші загрози як слабкі місця в кібербезпеці (49 %) і витоки інформації про співробітників (48 %). У звіті зазначено, що такі загрози посилюються зміною культури праці, спричиненої пандемією. Згідно з опитуванням, яке було проведено міжнародною юридичною фірмою Baker McKenzie, варто зазначити, що кожна п’ята компанія (20 %) знає або вважає, що їхні комерційні секрети були викрадені, а головними винуватцями є колишні співробітники [5].

Головне для Китаю — захистити свої інновації, наголос передбачено зробити на охороні ІВ. Так, у третьому номері журналу “Цюші” за 2021 р. опубліковано статтю голови КНР Сі Цзіньпіна “Всебічно посилити роботу із захисту прав інтелектуальної власності, надати інноваціям життєві сили, стимулювати побудову нової моделі розвитку”. У вступній частині статті сказано: “Інновації — це рушійна сила розвитку, захист прав інтелектуальної власності — це захист інновацій. Захист прав інтелектуальної власності безпосередньо стосується національної безпеки. Лише за умови суворого захисту прав інтелектуальної власності можливий ефективний захист власних досліджень і розробок у галузі критично важливих ключових технологій, запобігання та нейтралізації величезних ризиків” [6].

Глобальний економічний та інноваційний вплив комерційної таємниці. Комерційні таємниці є глобальними правами, хоча їх юридична конструкція залежить від юрисдикції. Вони включені до ст. 39 Угоди про торговельні аспекти прав інтелектуальної власності (ТРІПС) і тому є мінімальним стандартом правозастосування в 164 державах — членах Світової організації торгівлі (СОТ). Комерційні таємниці – це гнучкий інноваційний інструмент, що використовується в різних юрисдикціях, секторах економіки та типах фірм. В аналітичному звіті Відомства інтелектуальної власності Великої Британії “Економічний та інноваційний вплив комерційної таємниці” (Economic and innovation impacts of trade secrets), опублікованому 19 квітня 2021 р. узагальнено загальнодоступні економічні дослідження з питань комерційної таємниці, а також висвітлюються ключові аспекти інновацій [7]. Розглянемо його основні положення та висновки. Комерційна таємниця — це знання, які є секретними, цінними і належним чином охороняються. Згідно з галузевими оцінками, незаконне присвоєння чи крадіжка комерційної таємниці коштує 1–3 % ВВП у розвинених країнах. Комерційні таємниці, що закріплені в Угоді ТРІПС СОТ, стають дедалі важливішою інноваційною політикою. Комерційні таємниці є кращою стратегією для інноваційних фірм. Так, 70 % фірм, які розробляють інноваційні продукти та процеси, використовують комерційну таємницю для захисту цих інновацій. Комерційні таємниці особливо важливі для фірм, що працюють у сфері НДДКР, технологій, а також у виробничому та невиробничому секторах. Великі фірми покладаються на комерційну таємницю більше, ніж дрібні. Комерційні таємниці можуть бути дуже цінними активами фірми, хоча більшість комерційних секретів такими є. Комерційні таємниці мають широке охоплення та підтримують інноваційну екосистему, захищаючи технологічні, продуктові, ринкові й організаційні інновації, а також забезпечуючи ключове доповнення та підтримку іншої ІВ. Фірми вибирають комерційну таємницю, щоб зберегти конкурентну перевагу, уникаючи розкриття, пов’язаного з іншими видами ІВ. Проте комерційна таємниця вразлива для зворотного проєктування, незаконного присвоєння чи крадіжки. Кіберкрадіжки та економічне шпигунство викликають дедалі більшу занепокоєність. Комерційна таємниця часто є дешевшою альтернативою іншим правам ІВ, хоча й захищена відносно слабше. Комерційні таємниці є заміною чи доповненням до патентів. Дослідження, що було проведено за останні два десятиліття, показали, що комерційна таємниця є кращим механізмом захисту. Наприклад, у дослідженні виробничих фірм США, присвяченому їх технологічним і продуктовим інноваціям, виявили, що для обох типів інновацій перевага надається як секретності, так і часу виходу на ринок, а не патентам. Патенти та інші офіційні права ІВ можуть бути менш важливими, аніж передбачалося спочатку. Патенти є кращими

для інноваційних продуктів, а комерційні секрети — для технологічних інновацій. Більшість комерційних таємниць стосується таких непатентованих інновацій, як маркетингові та організаційні. З огляду на це, комерційна таємниця відіграє дедалі більш важливу роль у практичному та політичному інноваційному середовищі для фірм та економіки. Комерційні таємниці підтримують інновації, але також обмежують потоки знань і мобільність робочої сили. Більш жорстка політика приносить користь власникам комерційної таємниці та заохочує інвестиції в НДДКР, але знижує майбутні інновації та створює бар'єри для входу. Необхідно знайти баланс між комерційною таємницею, яка заохочує інновації, і комерційною таємницею, яка перешкоджає інноваціям.

Загрози національній безпеці США з боку Китаю. Китай має низку національних планів, які включають Made in China 2025 та їх 14-й п'ятирічний план, у якому перераховано близько 10 технологій, у яких вони прагнуть домінувати. До них належать технології, від яких залежать галузі та генератори багатства майбутнього: штучний інтелект, квантові інформаційні системи, біотехнології, напівпровідники та автономні системи. Китайський уряд використовує всі інструменти національної влади (від шпигунства до легальних придбань та спільних підприємств) для придбання конкретних технологій, щоб вони могли бути світовими лідерами в цих технологіях. Китай розглядає національну безпеку й економічну безпеку як одне й те саме, зазначає Анна Пуглісі — директор біотехнологічних програм і старший науковий співробітник Центру безпеки та нових технологій Джорджтаунського університету. "Китай дійсно дивиться на розвиток науки і техніки як на нульову суму. Це справді рушійна сила багатьох заходів, які ми бачимо", — вказала вона.

У доповіді Національної комісії з розвитку та реформ від 2017 р. А. Пуглісі наголосила: "[президент Китаю Сі Цзіньпін] описує науку та техніку як національну зброю, що якщо Китай хоче бути сильним, він повинен мати потужну науку та технології" [8]. Варто зауважити, що Сі Цзіньпін повторив аналогічні формулювання у нещодавній промові, де він назвав науку та техніку *"гострою зброєю для розвитку" і сказав, що "якщо наука та техніка сильні, то і країна буде сильною".*

Коли справа доходить до чутливих технологій, відносини між китайськими фірмами та їх урядом відрізняються від відносин у таких країнах, як США, Корея, Японія чи Європа. Китайські фірми можуть попросити спеціалізованих "науково-технічних дипломатів" допомогти їм зв'язатися з іноземними компаніями, які мають потрібні їм технології. Співробітники розвідки кажуть, що атаки хакерів, як і кібератаки First Solar, були потужним інструментом, який уряд Китаю використовував для отримання технологій і економічних переваг з іноземних компаній.

У 2015 р. тодішній президент США Барак Обама, на боці якого був Сі Цзіньпін, оголосив про угоду між двома лідерами про те, що жодна з країн не *"проводитиме або свідомо підтримуватиме кіберкрадіжку інтелектуальної власності"* для отримання комерційної вигоди. Китай не виконав це зобов'язання, і в нещодавній доповіді CrowdStrike назвав його "*одним із найплодючіших спонсорованих державою кібердекторів на планеті".*

Дослідження свідчать, що крадіжка комерційної таємниці з країн ОЕСР становить від 1 % до 3 % ВВП. І незалежно від того, як ви це вимірюєте, і типу крадіжки ІВ від крадіжки комерційної таємниці, підробки, копіювання програмного забезпечення, Китай завдає від 60 % до 80 % збитків [8].

Зокрема 12 серпня 2020 р. голова відділу національної безпеки (NSD) Міністерства юстиції (DOJ) Дж. Демерс публічно доповів про загрози національній безпеці з боку Китаю. Він зосередився на зусиллях Китаю з крадіжки американської ІВ у американських компаній та інших установ, а також на тому, як "китайська ініціатива" Міністерства юстиції прагне протистояти цій загрозі.

Сучасне змінене середовище загроз. Так, Дж. Демерс підкреслив, що Китай несе основну відповідальність за крадіжку ІВ США і що внутрішня загроза стає дедалі серйознішою проблемою: понад 80 % усіх справ, обвинувачених в економічному шпигунстві (тобто справ, що пов'язані з крадіжкою комерційної таємниці китайським урядом або від його імені, його інструментів чи агентів), пов'язані з Китаєм, а 60 % усіх справ, що пов'язані з комерційною таємницею, пов'язані з Китаєм. [9]. Типовий метод дій Китаю полягає в тому, щоб вкрасти американську ІВ, відтворити її, замінити американську компанію, яка створила цю ІВ на внутрішньому ринку Китаю, а потім витіснити США на світовому ринку. Останніми роками спецслужби Китаю стали більш активні в крадіжці ІВ: з 2014 р. відповідальність за крадіжку американської ІВ перемістилася з кібероперацій, які проводить Народно-визвольна армія (НДАК), на операції, зорієнтовані на інсайдерів, що проводять Міністерство державної безпеки (MSS) і агентство розвідки та безпеки Китаю, яке відповідає за контррозвідку, зовнішню розвідку та політичну безпеку. MSS успішно розвиває

відносини зі співробітниками американських компаній, які мають доступ до ІВ, і багато судових переслідувань Міністерства юстиції у зв'язку з порушенням комерційної таємниці наразі є наслідком внутрішніх загроз.

Китайська програма "Тисяча талантів" є засобом придбання американської ІВ. Особи, які подають заявку на участь у програмі, мають продемонструвати, що вони привезуть ІВ до Китаю [10]. Масштаби китайських операцій із крадіжки американської ІВ також впливають на стратегію уряду США щодо протидії цій загрозі: Міністерство юстиції збільшило кількість прокурорів у відділі контррозвідки та експортного контролю РНБ (що відповідає за судове переслідування за економічне шпигунство) для роботи в справах, пов'язаних з Китаєм, а також Федеральне бюро розслідувань (ФБР) збільшило свої виділені ресурси. Деструктивна діяльність уряду також передбачає посилену "цільову" перевірку китайських студентів, які від'їжджають, в аеропортах США, де їх можуть розпитати про сфери навчання і про те, з якими освітніми закладами вони пов'язані в Китаї.

Протидія внутрішній загрозі **[9]**. З огляду на зміну тактики Китаю, американські компанії мають активно захищати свою цінну ІВ від внутрішніх загроз, а також широко мислити під час розгляду потенційної сукупності загроз. До інсайдерів належать не лише співробітники, а й підрядники, ділові партнери і, можливо, особи в їхньому ланцюжку поставок — по суті, усі, хто має авторизований доступ до їхніх внутрішніх систем і ресурсів. Тому компанії повинні менше зосереджуватися, наприклад, на посаді конкретної людини, а більше концентруватися на безлічі людей, які мають доступ до інформації, що найбільше хвилює компанію. Увагу потрібно зосереджувати на виявленні "зловмисних інсайдерів" — тих, хто не лише санкціонував доступ, а й навмисне перевищує його чи зловживає їм у мерзенних цілях. Моніторинг мережі відповідно до застосовних федеральних законів і законів штатів необхідний для виявлення підозрілої внутрішньої поведінки, і навіть зовнішніх вторгнень. Водночас технічних інструментів замало для реалізації надійної програми зниження внутрішніх загроз. Важливими є збір, судження та аналіз людської інформації, зосереджені на людській поведінці. ФБР визначило декілька поведінкових ознак того, що співробітник може вкрасти ІВ компанії, зокрема: без необхідності чи дозволу бере додому пропрієтарні матеріали у вигляді документів, флеш-накопичувачів або інших цифрових носіїв; прояв інтересу до питань, що виходять за рамки обов'язків працівника, особливо до тих, які становлять інтерес для іноземних організацій або ділових конкурентів; робота в позаурочний час без дозволу та віддалений доступ до комп'ютерної мережі в неурочний час; незрозуміле багатство; незареєстровані закордонні контакти; короткі поїздки до інших країн із незрозумілих чи дивних причин. З'явилося декілька провідних корпоративних практик виявлення внутрішніх загроз і реагування на них. Компаніям варто створити та впровадити програму запобігання інсайдерським загрозам, що спирається на підтримку та виділення ресурсів із боку ради директорів і виконавчого керівництва компанії, а також на міжорганізаційну участь таких компонентів, як кадри, внутрішній аудит і порада юридичного відділу. Компанії мають переконатися, що вони мають план реагування на інциденти, у якому беруть участь усі зацікавлені сторони компанії, і переконатися, що вони відпрацювали його. Так, компанії мають створити спеціальну групу боротьби з внутрішніми загрозами для реалізації цієї програми. У процесі реалізації програми компаніям варто: розробити перелік найбільш цінної ІВ, вказавши, хто має до неї доступ і за якими напрямами; розробити критерії аномальної поведінки, щоб сфокусувати операції програми боротьби з внутрішніми загрозами; розробити та проводити регулярні програми навчання та підвищення обізнаності для всього персоналу; використовувати такі технічні інструменти, як програмне забезпечення для моніторингу мережі, засоби управління ідентифікацією та доступом, а також інструменти запобігання втраті даних, щоб контролювати поведінку працівників у мережах компанії. З огляду на це, компаніям варто розглянути можливість застосування штучного інтелекту для виявлення чи попередження ризиків внутрішніх загроз. Технологічні рішення мають супроводжуватися людським аналізом на основі інтелекту для інтерпретації технічних даних і винесення судження під час виявлення та оцінки аномальної поведінки. Проте будь-яке поєднання інструментів моніторингу й аналізу, які використовують компанії для виявлення ризиків, має передбачати їх об'єктивне застосування на основі фактичних даних.

Нові законодавчі механізми захисту ІВ і комерційної таємниці в США. Крадіжка ІВ, особливо комерційної таємниці, залишається суттєвою загрозою для розвинених галузей промисловості США, її глобальної конкурентоспроможності та національної безпеки. Це є основним аспектом у торговій суперечці США з Китаєм, з урахуванням тих зусиль, які держава докладає, щоб вкрасти якнайбільше американських ноу-хау. ***Законопроєкт про захист***

американських інновацій. У червні 2020 р. двопартійна група сенаторів оприлюднила законопроєкт, що спрямований на зупинення крадіжки ІВ США іноземними урядами, з акцентом на Китай [11]. Законопроєкт, що має назву "Закон про захист американських інновацій" (Safeguarding American Innovation Act), містить такі положення:

- карати осіб, які навмисно не розкривають іноземну підтримку в заявках на федеральні гранти, з покаранням у вигляді штрафів і позбавлення волі на строк не більше п'яти років або обох і п'ятирічної заборони на отримання федерального гранту;
- зміцнити програму для студентів і обмінних відвідувачів, вимагаючи від спонсорів програми обміну державного департаменту захисту від несанкціонованого доступу до чутливих технологій і повідомляти державі, чи буде відвідувач обміну мати доступ до чутливих технологій;
- посилити повноваження Державного департаменту щодо відмови у видачі віз певним іноземним громадянам, які бажають отримати доступ до чутливих технологій, коли це суперечить інтересам США в галузі національної безпеки й економічної безпеки США;
- надати наказ про стандартизований процес надання грантів урядом США, уповноваживши Управління керування бюджетом співпрацювати з федеральними агентствами, які надають гранти, з метою стандартизації процесу подачі заявок на гранти;
- ділитися інформацією про грантоотримувачів;
- створити в США урядову базу даних федеральних грантоотримувачів;
- знизити поріг звітності для шкіл і університетів США, які отримують іноземні подарунки, з 250 тис. до 50 тис. дол. США;
- наділити Департамент освіти повноваженнями карати школи, які не в змозі належним чином відзвітувати.

Закон SECRETS. Замість нових законів і правил США покладалися на тарифи в непрямих спробах переконати Китай приборкати цю незаконну практику. Нині Конгрес і адміністрація Байдена завершують роботу над законопроєктом, який принесе користь американським підприємствам і працівникам, борючись із китайською загрозою для промисловості США — Закон SECRETS (S.2067 — SECRETS Act of 2021), який було презентовано влітку 2021 р. сенаторами Джоном Корніном (R-TX), Крісом Кунсом (D-DE) та Тоддом Янгом (R-IN) [12].

***Китайська небезпека* [12].** Крадіжка комерційної таємниці та іншої ІВ, що спонсорується державою, є ключовою частиною стратегії промислового розвитку Китаю. Хижацькі зусилля Китаю демонструють повну зневагу до законів США та міжнародних норм у галузі ІВ, а також до торговельних зобов'язань, які він узяв на себе перед іншими країнами — членами СОТ. Для Китаю все буде, якщо він просуватиме всеосяжну мету країни – допомогти китайським фірмам наздогнати рівень продуктів і технології конкурентів США. Хоча китайські компанії регулярно користуються захистом ІВ у США та інших країнах світу, але американським компаніям регулярно відмовляють або позбавляють таких прав у Китаї. Щойно комерційну таємницю вкрадено, іноземні організації, що спонсоруються державою, можуть пожинати плоди зусиль американських працівників і підривати американський бізнес. Це призводить до скорочення інновацій, втрати робочих місць, а також економічних і конкурентних переваг для промисловості США. Фірми, які постраждали від крадіжки ІВ, стикаються з втратою експортних і ліцензійних ринків та недобросовісною конкуренцією в США і на світових ринках. Згідно з оцінками дослідження, що було проведене Комісією з крадіжки американської інтелектуальної власності, збитки від крадіжки ІВ у Китаї обходиться США у 225–600 млрд дол. США на рік. Опитування корпорацій 2019 р. у Глобальній раді фінансових директорів CNBC показало, що приблизно 1 з 5 північноамериканських корпорацій стали жертвами крадіжки ІВ у китайських компаній. Крадіжка ІВ Китаєм зачіпає низку американських фірм. Варто зауважити, що Китай націлився не лише на інновації та НДДКР. Він шукає інформацію про витрати та ціни, внутрішні стратегічні документи, масові особисті дані — усе, що може дати китайським фірмам конкурентну перевагу. Розслідування USTR дій, політики та практики Китаю, що пов'язані з передачею технологій, ІВ та інноваціями, має всі докази, необхідні політикам для вжиття більш рішучих заходів.

***Інструменти SECRETS* [12].** Закон SECRETS створює новий потужний нетарифний захід для стримування крадіжки ІВ, що підтримується державою, шляхом розумного об'єднання зусиль правоохоронних, розвідувальних і торгових апаратів уряду США. Цей механізм швидкого реагування не дозволяє компаніям, які експортують товари до США, отримувати прибуток від крадіжки американської ІВ, що підтримується державою. Оскільки загальна тарифна політика може зашкодити економіці, то цей підхід є орієнтованим на конкретний випадок. Закон забезпечить швидкі й ефективні засоби запобігання фізичному чи цифровому проникненню на ринок

США фізичних або цифрових продуктів, виготовлених із використанням вкраденої комерційної таємниці. Він виконує давню рекомендацію Комісії з крадіжки американської ІВ щодо створення механізму швидкого реагування на крадіжку комерційної таємниці іноземним урядом. Законодавство створює новий цивільний позов ex parte для фірм, коли вони вважають, що стали жертвою крадіжки комерційної таємниці іноземною державою. Закон робить це шляхом створення нового розділу Закону про тарифи 1930 р. *"для забезпечення процедур виключення національної безпеки зі Сполучених Штатів предметів або компонентів предметів, що містять, були зроблені з використанням, отриманням вигоди або використанням комерційної таємниці, незаконно привласненої або придбаної неналежним чином іноземним агентом або іноземним інструментом, та інших цілей"*. Закон передбачає також створення спеціального слідчого комітету з метою прискорення допомоги жертвам крадіжки комерційної таємниці (що має важливе значення, враховуючи необхідність того, щоб механізм був швидким і корисний власникам комерційної таємниці). Новий Міжвідомчий комітет з комерційної таємниці (далі — Комітет) складається з директора Національної розвідки (виступає як єдиний член ex officio, який не має права голосу), міністра фінансів, міністра внутрішньої безпеки, міністра торгівлі, генерального прокурора, координатора із забезпечення дотримання прав ІВ, торгового представника США або інших керівників агентств або виконавчих посадових осіб. Комітет, діючи як прокурор, розглядає скарги Генерального прокурора чи власників комерційної таємниці США (під страхом покарання за лжесвідчення) з поглибленим аналізом, наданим Управлінням директора Національної розвідки. Якщо Комітет визначить, що звинувачення є досить обґрунтованими для продовження роботи, то Комісія з міжнародної торгівлі США (USITC) розгляне справу. Якщо USITC визначить, що цей продукт, швидше за все, тягне за собою комерційну таємницю, вкрадену іноземною суверенною державою, USITC може розпорядитися про виключення продукту з ринку США. Президент має право останнього слова в рішенні USITC, і виключення ринку триває допоки USITC не визначить, що умови, які призвели до його вирішення, більше не дійсні. Зацікавлені сторони також можуть клопотати про зміну чи скасування виняткових наказів. Процес ex parte закриває можливості для таких іноземних урядів, як Китай, щодо зловживання судовою системою США, щоб тримати двері Америки відчиненими для імпорту продуктів, виготовлених із вкрадених комерційних секретів. Це законодавство також є ключовим, оскільки пропонує швидке розв'язання проблеми, яка часто дуже швидко виходить з-під контролю. Продукти будуть виключені з ринку США протягом 60 днів із моменту видання наказу про забезпечення національної безпеки. Традиційні засоби правового захисту через судову систему США або Комісію з міжнародної торгівлі займають від 30 до 18 місяців відповідно. Тим часом більшість украдених комерційних секретів використовуються для відтворення продуктів упродовж 6–12 місяців.

Закон про боротьбу з розкраданням комерційної таємниці Китаєм. Сенатор США Ліндсі Грем (республіканець від штату Південна Кароліна) у квітні 2021 р. представив Закон про боротьбу з китайською крадіжкою (КПК) комерційної таємниці (The Combating Chinese Purloining (CCP) of Trade Secrets Act.) [13]. Документ спрямовано на захист американського бізнесу та державних установ від атак на крадіжку конфіденційної інформації. Закон Грема про комерційну таємницю CCP містить такі ключові положення:

- *збільшення штрафів за використання пристроїв перехоплення зв'язку для надання допомоги іноземному уряду.* Цей законопроєкт збільшує максимальне передбачене законом покарання з 5 до 20 років ув'язнення для тих осіб, які намагаються отримати вигоду з іноземного уряду шляхом виробництва, розповсюдження, володіння або реклами будь-яких пристроїв перехоплення провідного, усного чи електронного зв'язку;
- *захист американського бізнесу від крадіжки зовнішньої комерційної таємниці.* Законопроєкт розширює доступні штрафи для іноземних осіб (включаючи фізичних осіб, корпорації, бізнес-асоціації, державні установи, що діють як комерційне підприємство тощо), які незаконно привласнюють комерційну таємницю. Ці санкції передбачають обмеження на імпорт, запроваджені Митною та прикордонною службою США, відмову в експортних ліцензіях із боку Міністерства торгівлі США; відмову у видачі ліцензії на експорт оборонних товарів або оборонних послуг Державним департаментом США; заборону на подання патентних заявок Відомством США з патентів і торгових марок; та відмову у видачі віз Державним департаментом США;
- *боротьбу з кіберзлочинністю, закриваючи ботнети.* Законодавство розширює можливості Міністерства юстиції боротьби з

мережами скомпрометованих комп'ютерів, відомих як ботнети. Відповідно до чинного законодавства, повноваження Міністерства юстиції на отримання судової заборони на закриття ботнетів обмежені ботнетами, що займаються шахрайством або незаконним прослуховуванням. Це положення розширює повноваження Міністерства юстиції та допускає судові заборони проти ботнетів, що займаються ширшим спектром незаконної діяльності, включаючи знищення даних, атаку типу "відмова в обслуговуванні" (DoS) та інші злочинні дії. Законопроєкт також передбачає кримінальну відповідальність за свідоме заподіяння чи спробу заподіяння шкоди комп'ютеру критичної інфраструктури, коли суттєве пошкодження призводить до збою роботи комп'ютера чи самої критичної інфраструктури, зі штрафом та/або тюремним ув'язненням на строк до 20 років;

- *посилення покарання для тих, хто займається шпигунством, крадіжкою комерційної таємниці та неналежним втручанням у вибори у США.* Законодавство створює підстави для неприпустимості та депортації для тих, хто прагне в'їхати до США для участі у шпигунстві, крадіжці ІВ, включаючи комерційну таємницю, участь у схемах комерційного шахрайства та неналежне втручання у вибори до США;
- *обмеження доступу до фінансованих урядом дослідницьких проєктів.* Законопроєкт забороняє видачу віз китайським громадянам, які загрожують національній безпеці чи намагаються виконати курсову роботу на рівні випускників у таких чутливих галузях, як військова розвідка та ядерна інженерія. Він вимагає, щоб "застраховані особи" з Китаю (і будь-якої іншої "охопленої країни", що загрожує інтересам економічної або національної безпеки США), працювали над чутливими дослідженнями, щоб отримати схвалення від ODNI для участі. Окрім того, він передбачає кримінальну відповідальність за нерозкриття будь-якою особою іноземного фінансування для покритих досліджень [13].

Небезпечний Китай: мінімізація ризиків у співпраці України. За результатами 2020 р. Китай за товарообігом посідає перше місце серед усіх торговельних партнерів України. Китай – це глобальний гравець, який для реалізації власних інтересів готовий здійснювати кроки, які можуть нести загрозу національній безпеці нашої держави. Інтереси Китаю – виграти у стратегічній конкуренції з США, і Китай намагається використати Україну зокрема як джерело військових технологій, які можуть змінити баланс сил на його користь. В умовах посилення стратегічної конкуренції з США Китай зацікавлений у стабільних, дружніх і передбачуваних відносинах із Росією. Саме тому Пекін навряд чи робитиме кроки, які поставлять під сумнів російські інтереси, зокрема і щодо України. Це вже підтвердилося під час вторгнення Росії до України, адже напередодні китайські урядові хакери провели низку кібератак на українські військові та енергетичні об'єкти. Китайський уряд координував потужні кібератаки на понад 600 вебресурсів, що пов'язані з Міноборони України та іншими органами влади. Серія атак розпочалася перед завершенням Зимових Олімпійських ігор у Пекіні 20 лютого 2022 р., а найбільш потужні з них припали на 23 лютого — напередодні вторгнення військ РФ в Україну. Хакери намагалися вилучити або знищити цифрові дані з різних об'єктів України. Цілі охоплювали дані військових органів, Дерприкордслужби, Ради національної безпеки і оборони та Міноборони, а також цивільних об'єктів. Методи, які застосовували хакери Китаю, були націлені на викрадення важливих даних, пошук можливостей для знищення інформації щодо критичної інфраструктури [14; 15]. Тож, безсумнівно, Китай діє лише у своїх прагматичних інтересах, навіть готовий і здійснює дії, які загрожують інтересам інших держав, зокрема України. Так, Офіс Генерального прокурора України 28 серпня 2020 р. повідомив, що Верховний Суд визнав справедливими рішення судів попередніх інстанцій стосовно шпигунської діяльності громадянина КНР, якого було засуджено до 10 років позбавлення волі. У суді було доведено, що громадянин КНР Шу Юаньцзє, професор Сіанського НДІ сучасної хімії проводив шпигунську діяльність на Дніпропетровщині. Маючи ступінь доктора технічних наук, він здійснював розвідувальну діяльність під прикриттям офіційного науково-технічного співробітництва між КНР та Україною, організував на території області збір науково-технічної та технологічної документації в галузі бойового ракетобудування з метою передачі до іноземної організації інформації, яка становить державну таємницю України. Вирок для шпигуна набув законної сили [16].

Варто визначити ***виклики та ризики, пов'язані зі співпрацею з Китаєм*** [17]:

- спроби встановлення контролю над українськими стратегічними підприємствами та заволодіння чутливими військовими технологіями;
- технологічна експансія в такі критичні галузі України, як атомна енергетика, ІТ-сфера, кібербезпека;

- намагання створити критичну залежність від китайського ринку, фінансування та технологій;
- формування в політичному, академічному та експертному середовищі прокитайського лобі тощо.

Китайський уряд прискорює військовий розвиток, зокрема за рахунок своєї агресивної політики здобуття і відтворення чутливих технологій, що є необхідними для подальшої мілітаризації країни. Водночас Китаю бракує досвіду в деяких критичних технологіях, особливо в авіаційній, космічній, суднобудівній і військовій галузях. КНР намагається купувати не лише продукцію, а й технології, на яких вона базується. У рамках експортних контрактів у сфері високих технологій Китай часто намагається включити в контракт пункт про передачу ІВ. Проте, якщо такі положення не передбачаються, то китайські компанії намагаються провести зворотний інжиніринг і самостійно сконструювати пристрій / машину / транспортний засіб. Китай не готовий брати на себе ризики від укладення економічних угод з Україною, вдається лише до тактичних інвестицій і не береться розвивати свої проєкти в Україні без створення для них спеціальних комфортних умов. Таких висновків дійшли автори дослідження Центру економічної стратегії (ЦЕС) за підтримки Центру міжнародного приватного підприємництва (CIPE) [18].

ВИСНОВКИ

Захист прав ІВ століттями вважався критично важливим для інновацій та зростаючої економіки. Проте загрози правам ІВ зростають, а Інтернет спрощує її крадіжку. ІВ особливо цінна в галузі інформаційних і комунікаційних технологій (ІКТ). Роль ІВ і цифрової інфраструктури обороту прав ІВ стає ключовим чинником, що визначатиме рівень національної безпеки держави, зростання національної економіки і, як результат — вплив країни у світі. Понад 70 % трафіку глобальних цифрових мереж нині становить рух об'єктів ІВ. Вартість крадіжок комерційної таємниці у світі досягла 1,7 трлн доларів США на рік, керівники корпорацій очікують, що ризик розкрадання комерційної таємниці ще більше зросте в наступні п'ять років. Незаконне присвоєння чи крадіжка комерційної таємниці коштує 1–3 % ВВП у розвинених країнах. Загрози посилюються зміною культури праці, яку спричинила пандемія. Водночас 45 % керівників не володіють основами комерційної таємниці.

Китайський уряд активно виконує зобов'язання, прописані в американсько-китайській економічній та торговій угоді, підвищує захист прав ІВ (включаючи комерційну таємницю) та прагне створити в країні кращі умови для ведення бізнесу. Захист комерційної таємниці в Китаї здебільшого базується на оновленому "Законі про боротьбу з недобросовісною конкуренцією", а більшість реальних стандартів ґрунтуються на судовій практиці. Єдиний спосіб підтвердити комерційну таємницю в Китаї – це судовий процес.

Так, 22 вересня 2021 р. ЦК компартії Китаю та Державна рада видали "Керівні принципи побудови могутньої країни з правами інтелектуальної власності (2021–2035 рр.)" ("Guidelines for building a powerful country with intellectual property rights (2021–2035)") [19]. У документі викладено грандіозний план Китаю щодо прискорення будівництва держави, яка має силу ІВ. Китай перетворився з великої країни, що імпортує права на ІВ, у велику країну творчості, і трансформація роботи в галузі ІВ від гонитви за кількістю до покращення якості прискорилася в усіх відношеннях. Генеральний секретар Сі Цзіньпін наголосив, що захист інтелектуальної власності пов'язаний із модернізацією національної системи управління та можливостей управління, якісним розвитком, щастям життя людей, загальною ситуацією відкритості країни та національною безпекою [20].

Водночас США вбачають загрози національній безпеці з боку Китаю, тому застосовують нові законодавчі механізми захисту ІВ і комерційної таємниці, уважно стежать за тим, як Китай виконує свої зобов'язання в рамках Економічної і торгової угоди між США та Китаєм (Угода про перший етап). У 2020 р. Китай опублікував декілька проєктів правових і нормативних заходів, пов'язаних з ІВ, і завершив роботу над більш ніж десятком заходів. Примітно, що Китай вніс поправки в патентний закон, закон про авторське право і кримінальний кодекс. Однак ці кроки до реформи вимагають ефективної реалізації і не відповідають всьому спектру фундаментальних змін, необхідних для поліпшення ландшафту ІВ у Китаї.

Вплив на національну безпеку. Крадіжка ІВ щорічно висмоктує з економіки США від 200 до 250 млрд доларів США. Екстраполяція цих даних про крадіжку ІВ у Китаї дає приблизну оцінку від 3,8 до 4,8 млн робочих місць у США, втрачених унаслідок крадіжки ІВ у всьому світі [21]. Існує також зовнішньополітичний аспект крадіжки ІВ. Щорічно Торговий представник США (USTR) публікує Спеціальний звіт 301 про глобальне забезпечення дотримання прав ІВ. В опублікованому 27 квітня 2022 р. USTR Спеціальному звіті (2022 Special 301 Report) Китаю приділяється більша увага, ніж будь-якій іншій країні. USTR вважає, що, попри внесення змін

до свого законодавства, які спрямовані на покращення охорони та захисту прав ІВ, Китаю ще належить розв'язати такі більш фундаментальні проблеми, які переслідують власників ІВ, як "слабкі канали" захисту і відсутність прозорості та незалежності судових органів [22].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Полонская И.* Защита коммерческих секретов в Китае [Электронный ресурс] / И. Полонская. — Режим доступа: https://wiselawyer.ru/poleznoe/90838-zashhita-kommercheskikh-sekretov-kitae.
2. Sino Legend v. ITC: Federal Circuit affirms ITC's trade secret misappropriation determination [Electronic resource]. — Access mode: https://www.lexology.com/library/detail.aspx?g=f6cd69a3-323b-45ba-a4c6-555fc223b76c.
3. Vanillin Trade Secret Case Makes 2021 Top Ten Chinese People's Court Cases [Electronic resource]. — Access mode: https://www.natlawreview.com/article/vanillin-trade-secret-case-makes-2021-top-ten-chinese-people-s-court-cases.
4. *Андрощук Г. О.* Економічне шпигунство: зростання масштабів і агресивності (Ч. І) / Г. О. Андрощук // Наука, технології, інновації. — 2018. — № 3. — С. 39–49.
5. *Андрощук Г. О.* 45 % керівників не володіють основами комерційної таємниці: звіт [Електронний ресурс] // Юридична газета online. — Режим доступу: https://yur-gazeta.com/golovna/45-kerivnikiv-ne-volodiyut-osnovami-komerciynoyi-taemnici-zvit.html.
6. *Федин А.* Пекинская защита. Китай намерен кардинально изменить свой имидж в области интеллектуальной собственности [Электронный ресурс] / А. Федин. — Режим доступ**а**: https://www.cn-expert.pro/blog/pekinskaya-zaschita.
7. The economic and innovation impacts of trade secrets [Electronic resource]. Published 19 April 2021. — Access mode: https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets.
8. *Ben-Achour S.* China's state-sponsored industrial espionage is part of a larger system [Electronic resource] / S. Ben-Achour. — Published 9 Dec 2021. — Access mode: https://www.marketplace.org/2021/12/09/chinas-state-sponsored-industrial-espionage-is-part-of-a-larger-system/.
9. The Department of Justice's National Security Division Chief Addresses China's Campaign to Steal U.S. Intellectual Property [Electronic resource]. — Access mode: https://www.wiggin.com/publication/the-department-of-justices-national-security-division-chief-addresses-chinas-campaign-to-steal-u-s-intellectual-property/.
10. *Андрощук Г. О.* Безпрограшний для Китаю план "Тисяча талантів": звіт Сенату про розкрадання інтелектуальної власності США [Електронний ресурс] / Г. О. Андрощук. — Режим доступу: https://yur-gazeta.com/golovna/bezprograshniy-dlya-kitayu-plan-tisyacha-talantiv-zvit-senatu-pro-rozkradannya-iv-ssha.html.
11. *Андрощук Г. О.* Закон про захист інновацій в США: запобігти крадіжці Китаєм інтелектуальної власності [Електронний ресурс] / Г. О. Андрощук. — Режим доступу: https://yur-gazeta.com/golovna/zakon-pro-zahist-innovaciy-v-ssha-zapobigti-kradizhci-kitaem-intelektualnoyi-vlasnosti.html.
12. *MCdole Ja.* The SECRETS Act Adds a Critical New Defense Against IP Theft Threatening U.S. Tech Leadership [Electronic resource] / Jaci MCdole, NIGEL CORY. — FEBRUARY 24, 2022. Access mode: The SECRETS Act Adds a Critical New Defense Against IP Theft Threatening U.S. Tech Leadership (ipwatchdog.com).
13. Graham Legislation Protects America from Chinese Efforts to Steal Intellectual Property, Trade Secrets and Vital National Security Research [Electronic resource]. — Access mode: Graham Legislation Protects America from Chinese Efforts to Steal Intellectual Property, Trade Secrets and Vital National Security Research - Press Releases - United States Senator Lindsey Graham (senate.gov).
14. Brytyjczycy potwierdzili. Chiny przeprowadziły cyberataki na Ukrainę. [Electronic resource]. — Access mode: https://wiadomosci.wp.pl/brytyjczycy-potwierdzili-chiny-przeprowadzily-cyberataki-na-ukraine-6753865844537888a.
15. *Карловський Д.* Китайські урядові хакери вели кібератаки на Україну перед вторгненням Росії [Електронний ресурс] / Д. Карловський. — 1 квітня 2022. — Режим доступу: https://www.pravda.com.ua/news/2022/04/1/7336424/.
16. *Андрощук Г.О.* Вирок Верховного Суду України китайському шпигуну-науковцю: 10 років позбавлення волі [Електронний ресурс] / Г. Андрощук. — Режим доступу: https://yur-gazeta.com/publications/practice/inshe/virok-verhovnogo-sudu-ukrayini-kitayskomu-shpigununaukovcyu-10-rokiv-pozbavlennya-voli.html.
17. *Пойта Ю.* Небезпечний Китай: як Україні мінімізувати ризики у співпраці зі "стратегічним партнером" [Електронний ресурс] / Ю. Пойта. — Режим доступу: https://www.eurointegration.com.ua/experts/2021/12/6/7131099/.
18. *Горюнов Д.* Китайський економічний слід в Україні : аналітична записка [Електронний ресурс] / Д. Горюнов, Б. Прохоров, Г. Сахно // Центр економічної стратегії… — 24 вересня 2021 р. — Режим доступу: https://ces.org.ua/wp-content/uploads/2021/09/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9%D1%81%D1%8C%D0%BA%D0%B8%D0%B9-%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%B8%D0%B9-%D1%81%D0%BB%D1%96%D0%B4-%D0%B2-%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96-1.pdf.
19. Essentials of the "Guidelines for Building a Powerful Country with Intellectual Property Rights (2021–2035)" [Electronic resource]. — Access mode: http://www.lungtin.com/Content/2021/09-30/1106495335.html.
20. Comprehensively strengthen the protection of intellectual property rights and accelerate the construction of a strong country [Electronic resource]. — Access mode: http://www.kinhalo.com/index.php?m=content&c=index&a=show&catid=62&id=30.
21. Protecting Intellectual Property and the Nation's Economic Security [Electronic resource]. — Access mode: https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2013-14/may-june/protecting-intellectual-property-nations-economic-security/.
22. Eileen McDermott USTR Suspends Review of Ukraine, Remains Concerned with China in Latest

Special 301 Report [Electronic resource]. — Access mode: USTR Suspends Review of Ukraine, Remains Concerned with China in Latest Special 301 Report (ipwatchdog.com).

REFERENCES

1. Polonskaya, I. Zashchita kommercheskikh sekretov v Kitae [Protection of commercial secrets in China]. Retrieved from: https://wiselawyer.ru/poleznoe/90838-zashhita-kommercheskikh-sekretov-kitae [in Russ.].
2. Sino Legend v. ITC: Federal Circuit affirms ITC's trade secret misappropriation determination. Retrieved from: https://www.lexology.com/library/detail.aspx?g=f6cd69a3-323b-45ba-a4c6-555fc223b76c
3. Vanillin Trade Secret Case Makes 2021 Top Ten Chinese People's Court Cases. (December, 15, 2015). Retrieved from: https://www.natlawreview.com/article/vanillin-trade-secret-case-makes-2021-top-ten-chinese-people-s-court-cases.
4. Androshchuk, H. (2018). Ekonomichne shpyhunstvo: zrostannia masshtabiv i ahresyvnosti (Ch. I) [Economic espionage: increasing scale and aggressiveness (P.I)]. *Nauka, tekhnolohii, innovatsii* [Science, technologies, innovations], *3,* 39–49. [in Ukr.].
5. Androshchuk, H. (2021). 45 % of managers do not know the basics of trade secrets: report. *Yurydychna hazeta online. — Legal newspaper online*, *15 June*. Retrieved from: https://yur-gazeta.com/golovna/45-kerivnikiv-ne-volodiyut-osnovami-komerciynoyi-taemnici-zvit.html [in Ukr.].
6. Fedyn, A. Pekinskaya zashchita. Kitaj nameren kardinal'no izmenit' svoj imidzh v oblasti intellektual'noj sobstvennosti [Peking defense. China intends to radically change its image in the field of intellectual property]. Retrieved from: https://www.cn-expert.pro/blog/pekinskaya-zaschita [in Russ.].
7. The economic and innovation impacts of trade secrets. (April, 19, 2021). Retrieved from: https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets
8. Ben-Achour, S. China's state-sponsored industrial espionage is part of a larger system. Retrieved from: https://www.marketplace.org/2021/12/09/chinas-state-sponsored-industrial-espionage-is-part-of-a-larger-system.
9. The Department of Justice's National Security Division Chief Addresses China's Campaign to Steal U.S. Intellectual Property. Retrieved from: https://www.wiggin.com/publication/the-department-of-justices-national-security-division-chief-addresses-chinas-campaign-to-steal-u-s-intellectual-property.
10. Androshchuk, H. Zakon pro zakhyst innovatsii v SShA: zapobihty kradizhtsi Kytaiem intelektualnoi vlasnosti Yurydychna hazeta online [Win-win plan for China "Thousand talents": Senate report on theft of US intellectual property]. Retrieved from: https://yur-gazeta.com/golovna/bezprograshniy-dlya-kitayu-plan-tisyacha-talantiv-zvit-senatu-pro-rozkradannya-iv-ssha.html [in Ukr.].
11. Androshchuk, H. Zakon pro zakhyst innovatsii v SShA: zapobihty kradizhtsi Kytaiem intelektualnoi vlasnosti [The US Innovation Protection Act: to prevent intellectual property theft by China]. Retrieved from: https://yur-gazeta.com/golovna/zakon-pro-zahist-innovaciy-v-ssha-zapobigti-kradizhci-kitaem-intelektualnoyi-vlasnosti.html [in Ukr.].
12. MCdole, Ja., & Cory, N. (2022). The SECRETS Act Adds a Critical New Defense Against IP Theft Threatening U.S. Tech Leadership. Retrieved from: The SECRETS Act Adds a Critical New Defense Against IP Theft Threatening U.S. Tech Leadership Retrieved from: ipwatchdog.com.
13. Graham Legislation Protects America from Chinese Efforts to Steal Intellectual Property, Trade Secrets and Vital National Security Research. Retrieved from: Graham Legislation Protects America from Chinese Efforts to Steal Intellectual Property, Trade Secrets and Vital National Security Research — Press Releases — United States Senator Lindsey Graham (senate.gov).
14. Brytyjczycy potwierdzili. China carried out cyberattacks on Ukraine. Retrieved from: https://wiadomosci.wp.pl/brytyjczycy-potwierdzili-chiny-przeprowadzily-cyberataki-na-ukraine-6753865844537888a.
15. Karlovskyi, D. (2022). Kytaiski uriadovi khakery vely kiberataky na Ukrainu pered vtorhnenniam Rosii [Chinese government hackers conducted cyber attacks on Ukraine before the Russian invasion]. Retrieved from: https://www.pravda.com.ua/news/2022/04/1/7336424/ [in Ukr.].
16. Androshchuk, H. Vyrok Verkhovnoho Sudu Ukrainy kytaiskomu shpyhunu-naukovtsiu: 10 rokiv pozbavlennia voli [Sentence of the Supreme Court of Ukraine to the Chinese spy-scientist: 10 years of imprisonment]. Retrieved from: https://yur-gazeta.com/publications/practice/inshe/virok-verhovnogo-sudu-ukrayini-kitayskomu-shpigununaukovcyu-10-rokiv-pozbavlennya-voli.html [in Ukr.].
17. Poita, Yu. (2021). Nebezpechnyi Kytai: yak Ukraini minimizuvaty ryzyky u spivpratsi zi "stratehichnym partnerom" [Dangerous China: how Ukraine can minimize risks in cooperation with a "strategic partner"]. Retrieved from: https://www.eurointegration.com.ua/experts/2021/12/6/7131099/ [in Ukr.].
18. Horiunov, D., Prokhorov, B., & Sakhno, H. (2021). Kytaiskyi ekonomichnyi slid v Ukraini [The Chinese economic footprint in Ukraine]. *Center for Economic Strategy.* Retrieved from: https://ces.org.ua/wp-content/uploads/2021/09/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9%D1%81%D1%8C%D0%BA%D0%B8%D0%B9-%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87 %D0%BD%D0%B8%D0%B9-%D1%81%D0%BB%D1%96%D0%B4-%D0%B2-%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96-1.pdf [in Ukr.].
19. Essentials of the "Guidelines for Building a Powerful Country with Intellectual Property Rights (2021-2035)". Retrieved from: http://www.lungtin.com/Content/2021/09-30/1106495335.html.
20. Comprehensively strengthen the protection of intellectual property rights and accelerate the construction of a strong country. Retrieved from: http://www.kinhalo.com/index.php?m=content&c=index&a=show&catid=62&id=30.
21. Protecting Intellectual Property and the Nation's Economic Security. Retrieved from: https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2013-14/may-june/protecting-intellectual-property-nations-economic-security/
22. Eileen McDermott USTR Suspends Review of Ukraine, Remains Concerned with China in Latest Special 301 Report. Retrieved from: USTR Suspends Review of Ukraine, Remains Concerned with China in Latest Special 301 Report. Retrieved from: ipwatchdog.com.

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

TRADE SECRET AS A FACTOR OF ENSURING NATIONAL ECONOMIC SECURITY: THE PRACTICE OF CHINA AND THE USA (Part 2)

Abstract. *The global economic and innovative impact of trade secrets is studied. Trade secrets have a broad reach and support the innovation ecosystem by protecting technological, product, market and organizational innovations, as well as providing a key complement and support to other intellectual property (IP). It is shown that misappropriation or theft of trade secrets from OECD countries is 1–3 % of GDP. The cost of trade secret theft has reached $ 1.7 trillion per year. On the example of the economy of China and the USA, the growing importance of intangible assets, commercial secrets and the increasing threats of their theft are shown. In the US, more than 80% of all economic espionage cases and 60 % of trade secret cases are related to China. Given their negative impact on national security, the US is applying new legislative mechanisms to protect IP and trade secrets. The challenges and risks associated with Ukraine's cooperation with China are analyzed. Recommendations for their minimization and countermeasures against threats are given.*

Keywords: *intellectual property, innovation, commercial secret, cyber security, national security, economic espionage.*

ІНФОРМАЦІЯ ПРО АВТОРА

Андрощук Геннадій Олександрович — канд. екон. наук, доц., головний науковий співробітник, Науково-дослідний інститут інтелектуальної власності Національної академії правових наук України, вул. Казимира Малевича, 11, корп. 4, м. Київ, Україна, 03680; +38 (044) 200-08-76; genandro1@gmail.com; ORCID: 0000-0003-0781-9740

INFORMATION ABOUT THE AUTHOR

Androshchuk H. O. — PhD in Economics, Associate Professor, Chief Researcher, Scientific Research Institute of Intellectual Property of the National Academy of Legal Sciences of Ukraine; Kazymira Malevycha Str., 11, 4, Kyiv, Ukraine, 03680; genandro1@gmail.com; +38 044 200-08-76, ORCID: 0000-0003-0781-9740