DOI https://doi.org/10.51647/kelm.2020.6.2.28

DOŚWIADCZENIE PRAWNE W ZAKRESIE OCHRONY TAJEMNIC HANDLOWYCH W INTERNECIE NA UKRAINIE I W USA

Vladyslav Novytskyi
aspirant Katedry Prawa Własności Intelektualnej i Prawa Korporacyjnego Narodowego Uniwersytetu „Odeska Akademia Prawnicza" (Odessa, Ukraina)
ORCID ID: 0000-0003-0796-311X
e-mail: Vladyslav_Novytskyi@mail.ru

Adnotacja. Artykuł poświęcono analizie informacji, które składają się na tajemnicę handlową umieszczoną w Internecie, badaniu legislacyjnego zapewnienia ochrony, zapewnienia, wykorzystania i przechowywania takich informacji, identyfikacji aktualnych problemów, wyciągania wniosków, a także propozycji poprawy ochrony tajemnic handlowych na Ukrainie poprzez analizę porównawczą ochrony tajemnic handlowych w Internecie na Ukrainie i USA.

Podczas prowadzenia działalności informatycznej stale dochodzi do różnych komunikacji z klientami, między partnerami, wewnątrz zespołu. W związku z tym istnieje ryzyko ujawnienia informacji o ograniczonym dostępie w procesie takiej komunikacji. Jednocześnie niektóre informacje są niezwykle ważne i cenne, ponieważ dzięki ich posiadaniu dana firma zarabia pieniądze, ma pewne przewagi konkurencyjne. Jeśli takie informacje trafią do osób nieupoważnionych, firma może ponieść znaczne straty, a nawet cały model prowadzenia działalności może być zagrożony. Dlatego ochrona tajemnic handlowych jest jedną z kluczowych potrzeb biznesowych.

Słowa kluczowe: informacje, tajemnica handlowa w Internecie, bezpieczeństwo informacji, własność intelektualna.

EXPERIENCE OF LEGAL PROVISION OF PROTECTION OF COMMERCIAL SECRETS ON THE INTERNET IN UKRAINE AND THE USA

Vladyslav Novytskyi
Postgraduate Student at the Department of Intellectual Property Law and Corporate Law National University "Odesa Law Academy" (Odesa, Ukraine)
ORCID ID: 0000-0003-0796-311X
e-mail: Vladyslav_Novytskyi@mail.ru

Abstract. The article is devoted to the analysis of information constituting a trade secret posted on the Internet, the study of legislative protection, provision, use and storage of such information, identification of current issues, conclusions, and proposals for improving the protection of trade secrets in Ukraine through comparative analysis of trade protection. secrets on the Internet in Ukraine and the United States.

During the implementation of IT business, there are various communications – with customers, between partners, within the team. Therefore, there are risks of disclosing information with limited access in the process of such communications. At the same time, some information is extremely important and valuable, because due to its possession a particular business earns money, has certain competitive advantages. If such information is found by third parties, the business may suffer significant losses, or even the entire business model may be compromised. That is why the protection of trade secrets is one of the key needs of business.

Key words: information, trade secret on Internet, information security, intellectual property.

ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ ТА СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

Владислав Новицький
аспірант кафедри права інтелектуальної власності та корпоративного права Національного університету «Одеська юридична академія» (Одеса, Україна)
ORCID ID: 0000-0003-0796-311X
e-mail: Vladyslav_Novytskyi@mail.ru

Анотація. Стаття присвячена аналізу інформації, що становить комерційну таємницю, розміщену в мережі Інтернет, дослідженню законодавчого забезпечення захисту, забезпечення, використання та збереження такої інформації, виявленню актуальних проблем, формуванню висновків, а також пропозицій щодо вдосконалення захисту комерційної таємниці в Україні через порівняльний аналіз захисту комерційної таємниці у мережі Інтернет в Україні та Сполучених Штатах Америки.

Під час ведення IT-бізнесу постійно відбуваються різноманітні комунікації – із клієнтами, між партнерами, усередині колективу. Отже, виникають ризики розголошення інформації з обмеженим доступом у процесі таких

комунікацій. Водночас деяка інформація є надзвичайно важливою та цінною, оскільки завдяки володінню нею конкретний бізнес заробляє гроші, має певні конкурентні переваги. Якщо така інформація опиниться у сторонніх осіб, бізнес може зазнати суттєвих збитків, навіть уся модель ведення бізнесу може опинитися під загрозою. Саме тому захист комерційної таємниці є однією із ключових потреб бізнесу.

Ключові слова: інформація, комерційна таємниця в мережі Інтернет, інформаційна безпека, інтелектуальна власність.

Вступ. Актуальність досліджуваної тематики зумовлена необхідністю проведення порівняльного аналізу вже наявного досвіду правового забезпечення захисту комерційної таємниці в Україні та Сполучених Штатах Америки (далі – США). Передусім треба зазначити, що в умовах сучасної економіки, в основі якої лежить конкурентно-ініціююче середовище, актуальна проблема забезпечення захисту інформації суб'єкта підприємницької діяльності. Нині в Україні, як і в інших країнах світу, у процесі підприємницької діяльності, коли створюються нові інформаційні платформи в мережі Інтернет у результаті інтелектуальної праці, виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що мають комерційну цінність. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень, статистичних даних тощо, які націлені на досягнення такої цілі, як отримання прибутку, саме через таку різноманітність доречним є питання про критерії вибору інформації, яку необхідно захищати. Відповідь на це питання дає визначення поняття «комерційна таємниця», яке викладено у ст. 36 Господарського кодексу України (Господарський кодекс України, 2003): «Відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею».

Основна частина. Натепер проблема захисту комерційної інформації дуже гостра, оскільки інформація являє собою цінний складник професійної діяльності в сучасному суспільстві. Дослідження питань, що тісно перекликаються з даною тематикою, здійснював А.І. Марущак («Інформаційне право: доступ до інформації»), який визначає таємну інформацію як відомості, «що становлять державну або іншу передбачену законом таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі» (Марущак, 2007).

І.В. Смольнікова розглядала схожу з досліджуваною тематикою проблему розповсюдження комерційної таємниці в мережі Інтернет саме в карно-процесуальному аспекті, результати досліджень відображені в роботі «Проблемы охраняемой законом тайны в уголовном процессе» (Смольникова, 1998). Так, авторка зазначає, що «з моральних позицій таємниця уособлює комплекс важливих для існування окремої особи, суспільства або держави етичних категорій, ставлення до яких з боку держави означає певний рівень її цивілізованості та демократичності». Важливість збереження комерційної інформації в мережі Інтернет здебільшого досліджена американськими фахівцями, за їхніми підрахунками, втрата 20% інформації, що становить комерційну таємницю, веде до розорення фірми (організації) протягом місяця в 60 випадках зі 100.

Також схожу тематику, а саме «поняття комерційної таємниці», досліджувала д. ю. н. О.О. Кулініч. Авторка зазначала: «Законодавство щодо захисту комерційної таємниці є важливою складовою частиною законодавства, що регулює конфіденційні відносини. Воно має тривалу історію. Так, законодавство щодо крадіжки комерційної таємниці існує у Франції з 1844 р., у Німеччині – з 1909 р. Нещодавно ухвалені спеціальні закони про комерційну таємницю в Японії (1991 р.), Індії (1991 р.), перший закон про захист комерційної таємниці ухвалено у КНР (1993 р.)» (Кулініч).

З вищезазначеного виходить, що в різних країнах світу, де використовуються інформаційні об'єкти, які являють собою комерційну цінність, на жаль, ще не вироблений єдиний підхід до визначення та розуміння поняття такої інформації. Застосовуються різні визначення: «ділові секрети», «виробничі секрети», «торгольні секрети», «конфіденційна інформація», «комерційна таємниця». На превеликий жаль, Україна не є винятком, що, у свою чергу, додатково свідчить про необхідність дослідження обраної тематики.

Метою статті є дослідження можливості імплементації правого досвіду США у правову систему українського законодавства через порівняльний аналіз законодавства України та США, з метою законодавчого вдосконалення застосування правової норми, що пов'язано із захистом комерційної таємниці в мережі Інтернет.

Результати. У Цивільному кодексі України (Цивільний кодекс України) поняття комерційної таємниці розуміється як інформація, яка є секретною в тому розумінні, що вона загалом чи в певній формі та сукупності її складників є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку із цим має комерційну цінність та є предметом адекватних наявним обставинам заходів щодо збереження її секретності, ужитих особою, яка законно контролює цю інформацію.

З наведеного визначення можна виділити ознаки комерційної таємниці, як-от: інформаційність комерційної таємниці; таємність; комерційна цінність; обмежений доступ.

Усі види інформації, які можуть уважатися комерційною таємницею, зокрема й інформацію, що міститься в мережі Інтернет, умовно можна розділити на дві групи: технічна інформація і комерційна інформація.

До першої групи належать незапатентовані науково-технічні розробки, бази даних та інші комп'ютерні програми, створені підприємством, технічні проєкти, промислові зразки, незапатентовані товарні знаки тощо. У свою чергу, об'єкти, до складу яких входять елементи комерційної таємниці, охороняються відповідним законодавством, зокрема: законами України «Про охорону прав на винаходи і корисні моделі» (Про охорону прав на винаходи, 1993), «Про авторське право і суміжні права» (Про авторське право, 1993), «Про

охорону прав на промислові зразки» (Про охорону прав на промислові зразки, 1993), «Про охорону прав на знаки для товарів і послуг» (Про охорону прав на знаки, 1993).

До другої групи віднесено умови контрактів, дані про постачальників і покупців, інформацію про переговори, маркетингові дослідження, дані про розрахунок відпускних цін, розміри знижок тощо. Також Цивільним кодексом України (ст. 420) (Цивільний кодекс України, 2003) визначено, що комерційна таємниця є об'єктом інтелектуальної власності. Отже, майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором. Зокрема, до майнових прав інтелектуальної власності на комерційну таємницю належать: право на використання комерційної таємниці; виключне право дозволяти використання комерційної таємниці; виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці; інші майнові права інтелектуальної власності, встановлені законом, а саме Цивільним кодексом України (ст. 506) (Цивільний кодекс України). Господарським кодексом України (ст. 162) (Господарський кодекс України, 2003) визначено, що суб'єкт господарювання, який є власником технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а власник інформації вживає належних заходів до охорони її конфіденційності. Строк правової охорони комерційної таємниці обмежується в часі. Гарантії права на комерційну таємницю можна розділити на загальні та спеціальні. До загальних гарантій належать гарантії суб'єктивних прав на комерційну таємницю, які надаються кожному громадянину; спеціальні гарантії реалізації – це система передбачених законодавством засобів, спрямованих на вільне придбання і здійснення прав на комерційну таємницю, усунення перешкод у їх реалізації й ефективний захист від порушень цих прав. Отже, можна з упевненістю сказати, що склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються самостійно її власником або керівником підприємства з дотриманням норм чинного законодавства, саме захист комерційної таємниці є найбільш важливим питанням у процесі використання такої інформації.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого й іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Господарський кодекс України у ст. 162 лише вказує на правомочності суб'єктів господарювання щодо комерційної таємниці. Так, суб'єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до охорони її конфіденційності (Господарський кодекс України, 2003).

Відомості, які не можуть становити комерційну таємницю, визначено в постанові Кабінету Міністрів України № 611 від 9 вересня 1993 р. «Про перелік відомостей, що не становлять комерційної таємниці». Тобто законодавчим критерієм визначення комерційної таємниці можна вважати внесення (або невнесення) Кабінетом Міністрів України відомостей до зазначеного переліку (Про охорону прав на знаки, 1993).

Кваліфікуючою ознакою відомостей, що містять комерційну таємницю, є можливість завдання матеріальної шкоди підприємству або його діловій репутації. Не обов'язково, щоб розголошення відомостей завдало реальної шкоди. Також законодавчо не встановлено, яким саме інтересам може бути завдано шкоди. Можна припустити, що інтереси підприємства можуть бути порушені внаслідок розголошення цих відомостей, у використанні їх конкурентами з метою одержання певних переваг над іншими суб'єктами господарювання.

У Законі України «Про захист від недобросовісної конкуренції» заборонено «неправомірне» збирання таких відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання. За законодавством Німеччини, збирання відомостей визнається неправомірним тільки в тому разі, якщо воно здійснюється «без отримання на це повноважень», а також «із застосуванням технічних засобів» (копіювальна техніка, фотоапарати, телекамери, пристрої для прослуховування), «через виготовлення точного відображення таємниці» (копії, креслення, передрук, запис на магнітну плівку) або «через виїмку предмета, до якого включено таємницю» (Про перелік відомостей, що не становлять комерційної таємниці, 1993). Інформація з обмеженим доступом поділяється відповідно до Закону України «Про інформацію» на конфіденційну, таємну та службову. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (Про інформацію, 1992).

На жаль, в Україні немає єдиного спеціального законодавчого акта, яким були би врегульовані питання щодо застосування та захисту комерційної таємниці, що негативно впливає на пов'язані з нею правовідносини. Визначити правовий механізм захисту комерційної таємниці в межах правового поля України можна за допомогою таких нормативних актів у сукупності.

У сучасному світі інформація вкрай швидко поширюється завдяки широкому розвитку та доступу до мережі Інтернет та мобільному зв'язку – використання цих ресурсів є найбільш масовим, що водночас становить складність у контролі поширення та передачі інформації. Існує міжнародний досвід щодо запобігання

поширенню інформації, яка становить комерційну таємницю, але наслідкам таких дій потрібно давати чітку оцінку, оскільки вони становлять загрозу праву людини на недоторканність її особистого життя, а тому потребують індивідуалізації та постійного коригування. Наприклад, несанкціонованим доступом до інформації й електронним шпіонажем займаються переважно висококваліфіковані спеціалісти, які працюють як приватні особи або за завданням різних фірм та установ.

У різних країнах існують різні підходи щодо визначення того, що є конфіденційною комерційною інформацією. Так, у США захищаються окремі торгові таємниці й ноу-хау; у Німеччині – таємниці фірми. У законодавстві Росії, наприклад, використовуються водночас декілька паралельних термінів – «службова таємниця», «комерційна таємниця», «ноу-хау», що лише ускладнює формування єдиної системи захисту конфіденційної комерційної таємниці, яка розміщується в мережі Інтернет.

Одним із найбільш складних питань правового регулювання відносин, пов'язаних із комерційною таємницею, що розміщується в мережі Інтернет, є питання встановлення рівноваги публічних та приватних інтересів. З одного боку, суспільство та його громадяни мають право знати про те, що може спричинити їм шкоду, обмежити їхні права. З іншого боку, суб'єкти господарювання займаються підприємницькою діяльністю в умовах усе більш жорсткої конкуренції, яка може здійснюватися недобросовісними методами.

Дії суб'єктів господарювання, які спрямовані на отримання чужої конфіденційної інформації, нерідко здійснюються у формі, яка характеризується в законодавстві різних країн як промислове (комерційне) шпигунство. Небезпечність промислового шпигунства почали розуміти в багатьох розвинутих країнах. У США тільки приблизно 5% таких компаній (хоча за даними Ради з розроблення науково-технічної політики при Білому домі, щорічні втрати бізнесу США з таких причин становлять майже 100 млрд доларів). Найбільш відомий приклад – формула напою "Coca-Cola", яка вже більше ста десяти років суворо охороняється.

Електронним шпіонажем займається Агентство національної безпеки США (далі – АНБ), а також аналогічні органи Австралії, Канади, Нової Зеландії, Великобританії та багатьох інших країн. АНБ США здійснює це за допомогою програми «Проєкт Ешелон», у межах якої сканується весь потік інформації у мережі Інтернет, фіксуються всі розмови по мобільному зв'язку, факси і міжнародні телефонні дзвінки.

Згідно із серією звітів, підготовлених дослідним відділом Європарламенту під назвою STOA (Scientific and Technological Option Assessment program – Програма оцінки можливостей науки і техніки) (Звіт Європарламенту STOA щодо проєкту «Ешелон»), задіяне у «Проєкті Ешелон» обладнання здатне за тридцять хвилин опрацювати 1 млн повідомлень. Дослідники STOA засвідчили, що система аналізує ключові слова, фільтрує перехоплені матеріали настільки детально, що з 1 млн лише десять повідомлень відправляються на детальний аналіз, який становить фільтрацію другого рівня. Унаслідок цього до аналітиків АНБ США потрапляють ще менша кількість повідомлень.

Критерієм незаконного присвоєння відомостей, що становлять комерційну таємницю, тобто здійснення правопорушення, за законодавством США, є придбання, використання або розголошення зазначених відомостей іншою особою неналежними засобами. Таке придбання комерційної таємниці може оспорюватися шляхом подання позову до суду в разі, якщо відповідач купує зазначені вище відомості неналежними засобами, або якщо він їх купує в іншої особи і знає або має підстави вважати, що ці відомості були отримані неналежними засобами. Власник прав на комерційну таємницю повинен продемонструвати свої права на зазначені відомості, а також довести, що такі відомості становлять комерційну таємницю.

В умовах глобальної нестабільності значного поширилося використання кіберпростору для здійснення конкурентної розвідки та промислового (комерційного) шпигунства. Завдяки високим технологіям шпигувати за чужими промисловими секретами стало набагато простіше, ніж 10–15 років тому. Підприємці швидко засвоїли, що, вивідуючи комерційні секрети, можна оптимізувати процес входження на ринок, потіснити конкурентів, раніше за інших вивести новий товар, заволодіти новими технологіями і суттєво зекономити час і кошти. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкурентної боротьби роблять викрадення чужих комерційних таємниць особливо прибутковою і перспективною справою. Як результат, втрати Німеччини від промислового (комерційного) шпигунства оцінюють у 20 млрд євро щорічно, втрати США – від 100 млрд доларів. Наприклад, у 2013 р. суд у США засудив до тюремного ув'язнення сімейну пару китайського походження, яка здійснила крадіжку технологій гібридних силових установок у концерну "General Motors" із метою продажу Китаю для подальшого відтворення в автомобільній промисловості. Їм вдалося скопіювати приблизно 16 тисяч документів і завдати шкоди концерну в розмірі 46 млн доларів. Варто підкреслити, що сучасні IT-технології дають можливість на відстані відстежувати діяльність конкурентів, зокрема: сервіс SEMrush дозволяє аналізувати конкурентні сайти, джерела трафіку, ключові слова, за якими конкуренти просуваються в Google; Semantic Force здійснює моніторинг інформаційного поля і медійної активності конкурентів не тільки в соціальних мережах, а й в онлайн-виданнях, відстежує активність співробітників компанії. Крім того, для конкурентної розвідки використовують хмарні технології, SaaS системи і серверні ферми Google.

Правова охорона комерційної таємниці виникає автоматично в разі, якщо відомості, що мають цінність для правовласника, тримаються в секреті з використанням розумних заходів (reasonable measures). Розумність заходів, що використовуються для захисту конфіденційності відповідних відомостей, визначається в кожному конкретному випадку. Невикористання розумних заходів щодо захисту відомостей, як-от угода про конфіденційність, призводить до втрати прав на комерційну таємницю.

Серед типів відомостей, що зазвичай мають правову охорону, є формули, зразки, компіляції, програми, пристрої, інструкції, способи та технології. Відповідно, списки клієнтів, інструкції, виробничі процеси, методи розробки програмного забезпечення (зокрема, його коди), а також винаходи, які не були запатентовані, часто отримують правову охорону за законодавством США про комерційну таємницю.

Особи, які подають заявки про реєстрацію прав на винаходи, часто використовують положення законодавства про комерційну таємницю з метою правової охорони своїх винаходів під час їх розробки та протягом процесу розгляду заявки до того часу, поки заявка не буде опублікована і відомості, що містяться в такій заявці, не втратять статусу конфіденційності.

Незаконне присвоєння необхідно доводити в кожному конкретному випадку. Незаконне присвоєння нерідко можна довести за допомогою прямих доказів того, що відповідач одержав відомості, які становлять комерційну таємницю, за допомогою хабаря, крадіжки або шпигунства. Для доведення незаконного присвоєння не потрібно фізичного отримання документів, що містять комерційну таємницю, хоча це може бути корисним.

Несанкціоноване використання чи розголошення можна також довести, встановивши, що відповідач не був уповноважений правовласником використовувати комерційну таємницю, що він знав або мав підстави вважати, що його знання про комерційну таємницю походять від особи, яка використала незаконні засоби для її набуття, або що він одержав такі знання від особи, яка повинна була зберігати комерційну таємницю чи обмежувати її використання відповідності зі своїми службовими обов'язками.

Найчастіше справи, пов'язані з комерційною таємницею, стосуються крадіжки конфіденційних відомостей, що становлять комерційну таємницю, колишніми працівниками, економічного шпигунства за допомогою незаконних методів спостереження, а також несанкціонованої цифрової передачі програмних кодів і майстер-файлів. У зв'язку з необхідністю захищати конфіденційні відомості від несанкціонованого розголошення суди зазвичай видають охоронні накази, що обмежують розкриття таких відомостей тільки певним спеціально зазначеним особам, які несуть зобов'язання зберігати надані ним відомості в секреті. Суди також часто проводять закриті слухання та вводять обмежений режим доступу до матеріалів справ із метою подальшого забезпечення секретності комерційної таємниці (Практика защиты коммерческой тайны и интеллектуальной собственности в США, 1992).

З огляду на викладене вище та враховуючи практику вживання заходів охорони комерційної таємниці в мережі Інтернет у США, можна сформулювати низку пропозицій щодо захисту останньої в цивільному праві України. Так, знаючи головні канали та джерела інформації, яка має характер комерційної таємниці, можна запропонувати систему заходів з її захисту, яка повинна відрізнятися ефективністю, простотою, керованістю та маи всеохоплюючий характер.

По-перше, для створення системи гарантування інформаційної безпеки суб'єкта господарювання або звичайної фізичної особи в мережі Інтернет необхідно:

– виявити інформацію, яка буде мати характер комерційної таємниці;
– встановити місця її накопичення (на серверах або на будь-якій інформаційні платформі);
– визначити найбільш вірогідні канали та джерела її витікання;
– оцінити ефективність заходів з її захисту;
– розробити систему контролю за здійсненням вказаних заходів.

По-друге, створення системи захисту інформації від несанкціонованого доступу потребує особливо кропіткої роботи з кадровим потенціалом – відповідними підрозділами роботи з інформацією, що знаходяться на електронних носіях, серверах та загалом у мережі Інтернет. Охорона конфіденційної інформації, що становить комерційну таємницю, може бути забезпечена комплексом юридичних, фізичних, технічних і психологічних заходів, як-от:

– розробка інструкцій із забезпечення збереження комерційної таємниці;
– регулювання відносин із використання інформації, що становить комерційну таємницю, викладену в мережу Інтернет, працівниками на підставі трудових договорів та контрагентами на підставі цивільно-правових договорів.

Висновки. Співвідношення важливості порядку використання інформації, що становить комерційну таємницю, у мережі Інтернет, відповідальності за її незаконне збирання, використання та розголошення не відображає повною мірою цінності цієї інформації. Тому вкрай важливо налагодити правові інструменти захисту, збереження інформації, що становить комерційну таємницю, викладену в мережу Інтернет, та відповідальності за її незаконне збирання, використання та розповсюдження. Дотримання зазначених вище заходів щодо організації захисту комерційної таємниці не тільки буде запорукою спокою суб'єктів господарської діяльності та звичайних фізичних осіб, але й стане підгрунтям у разі розгляду спору в судовому порядку, оскільки перевірка захисту комерційної таємниці здійснюється лише тоді, коли права на комерційну таємницю, розміщену в мережі Інтернет, порушуються і потрібно встановити, чи існували вони взагалі. Окрім цього, зважаючи на об'єктивну недостатність спеціалізованих норм про захист комерційної таємниці в мережі Інтернет у законодавстві України, варто звернути увагу на вже наявний досвід США як однієї з найпрогресивніших країн із даної тематики, можливість запозичення її досвіду для створення плацдарму для подальшого правого врегулювання обраної проблеми.

Список використаних джерел:

1. Господарський кодекс України від 16 січня 2003 р. № 436–IV. *Відомості Верховної Ради України.* 2003. № № 18–22. Ст. 144.

2. Цивільний кодекс України від 16 січня 2003 р. № 435–IV. *Відомості Верховної Ради України.* 2003. № № 40–44. Ст. 356.
3. Про охорону прав на винаходи і корисні моделі : Закон України від 15 грудня 1993 р. № 3687–XII. *Законодавство України* : база даних / Верховна Рада України. URL: http://zakon4.rada.gov.ua/laws/show/3687-12 (дата звернення: 17.07.2020).
4. Про авторське право і суміжні права : Закон України від 23 грудня 1993 р. № 3792–XII. *Законодавство України* : база даних / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/3792-12 (дата звернення: 17.07.2020).
5. Про охорону прав на промислові зразки : Закон України від 15 грудня 1993 р. № 3688–XII. *Законодавство України* : база даних / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/3688-12 (дата звернення: 17.07.2020).
6. Про охорону прав на зразки для товарів і послуг : Закон України від 15 грудня 1993 р. № 3689–XII. *Законодавство України* : база даних / Верховна Рада України. URL: http://zakon4.rada.gov.ua/laws/show/3689-12 (дата звернення: 17.07.2020).
7. Звіт Європарламенту STOA щодо проєкту «Ешелон». URL: http://cryptome.org/echelon-090501.htm (дата звернення: 17.07.2020).
8. Практика защиты коммерческой тайны и интеллектуальной собственности в США. Киев : Хрещатик, 1992. 168 с.
9. Марущак А.І. Інформаційне право: доступ до інформації : навчальний посібник. Київ : КНТ, 2007. С. 134.
10. Смольникова И.В. Проблемы охраняемой законом тайны в уголовном процессе. Иркутск, 1998. С. 32.
11. Кулініч О.О. Інформація з обмеженим доступом як об'єкт цивільних прав. URL: https://mydisser.com/dfiles/66956225 (дата звернення: 17.07.2020).
12. Про перелік відомостей, що не становлять комерційної таємниці : постанова Кабінету Міністрів України № 611 від 9 вересня 1993 р. URL: http://zakon2.rada.gov.ua/laws/show/611- 93-п (дата звернення: 17.07.2020).
13. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657–XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

References:

1. Hospodarskyi kodeks Ukrainy [Economic Code of Ukraine] vid 16.01.2003 № 436–IV Vidomosti Verkhovnoi. Rady Ukrainy. 2003. № 18, № 19–20, № 21–22. St. 144 [in Ukrainian].
2. Tsyvilnyi kodeks Ukrainy [The Civil Code of Ukraine] vid 16.01.2003 № 435–IV Vidomosti Verkhovnoi. Rady Ukrainy. 2003. № № 40–44. St. 356 [in Ukrainian].
3. Pro okhoronu prav na vynakhody i korysni modeli [About the protection of rights to inventions and utility models] : Zakon Ukrainy vid 15.12.1993 № 3687–XII. Zakonodavstvo Ukrainy : baza danykh / Verkhov. Rada Ukrainy. URL: http://zakon4.rada.gov.ua/laws/show/3687-12 (data zvernennia: 17.07.2020). [in Ukrainian].
4. Pro avtorske pravo i sumizhni prava [About copyright and related rights] : Zakon Ukrainy vid 23.12.1993 № 3792–XII. Zakonodavstvo Ukrainy : baza danykh / Verkhov. Rada Ukrainy. URL: http://zakon3.rada.gov.ua/laws/show/3792-12 (data zvernennia: 17.07.2020) [in Ukrainian].
5. Pro okhoronu prav na promyslovi zrazky [About protection of the rights to industrial designs] : Zakon Ukrainy vid 15.12.1993 № 3688–XII. Zakonodavstvo Ukrainy : baza danykh / Verkhov. Rada Ukrainy. URL: http://zakon3.rada.gov.ua/laws/show/3688-12 (data zvernennia: 17.07.2020) [in Ukrainian].
6. Pro okhoronu prav na zrazky dlia tovariv i posluh [About protection of the rights to samples for the goods and services] : Zakon Ukrainy vid 15.12.1993 № 3689–XII. Zakonodavstvo Ukrainy : baza danykh / Verkhov. Rada Ukrainy. URL: http://zakon4.rada.gov.ua/laws/show/3689-12 (data zvernennia: 17.07.2020) [in Ukrainian].
7. Zvit Yevroparlamentu STOA shchodo proektu "Eshelon". [STOA European Parliament report on the Echelon project] URL: http://cryptome.org/echelon-090501.htm (data zvernennia: 17.07.2020) [in Ukrainian].
8. Praktyka zashchyty kommercheskoi tainy y yntellektualnoi sobstvennosty v SShA. [The practice of protecting trade secrets and intellectual property in the United States.] K.: Khreshchatyk, 1992. 168 p. [in Russian].
9. Marushchak A.I. (2007). Informatsiine pravo: dostup do informatsii [Information law: access to information] : navchalnyi posibnyk. KNT, p. 134 [in Ukrainian].
10. Smolnykova Y.V. (2007). Problemy okhraniaemoi zakonom tainy v uholovnom protsesse. [Problems of legally protected secrecy in criminal proceedings] Yrkutsk, 1998. p. 32 [in Russian].
11. Kulinich O.O. Informatsiia z obmezhenym dostupom yak obiekt tsyvilnykh prav. [Restricted information as an object of civil rights] URL: https://mydisser.com/dfiles/66956225. (data zvernennia: 17.07.2020) [in Ukrainian].
12. Pro perelik vidomostei, shcho ne stanovliat komertsiinoi taiemnytsi [About the list of information that does not constitute a trade secret] : postanova Kabinetu Ministriv Ukrainy № 611 vid 9 veresnia 1993 r. URL: http://zakon2.rada.gov.ua/laws/show/611- 93-p. (data zvernennia: 17.07.2020) [in Ukrainian].
13. Pro informatsiiu : [About information] Zakon Ukrainy vid 02.10.1992 № 2657–XII. Vidomosti Verkhovnoi Rady Ukrainy. 1992. № 48. St. 650 [in Ukrainian].