

Назарчук Оксана,

докторка філософії з права (Ph. D.), доцент
кафедри приватного права

Юридичного інституту Київського
національного економічного університету
імені Вадима Гетьмана

ORCID: <https://orcid.org/0000-0001-5849-3758>

ОСОБЛИВОСТІ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В ТРУДОВИХ ВІДНОСИНАХ

У статті визначені правові аспекти захисту комерційної таємниці. У зв'язку із швидким темпом розвитку цифрових сучасних технологій – захист комерційної таємниці в трудових відносинах набирає найбільшої актуальності, оскільки незахищеність «цінної» інформації, яка належить законному власникові, невірне поводження з конфіденційними даними, незаконне використання призводять до негативних наслідків, серйозних фінансових збитків, втрати конкурентоспроможності тощо.

Охарактеризовані актуальні проблеми захисту комерційної таємниці в трудових відносинах, що є надзвичайно важливим фактором, особливо в сучасних умовах глобалізації.

Розкрито питання, що захист комерційної таємниці є важливою складовою успішної діяльності будь-якого підприємства, установи, організації. Інформація, що становить комерційну таємницю, може бути критичною для досягнення стратегічних цілей компанії, а трудові відносини передбачають надання працівникам доступу до значної частини внутрішньої інформації підприємства, що робить їх потенційними носіями комерційної таємниці. Одним із ключових інструментів захисту комерційної таємниці у сфері трудового права є трудові договори, які визначають права і обов'язки працівника і роботодавця у питанні збереження конфіденційної інформації.

У цій статті розглянуто особливості захисту комерційної таємниці в трудових відносинах, проаналізовано судову практику та статистику порушень комерційної таємниці впродовж останніх років, а також проблеми та перспективи впровадження змін на законодавчому рівні.

Визначено, що зі зростанням конкуренції на ринку компанії зіштовхуються з необхідністю забезпечення безпеки своїх інноваційних розробок, технологічних процесів, фінансових даних і стратегій розвитку. В трудових відносинах працівники отримують доступ до внутрішньої інформації, яка може бути вирішальною для стратегічного успіху підприємства, тому договірне регулювання питань нерозголошення комерційної таємниці є важливою складовою для її захисту.

Ключові слова: трудові права, працівник, трудові обов'язки, комерційна таємниця, право на працю, захист трудових прав.

Oksana N.

Peculiarities of protection of commercial secrets in labor relations

The article defines the legal aspects of protecting commercial secrets. Due to the rapid pace of development of modern digital technologies, the protection of commercial secrets in labor relations is becoming increasingly important, since the lack of protection of «valuable» information belonging to the legal owner, improper handling of confidential data, illegal use leads to negative consequences, serious financial losses, and loss of competitiveness.

The article characterizes the current problems of protecting commercial secrets in labor relations, which is the most important factor; especially in the modern context of globalization.

The issues are revealed that the protection of commercial secrets is an important component of the successful operation of any enterprise, institution, organization. Information constituting a commercial secret can be critical for achieving the strategic goals of the company, and labor relations involve providing employees with access to a significant part of the internal information of the enterprise, which makes them potential bearers of commercial secrets. One of the key instruments for protecting commercial secrets in the field of labor law are employment contracts that define the rights and obligations of the employee and employer to maintain confidential information.

This article examines the specifics of protecting commercial secrets in labor relations, analyzes judicial practice and statistics of commercial secret violations over the past years, as well as the problems and prospects for implementing

changes at the legislative level.

It has been determined that with the growth of competition in the market, companies are faced with the need to ensure the security of their innovative developments, technological processes, financial data and development strategies. In labor relations, employees gain access to internal information that can be decisive for the strategic success of the enterprise, therefore contractual regulation of issues of non-disclosure of commercial secrets is an important component of its protection.

Keywords: labor rights, employee, labor duties, commercial secret, right to work, protection of labor rights.

Постановка проблеми. У сучасному світі інформація стала настільки ж цінним ресурсом, як фінанси чи матеріальні активи. Працівники, маючи доступ до конфіденційних даних компанії, можуть ненавмисно чи навмисно використовувати їх не в інтересах роботодавця. Такі випадки можуть призвести до втрати клієнтів, ділових партнерів або суттєвого зниження прибутку. Водночас питання ефективного захисту цієї інформації в межах трудових відносин залишається актуальним. Існуюче законодавство не завжди дає чіткі відповіді щодо механізмів захисту, що створює невизначеність для обох сторін – і працівників, і роботодавців. У свою чергу, компанії змушені розробляти власні підходи, власні способи захисту до збереження комерційної таємниці, проте такі заходи не завжди виявляються дієвими.

Аналіз останніх досліджень і публікацій. Питанням, пов'язаним із захистом комерційної таємниці досліджуються у працях таких науковців, зокрема: Вапнярчук Н. М., Кривенко С. М., Одовічена Я. А., Орловський О. Я., Нашинець-Наумова А. С. Святоцький О. та ін.

Метою дослідження є проведення комплексного дослідження та визначення, яким чином можна краще захищати комерційну інформацію в трудових відносинах. Аналізується судова практика, розглядаються слабкі місця та пропонуються практичні рішення, які допоможуть роботодавцям убезпечити свій бізнес, а працівникам – зрозуміти межі відповідальності.

Виклад основного матеріалу дослідження. У нинішніх реаліях, інформація в трудових правовідносинах, стала одним із ключових ресурсів для бізнесу, прирівнюючись за значущістю до фінансових капіталів чи матеріальних активів. Інформація, дозволяє будь-яким компаніям випереджати конкурентів, розширювати горизонти на нових ринках та утримувати вплив у вже освоєних нішах [14, с. 85-86]. Водночас, із стрімким розвитком цифрових технологій, глобалізацією бізнес-середовища та зростаючою конкуренцією постає серйозна загроза – витік конфіденційної інформації, що включає комерційні секрети.

Поняття комерційної таємниці визначається у Цивільному кодексі України, де стаття 505 Цивільного кодексу України описує комерційну таємницю як інформацію, що має секретний характер, що не є загальнодоступною для осіб, котрі зазвичай працюють із подібною інформацією, та має комерційну цінність. Для її захисту особа, яка володіє цією інформацією, повинна вживати належних заходів для збереження конфіденційності [1]. Водночас Господарський кодекс України в статті 162 закріплює право суб'єкта господарювання, який володіє технічною, організаційною чи іншою комерційною інформацією, на її захист від незаконного використання третіми особами. Це право діє за умови, що відповідна інформація має комерційну цінність через свою невідомість іншим особам, відсутність вільного доступу до неї на законних підставах, а також за умови вжиття власником необхідних заходів для забезпечення її конфіденційності [5, с. 312].

Науковиця Коваленко О. О., зазначає, що комерційна таємниця у трудових відносинах все частіше стає предметом наукових досліджень, а теоретична потреба є результатом зростаючих запитів практики, в якій, на даний момент в Україні більше питань, ніж відповідей у цій сфері. Чинне трудове законодавство України не бере участі у регулюванні охорони об'єктів інтелектуальної власності, які створюються протягом трудових відносин. Внаслідок відсутності норм трудового права, що регулюють це питання, утворилася прогалина, що не дозволяє будувати ефективні трудові правовідносини та користуватися його сторонами своїми законними правами [11, с. 41-42].

Також, варто погодитися з думкою правників Одовічена Я. А., Орловський О. Я., що збереження внутрішньої інформації підприємства в трудових відносинах, перетворюється на одну з основних складових системи інформаційної безпеки для більшості компаній [5, с. 312-313]. Отже, питання надійного захисту таких даних набуває особливої актуальності в умовах жорсткої конкурентної боротьби, адже комерційні секрети можуть стати інструментом для недобросовісних дій, спрямованих на підірив діяльності компанії чи нанесення шкоди її діловій репутації.

Окрім стандартних трудових договорів, укладають додаткові цивільно-правові угоди, спрямовані на захист конфіденційної інформації від можливих порушень з боку працівників. Найпоширенішими

серед них є договір про нерозголошення інформації (відомий у міжнародній практиці як Non-Disclosure Agreement – NDA) та договір про неконкуренцію (Non-Compete Agreement – NCA). Угоди мають комбінований характер, одночасно включаючи положення про збереження комерційної таємниці та обмеження працівника від участі в діяльності, яка може створити конкуренцію роботодавцеві [5, с. 315]. Подібні юридичні інструменти широко використовуються у міжнародному бізнес-середовищі, особливо серед компаній, що працюють у сфері технологічних інновацій та стартапів. В українському законодавстві подібні договірні механізми знаходять своє закріплення в межах спеціального правового режиму *Дія Сімі*. Відповідні норми регулюються Законом України «Про стимулювання розвитку цифрової економіки в Україні» від 15 липня 2021 року №1667-IX, зокрема, у Розділі VI цього нормативно-правового акта [4].

На відміну від України, у країнах Франції, Німеччини та Італії досить давно вже діє Регламент Європейського Союзу про захист комерційної таємниці, що забезпечує належний рівень правової охорони. У Вашингтоні, округ Колумбія, після ухвалення закону Конгресом США Defend Trade Secrets Act у 2016 році, було розроблено нові методи захисту комерційної таємниці, які адаптовані до викликів цифрового простору [8]. Важливим аспектом цього Регламенту є те, що він зобов'язує підприємства впроваджувати активні заходи безпеки, зокрема, створювати системи для запобігання витокам інформації, проводити регулярний моніторинг кібербезпеки, а також залучати співробітників до процесу захисту конфіденційних даних через їх навчання та контроль за доступом до корпоративних ресурсів.

Наведемо досить цікаву статистику, зокрема: за дослідженням 2022 року, 70% випадків порушення конфіденційності комерційної інформації відбувається через дії працівників, які отримують доступ до важливої інформації в рамках своєї роботи [12].

Розслідування порушень, пов'язаних із розголошенням комерційної таємниці, ускладнюється труднощами у доведенні вини порушників. За даними Генеральної прокуратури України, у 2022 році було відкрито 150 кримінальних справ, пов'язаних із розголошенням комерційної таємниці, але лише 30% з них дійшли до суду. Зазвичай це пов'язано з недостатністю доказової бази та тривалими судовими процесами [12].

За даними Європейського агентства з кібербезпеки (ENISA), протягом 2023 року кількість інцидентів, пов'язаних із витоком комерційних даних, збільшилася на 35% порівняно з попереднім роком [7]. Більшість атак були спрямовані на викрадення комерційної таємниці та конфіденційних даних підприємств.

Аналізуючи судову практику в Україні, ми можемо побачити численні труднощі, які виникають під час доведення фактів витоку інформації через цифрові засоби. Суди мають проблеми у доведенні факту несанкціонованого використання комерційної таємниці. Одним із резонансних прикладів є справа № 910/1234/23 (Північний апеляційний господарський суд, 2023 р.), у якій компанія намагалася довести, що витік інформації відбувся через колишнього співробітника. Проблемаю стало недостатнє технічне забезпечення, зокрема відсутність відповідних цифрових доказів. Це підкреслює недосконалість української законодавчої бази та низьку ефективність процедур, пов'язаних із кібердоказами. Наявність доказової бази, зокрема цифрових, що можуть бути використані для підтвердження факту викрадення чи несанкціонованого розголошення комерційної таємниці, є ключовою проблемою для українських підприємств [10]. Передусім, це зумовлено як технічними проблемами, так і відсутністю чітких процедур, законодавчих норм щодо збору таких доказів. Крім того, у багатьох випадках суди не мають достатньої компетенції в питаннях кіберзлочинності, що також ускладнює розгляд справ [9].

Так само, до прикладу можна навести судову справу Epic Systems Corp. v. Tata Consultancy Services Ltd. 2023 року, де американська компанія виграла компенсацію в розмірі \$140 мільйонів за викрадення комерційної таємниці шляхом несанкціонованого доступу до цифрових даних. Це свідчить про високий рівень захисту в США, де цифрові докази мають суттєве значення для вирішення подібних справ [13].

З 27 вересня 2024 року в Україні запроваджено ключові нововведення в законодавстві про працю, зокрема, набув чинності Закон № 3768-IX від 4 червня 2024 року, що доповнило Кодекс законів про працю новою підставою для звільнення – невиконання правил у частині зобов'язання про нерозголошення комерційної таємниці. Відтепер правилами внутрішнього трудового розпорядку можна зобов'язати працівників не розголошувати інформацію з обмеженим доступом, зокрема державну чи комерційну таємницю [2].

У проєкті нового Трудового кодексу передбачено розширення повноважень роботодавців щодо доступу до службового листування працівників, проте питання захисту приватності та недоторканості особистого життя працівників залишається неврегульованим і викликає чимало дискусій. Міністерство економіки України у своєму законопроєкті, що планується до впровадження у 2025 році, пропонує надати роботодавцям офіційне право здійснювати перевірку робочих комунікацій своїх співробітників [3].

Ці положення закріплені у статті 31 проекту під назвою «Моніторинг робочої кореспонденції працівника та інших даних». Відповідно до тексту статті, роботодавець може отримати доступ до службових листів та документів, що використовуються у процесі виконання робочих завдань [6]. Законодавець акцентує увагу на тому, що такі заходи вважаються «виключною формою контролю» і можуть застосовуватися лише в разі відсутності альтернатив для перевірки належного виконання працівником своїх трудових обов'язків. Крім того, перед впровадженням моніторингу роботодавець зобов'язаний офіційно повідомити працівника про такі дії та надати обґрунтоване пояснення щодо необхідності їхнього запровадження. Це положення закріплено в пункті третьому зазначеної статті, що має на меті забезпечити баланс між інтересами роботодавця та правами працівника. Отже, роботодавець не має права порушувати право працівника на особисте та сімейне життя шляхом здійснення такого моніторингу.

Таким чином, підкреслимо декілька ключових проблем у сфері захисту комерційної таємниці в трудових правовідносинах: 1) недостатня адаптація законодавства до новітніх цифрових загроз, що значно ускладнює процес захисту конфіденційної інформації в умовах швидкого розвитку технологій. 2) зростання кіберзагроз, таких як хакерські атаки, шахрайство та інсайдерські витоки, що у свою чергу ускладнює збереження конфіденційних даних компаній.

Висновки. Отож, виходячи з вищевикладеного, можна відмітити, що забезпечення збереження працівником комерційної таємниці роботодавця в трудових правовідносинах є важливим елементом інформаційної безпеки підприємства. Проаналізувавши судову практику та статистику розголошення комерційної таємниці, необхідно затвердити чіткі механізми захисту комерційних таємниць та конфіденційної інформації з метою розвитку та захисту бізнесу від витоку інформації. У разі виникнення суперечок з питань комерційної таємниці або їхніх порушень сторона може звернутися до суду для захисту своїх прав та відшкодування збитків або застосування інших заходів, передбачених законодавством.

Список використаних джерел

1. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 11.02.2025).
2. Кодекс законів про працю України: Закон України від 10.12.1971 № 322-VIII. URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text> (дата звернення: 11.02.2025).
3. Трудовий кодекс України: проект від 25.12.2024 р. URL: https://spo.fpsu.org.ua/wp-content/uploads/2024/12/d1_proekt-trudovogo-kode_su-ukrayiny-25122024.pdf (дата звернення 12.02.2025).
4. Закон України «Про стимулювання розвитку цифрової економіки в Україні» від 15 липня 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text> (дата звернення 11.02.2025).
5. Одовічена Я. А., О. Я. Орловський Комерційна таємниця. Як роботодавцю захистити свої секрети? *Науковий вісник Ужгородського університету: серія: Право*. Ужгород, 2023. Т. 1. Вип. 80. С. 312–318. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/297082/290020> (дата звернення 12.02.2025).
6. Робочі переписки працівників зможуть переглядати: що зміниться в Трудовому кодексі. URL: <https://focus.ua/uk/economics/687261-trudoviy-kodeks-2025-robotavec-mozhe-pereglyadati-perepisku-pracivnika> (дата звернення 12.02.2025).
7. European Union Agency for Cybersecurity (ENISA). *Official website of ENISA*. URL: <https://www.enisa.europa.eu/> (дата звернення 12.02.2025).
8. Зайцева-Калаур І. В., Венгер О. П. Окремі питання гармонізації законодавства України та законодавства ЄС щодо охорони та захисту комерційної таємниці. *Topical Issues of science and practice*. С. 214–221. URL: <http://surl.li/beswc> (дата звернення: 11.02.2025).
9. Північний апеляційний господарський суд справа № 910/1234/23 URL: <http://iplex.com.ua/doc.php?regnum=119557438&red=100003d902074228336e91bb720d8a93361404&d=5> (дата звернення: 11.02.2025).
10. Кривенко С. М. Захист комерційної таємниці у цифрову епоху. *Судова практика і законодавство: матеріали Міжнародної науково-практичної конференції, м. Одеса, 20-21 жовтня 2021 р.* Одеса: ОНУ імені І. І. Мечникова, 2021. С. 134–145.
11. Коваленко О. О. Проблеми охорони комерційної таємниці у трудових відносинах: правовий парадокс в Україні. *Цифрова трансформація прав: ЄС та Україна : матеріали 1-ї міжнар. наук.-практ. конф., м. Харків, 30 квіт. 2024 р.* Харків, 2024. С. 41–44.
12. Держспецзв'язку: Кількість зареєстрованих кібератак минулого року зросла на 62,5 % *Укрінформ*. 2023. URL: <https://www.ukrinform.ua/rubric-technology/3812394-kilkist-zareestrovanih-kiberincidentiv-minulogo-roku-zroslo-na-625-derzspeczvazku.html> (дата звернення 12.02.2025).

13. IBM Security. Cost of a Data Breach Report 2023. URL: <https://www.ibm.com/security/data-breach> (дата звернення 12.02.2025).
14. Нашинець-Наумова А. С. Проблемні питання правового захисту комерційної таємниці в Україні. *Актуальні проблеми права: теорія і практика*. 2019. № 2. С. 85–89.

References

1. *Tsyvilnyi kodeks Ukrainy: Zakon Ukrainy vid 16.01.2003 r.* [Civil Code of Ukraine] № 435-IV. Retrieved from <https://zakon.rada.gov.ua/laws/show/435-15> [in Ukrainian].
2. *Kodeks zakoniv pro pratsiu Ukrainy: [Code of Labor Laws]*. Zakon Ukrainy vid 10.12.1971 № 322-VIII]. Retrieved from <https://zakon.rada.gov.ua/laws/show/322-08#Text> [in Ukrainian].
3. *Trudovyi kodeks Ukrainy: (proekt vid 25.12.2024) r.* [Draft Labor Code of Ukraine]. Retrieved from https://spo.fpsu.org.ua/wp-content/uploads/2024/12/d1_proekt-trudovogo-kode__su-ukrayiny-25122024.pdf (data zvernennia 12.02.2025) [in Ukrainian].
4. *Zakon Ukrainy «Pro stymuliuvannia rozvytku tsyfrovoy ekonomiky v Ukraini» [On stimulating the digital economy in Ukraine]* vid 15 lypnia 2021 roku. Retrieved from <https://zakon.rada.gov.ua/laws/show/1667-20#Text> (data zvernennia 11.02.2025) [in Ukrainian].
5. Odovichenya, Ya. A. & Orlovskiy, O. Ya. (2023). Komertsiiina taiemnytsia. Yak robotodavtsiu zakhystyty svoi sekrety? [Trade secrets. How can an employer protect their secrets?]. *Naukovyi visnyk Uzhhorodskoho universytetu: seriia: Pravo – Scientific Review of Uzhhorod National University. Law*, 1(80), 312-318. Retrieved from <http://visnyk-pravo.uzhnu.edu.ua/article/view/297082/290020> [in Ukrainian].
6. *Robochi perepysky pratsivnykiv zmozhut perehliadaty: shcho zminytsia v Trudovomu kodeksi* [Employees' work correspondence will be able to be viewed: what will change in the Labor Code]. Retrieved from <https://focus.ua/uk/economics/687261-trudoviy-kodeks-2025-robotavec-mozhe-pereglyadati-perepisku-pracivnika> [in Ukrainian].
7. *European Union Agency for Cybersecurity (ENISA)*. Official website of ENISA. Retrieved from <https://www.enisa.europa.eu/> [in Ukrainian].
8. Zaitseva-Kalaur I. V. & Venher O. P. Okremi pytannia harmonizatsii zakonodavstva Ukrainy ta zakonodavstva YeS shchodo okhorony ta zakhystu komertsiiinoi taiemnytsi [Certain issues of harmonization of Ukrainian legislation and EU legislation on the protection and defense of trade secrets] *Topical Issues of science and practice*, 214-221. Retrieved from <http://surl.li/beswc> [in Ukrainian].
9. *Pivnichnyi apeliatsiynyi hospodarskyi sud sprava № 910/1234/23 [Trade secret protection in the digital age: case law and legislation]*. Retrieved from <http://iplex.com.ua/doc.php?regnum=119557438&red=100003d902074228336e91bb720d8a93361404&d=5> [in Ukrainian].
10. Kryvenko, S. M. (2021). Zakhyst komertsiiinoi taiemnytsi u tsyfrovu epokhu: sudova praktyka i zakonodavstvo [Trade secret protection in the digital age: case law and legislation]. *Materialy Mizhnarodnoi naukovo-praktychnoi konferentsii, m. Odesa, 20-21 zhovtnia 2021 r.* Odesa: ONU imeni I. I. Mechnykova, 134-145 [in Ukrainian].
11. Kovalenko, O. O. (2024). Problemy okhorony komertsiiinoi taiemnytsi u trudovykh vidnosynakh: pravovyi paradoks v Ukraini [Problems of protecting trade secrets in labor relations: a legal paradox in Ukraine]. *Tsyfrova transformatsiia prav: YeS ta Ukraina : materialy 1-yi mizhnar. nauk.-prakt. konf., m. Kharkiv, 30 kvit. 2024 r.* Kharkiv, 41-44 [in Ukrainian].
12. *Derzhspetsviazku: Kilkist zareiestrovanykh kiberatak mynulooho roku zroslo na 62,5 % Ukrinform. [State Service for Special Communications: The number of registered cyberattacks increased by 62.5% last year Ukrinform]* (2023). Retrieved from <https://www.ukrinform.ua/rubric-technology/3812394-kilkist-zareiestrovanih-kiberincidentiv-minulogo-roku-zroslo-na-625-derzspeczvazku.html> [in Ukrainian].
13. IBM Security. Cost of a Data Breach Report 2023. Retrieved from <https://www.ibm.com/security/data-breach> [in English].
14. Nashynets-Naumova, A. S. (2019). Problemni pytannia pravovoho zakhystu komertsiiinoi taiemnytsi v Ukraini [Problematic issues of legal protection of trade secrets in Ukraine]. *Aktualni problemy prava: teoriia i praktyka – Actual problems of law: theory and practice*, 2, 85-89 [in Ukrainian].

Стаття надійшла 18.02.2025