Національні інтереси України
3(20) 2026
ISSN 3041-1793 Online
УДК: 347.45/.47
https://doi.org/10.52058/3041-1793-2026-3(20)-1177-1193

Єрофєєнко Лариса Василівна кандидат юридичних наук, доцент, доцент кафедри правового регулювання економіки ХНЕУ ім. С. Кузнеця, м. Харків, https://orcid.org/0000-0001-8436-2065

Чуприна Яніна Олександрівна старший викладач кафедри правового регулювання економіки ХНЕУ ім. С. Кузнеця, м. Харків, https://orcid.org/0000 0002 6645 0296

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ЗА ДОПОМОГОЮ NDA: ПРОБЛЕМИ ДОКАЗУВАННЯ ТА ДОСВІТ DIIA CITI

Анотація: В статті проведено комплексний аналіз ролі та ефективності договору про нерозголошення (NDA) як непоіменованого цивільно-правового інструменту захисту комерційної таємниці (КТ) в Україні, а також розроблено практичні рекомендації щодо його юридично стійкого застосування, зокрема в умовах Diia City та новітньої судової практики Верховного Суду. Встановлено, що NDA є непоіменованим цивільно-правовим договором, правомірність якого базується на принципі свободи договору (ч. 1 ст. 6 ЦКУ).

Обґрунтовано потребу у виділенні NDA в окремий інститут договірного права через його особливі ознаки: необхідність «достатнього рівня довіри» та чинність зобов'язань після припинення співпраці. Доведено, що ефективність NDA залежить від створення «подвійного бар'єру захисту»: чіткої індивідуалізації предмета договору та посилання на внутрішні локальні акти підприємства (Положення про КТ) як доказ вжиття «адекватних заходів» відповідно до ст. 505 ЦКУ та Директиви ЄС 2016/943.

Визначено, що Закон України № 4196-20 вимагає укладання NDA (та NCA) окремо від гіг-контракту. Це забезпечує автономність та юридичну стійкість зобов’язань щодо конфіденційності, незалежно від змішаної правової природи гіг-контракту. Проаналізовано, що найскладнішою проблемою залишається доведення причинно-наслідкового зв'язку при стягненні збитків.

Рекомендовано використовувати комбінований підхід до санкцій (фіксований штраф за факт порушення + відшкодування збитків понад суму штрафу), оскільки штраф спрощує процес стягнення. Проаналізовано прогресивну позицію Верховного Суду (ВС КГС, справи №914/1003/21 та №910/5408/21), який визнав, що відсутність кваліфікованого електронного підпису

ISSN 3041-1793 Online

(КЕП) не є безумовною підставою для відмови у прийнятті електронних доказів (листування в месенджерах, корпоративна пошта). Це підвищує правову силу цифрових слідів.

Для забезпечення належності доказів рекомендовано договірне закріплення допустимості таких каналів комунікації. Сформульовано комплексну стратегію захисту, що включає диференціацію строків дії зобов'язань (наприклад, 3-5 років для ноу-хау) та використання судової заборони як забезпечувального заходу для негайного припинення розголошення.

Ключові слова: договір про нерозголошення (NDA), комерційна таємниця (КТ), ноу-хау, адекватні заходи захисту, непоіменований договір, гіг-контракт, Diia City, електронні докази, фіксований штраф, Верховний Суд (ВС КГС).

Yerofieienko Larysa PhD in Law, Associate Professor, Associate Professor of Department of Legal Regulation of Economics, Simon Kuznets Kharkiv National University of Economics, Kharkiv, https://orcid.org/0000-0001-8436-2065

Chupryna Yanina Senior Lecturer, of Department of Legal Regulation of Economics, Simon Kuznets Kharkiv National University of Economics, Kharkiv, https://orcid.org/0000 0002 6645 0296

ENSURING THE PROTECTION OF COMMERCIAL SECRETS WITH AN NDA: PROBLEMS OF PROOF AND THE EXPERIENCE OF DIIA CITI

Abstract: The article provides a comprehensive analysis of the role and effectiveness of non-disclosure agreements (NDAs) as an unnamed civil law instrument for protecting trade secrets in Ukraine, and develops practical recommendations for their legally sound application, particularly in the context of Diia City and the latest case law of the Supreme Court. It has been established that an NDA is an unnamed civil law agreement, the legality of which is based on the principle of freedom of contract (Part 1 of Article 6 of the Civil Code of Ukraine).

The need to single out NDAs as a separate institution of contract law has been justified due to their special features: the need for a ‘sufficient level of trust’ and the validity of obligations after the termination of cooperation. It has been proven that the effectiveness of an NDA depends on the creation of a ‘double barrier of protection’: clear individualisation of the subject matter of the agreement and reference to the internal local acts of the enterprise (Regulations on the Labour Code) as evidence of the implementation of ‘adequate measures’ in accordance with Article 505 of the Civil Code and EU Directive 2016/943.

ISSN 3041-1793 Online

It has been determined that Law of Ukraine No. 4196-20 requires the conclusion of an NDA (and NCA) separately from the gig contract. This ensures the autonomy and legal stability of confidentiality obligations, regardless of the mixed legal nature of the gig contract. It has been analysed that the most difficult problem remains proving causality when recovering damages.

It is recommended to use a combined approach to sanctions (a fixed penalty for the violation + compensation for damages in excess of the penalty amount), as the penalty simplifies the recovery process. The progressive position of the Supreme Court (VS KGS, cases No. 914/1003/21 and No. 910/5408/21) is analysed, which recognised that the absence of a qualified electronic signature (QES) is not an absolute ground for refusing to accept electronic evidence (correspondence in messengers, corporate mail). This increases the legal force of digital traces.

To ensure the admissibility of evidence, it is recommended to contractually establish the admissibility of such communication channels. A comprehensive protection strategy has been formulated, which includes differentiation of the terms of obligations (e.g., 3-5 years for know-how) and the use of a court injunction as a protective measure to immediately stop disclosure.

Keywords: non-disclosure agreement (NDA), trade secret (TS), know-how, adequate protective measures, unnamed agreement, gig contract, Diia City, electronic evidence, fixed penalty, Supreme Court (SC SC).

Постановка проблеми. Захист інформації, що має комерційну цінність, є фундаментальною умовою успіху сучасного бізнесу. В українському законодавстві цей захист реалізується через інститут комерційної таємниці (КТ), визначення якої закріплено у статті 505 Цивільного кодексу України (ЦКУ). Комерційна таємниця — це інформація, яка є секретною, тобто не є загальновідомою чи легкодоступною для осіб, які зазвичай мають справу з таким видом інформації, має комерційну цінність та була предметом адекватних заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.[1]

Важливою передумовою для ефективного захисту є відповідність національного визначення міжнародним стандартам. Критерії віднесення інформації до нерозкритої, закладені в українському законодавстві, узгоджуються з положеннями Угоди TRIPS та Директивою Європейського Парламенту та Ради (ЄС) 2016/943 від 8 червня 2016 року про захист нерозкритих ноу-хау та ділової інформації.[2] Гармонізація із Директивою ЄС 2016/943 вимагає від власника інформації не просто оголосити її таємною, але й забезпечити наявність вжитих "розумних/адекватних заходів" для збереження її секретності. Ця відповідність є критичною, оскільки дозволяє судовим органам України використовувати європейську судову практику (jurisprudence) при

ISSN 3041-1793 Online

інтерпретації вимог до належного захисту комерційної таємниці. Таким чином, успішне доказування порушення КТ вимагає не лише договірних зобов'язань, але й демонстрації системних організаційно-технічних заходів.

Особливе значення має розмежування комерційної таємниці та суміжних понять, зокрема ноу-хау. «Ноу-хау» (секрети виробництва) часто розглядається як складова комерційної таємниці. Водночас, комерційна таємниця не може існувати поза підприємством, тоді як ноу-хау за своєю природою може існувати окремо. Хоча будь-яке ноу-хау є комерційною таємницею, не всяка комерційна таємниця є ноу-хау.[3] Чітке розуміння цього співвідношення необхідне для правильного формулювання предмета договору про нерозголошення (NDA), особливо в IT-секторі.

Договір про нерозголошення конфіденційної інформації (NDA) в українському правовому полі має цивільно-правову природу, але є непоіменованим договором. Це означає, що спеціальні статті, які б детально регулювали його положення, в Цивільному кодексі України (ЦКУ) відсутні. Його правомірність базується на принципі свободи договору, закріпленому у частині 1 статті 6 ЦКУ, що дозволяє сторонам укладати договори, не передбачені актами цивільного законодавства.

Об'єктом такого договору є конфіденційна інформація — відомості, доступ до яких обмежений фізичною або юридичною особою. При цьому не може бути об'єктом NDA інформація, яка є публічною, загальнодоступною, або відомості про протиправні дії, оскільки доступ до них не може бути обмежений законом.

NDA має особливі ознаки, які виокремлюють його серед інших цивільно-правових угод. По-перше, однією зі специфічних ознак є необхідність наявності «достатнього рівня довіри» між сторонами. По-друге, зміст договору є унікальним, оскільки обов'язок щодо нерозголошення повинен діяти не лише під час співпраці, але й після її припинення, охоплюючи теперішні та майбутні правовідносини. Хоча традиційно NDA є безоплатним та одностороннім (одна сторона, конфіденціал, зобов'язується зберігати обмежений доступ до інформації, отриманої від конфідента), законодавством не заборонена його «оплатність» або встановлення зустрічного обов'язку. Саме ці особливі ознаки — особливий суб'єкт (довіра) та специфічний зміст (тривалість зобов'язань) — вказують на обґрунтовану потребу у виділенні NDA в окремий інститут договірного права для підвищення правової визначеності та ефективності його застосування.[4]

Аналіз останніх досліджень і публікацій. Питання, пов'язані з договірним захистом комерційної таємниці (ноу-хау), зокрема через договір про нерозголошення (NDA), та їхня роль у забезпеченні економічної цінності об'єкта права інтелектуальної власності, є однією з найактуальніших і комерційно значущих тем у сфері права ІВ.

ISSN 3041-1793 Online

Оскільки ефективність захисту комерційної таємниці прямо залежить від вжиття власником адекватних заходів (Ст. 505 ЦКУ), а NDA є основним юридичним механізмом таких заходів, дослідження сфокусовані на цивільно-правовій кваліфікації NDA та практиці стягнення збитків.

Серед фахівців, які активно аналізують правові аспекти захисту комерційної таємниці та договірні механізми (NDA), можна виділити наступних науковців-правознавців:

Олена Олексіївна Підопригора (Київська наукова школа): фокус: теоретичні основи права ІВ. У працях, присвячених загальним проблемам права ІВ, вона обґрунтовує правову природу комерційної таємниці як самостійного об'єкта виключних прав. Це дає теоретичну підставу для висновку, що NDA є інструментом реалізації виключного права власника встановлювати режим доступу та користування цією інформацією.

Олексій Олексійович Слюсарєв: фокус: правова охорона ноу-хау та комерційної таємниці. Він досліджує саме договірні засоби захисту ноу-хау. Наголошує на тому, що NDA є ключовим доказом виконання вимоги про "вжиття адекватних заходів" (ст. 505 ЦКУ). Його роботи важливі для розуміння практичного застосування NDA у судах.

Олена Миколаївна Орлюк (Інститут економіко-правових досліджень НАН України): фокус: комплексні проблеми права ІВ та господарського права. Вона аналізує NDA у контексті господарських договорів (підряду, ліцензійних, спільних підприємств), де відбувається передача ноу-хау. Дослідження стосуються забезпечення балансу інтересів сторін та кваліфікації NDA як адгезійного або самостійного договору.

Ганна Олександрівна Штефан: фокус: цивільно-правовий захист ІВ та недобросовісна конкуренція. Вона досліджує взаємозв'язок між порушенням NDA та актом недобросовісної конкуренції (неправомірне розголошення та використання комерційної таємниці). Це забезпечує подвійний правовий захист.

Борис Андрійович Копилов та інші фахівці з трудового права: фокус: захист комерційної таємниці в трудових відносинах. Їхні роботи розкривають особливості застосування NDA до працівників (зобов'язання про нерозголошення після звільнення) та аналізують допустимість встановлення неустойки за порушення таємниці у внутрішніх документах та трудових договорах.

Міжнародні та порівняльно-правові дослідження, які допомагають зрозуміти глобальну функцію NDA та його ефективність:

Фрідріх-Карл Бейер (Friedrich-Karl Beier). Один із засновників сучасної доктрини захисту ноу-хау в Європі. Його концепція ґрунтується на тому, що захист комерційної таємниці є частиною заборони недобросовісної конкуренції. Якщо особа підписала NDA, а потім розголосила інформацію, це

ISSN 3041-1793 Online

розглядається як порушення довіри та акт недобросовісної конкуренції. NDA створює правовий бар'єр для таких дій.

Роджер Шерман (Roger Sherman). Досліджує економічну цінність ноу-хау. Акцентує на тому, що комерційна таємниця існує доти, доки її економічна цінність забезпечується фізичними та юридичними заходами захисту. NDA розглядається як недорогий, але критично важливий юридичний захід, який дозволяє компаніям зберігати монополію на інформацію, поки патентний захист є недоступним.

Роберт Мергес (Robert Merges). Аналізує взаємодію різних режимів ІВ. Розглядає NDA як договірну альтернативу патентному праву. NDA дозволяє власникам захищати інформацію з необмеженим терміном дії (на відміну від патенту), доки виконуються договірні зобов'язання. Це особливо важливо для рецептів або технологічних процесів, які неможливо або недоцільно патентувати.

Мішін Чой (Minshik Choi). Порівняльний аналіз захисту ноу-хау в різних юрисдикціях (особливо в контексті TRIPS та ЄС). Досліджує, як міжнародні стандарти (ТРІПС) вимагають від держав забезпечити "засоби правового захисту" проти несанкціонованого розголошення. NDA є основним проявом такого "засобу" в приватному праві, що доповнює публічно-правовий захист.

Особлива увага в сучасних дослідженнях приділяється такій тематиці:

1. Договірно-правова природа та кваліфікація NDA: науковий аналіз того, чи є NDA завжди самостійним договором, чи може розглядатися як забезпечувальне зобов'язання (аналогічно неустойці чи поруці), яке застосовується до основного договору (трудового, про надання послуг).

2. Проблеми доведення збитків: дослідження ефективності застосування штрафної неустойки (заздалегідь визначена сума в NDA) порівняно зі складним процесом доведення реальних збитків (втраченої вигоди), спричинених розголошенням комерційної таємниці, як це передбачено нормами ЦКУ.

3. Імплементація міжнародних стандартів: аналіз впливу Директиви ЄС 2016/943 та Угоди ТРІПС на формування вимог до NDA в Україні, особливо щодо встановлення розумних строків дії зобов'язань та винятків із конфіденційності (наприклад, розголошення в інтересах громадськості).

4. Електронний NDA та цифрова конфіденційність: дослідження чинності електронних (digital) NDA, підписаних за допомогою електронних підписів, у контексті захисту комерційної таємниці, яка існує виключно у цифровій формі.

NDA є необхідним, хоча і недостатнім, договірним інструментом для переведення фактичної секретності інформації у категорію юридично захищеної комерційної таємниці.

Ефективність NDA залежить від чіткого визначення об'єкта ІВ та встановлення суворої відповідальності.

ISSN 3041-1793 Online

Договірний захист через NDA є стратегічним вибором, який дозволяє зберегти секретність на довший термін, ніж патент, відповідно до економічної доцільності.

Мета та завдання дослідження. Метою цього дослідження є комплексний аналіз ролі та ефективності договору про нерозголошення (NDA) як непоіменованого цивільно-правового інструменту захисту комерційної таємниці (КТ) в українському правовому полі, а також розробка практичних рекомендацій щодо його юридично стійкого застосування, особливо в умовах цифрової економіки та з урахуванням новітньої судової практики Верховного Суду.

Для досягнення поставленої мети в рамках статті послідовно вирішуються наступні завдання:

Визначити правову природу NDA в українському законодавстві, обґрунтувавши його статус як непоіменованого договору, що базується на принципі свободи договору.

Провести розмежування між поняттями "комерційна таємниця" (КТ) та "ноу-хау" (секрети виробництва) для коректного формулювання предмета NDA, особливо в IT-секторі.

Дослідити ключові вимоги до змісту NDA, які забезпечують його судову стійкість, включаючи необхідність чіткої індивідуалізації предмета захисту.

Обґрунтувати важливість "подвійного бар'єру захисту": посилання в NDA на внутрішні локальні акти підприємства (Положення про КТ) як доказ вжиття "адекватних заходів".

Проаналізувати особливості регулювання строку дії зобов'язань, включаючи диференціацію строків для різних категорій інформації.

Проаналізувати форми відповідальності (цивільно-правова, дисциплінарна, адміністративна, кримінальна), що настає за порушення NDA та розголошення КТ.

Дослідити ефективність комбінованого підходу до санкцій (фіксований штраф vs. відшкодування збитків) та виклики доведення причинно-наслідкового зв'язку при стягненні збитків у суді.

Визначити специфіку регулювання NDA в умовах правового режиму Diia City, зокрема вимогу відокремлення NDA від гіг-контракту та її юридичне значення.

Проаналізувати виклики доведення факту порушення та причинно-наслідкового зв'язку в українському судочинстві.

Дослідити еволюцію позиції Верховного Суду (КГС) щодо допустимості електронних доказів (листування в месенджерах, корпоративна пошта) та їхньої юридичної сили навіть без кваліфікованого електронного підпису (КЕП).

ISSN 3041-1793 Online

Надати комплексну стратегію юридичного захисту КТ.

Сформулювати практичні рекомендації щодо істотних умов NDA та превентивних заходів (організаційних, договірних, процесуальних) для забезпечення максимальної ефективності захисту.

Виклад основного матеріалу дослідження. Ефективність NDA в українському судочинстві прямо залежить від якості його формулювань, особливо у частині визначення предмета захисту. Ключовим елементом є чітка та однозначна конкретизація, яка саме інформація вважається конфіденційною або комерційною таємницею. Це можуть бути бази даних клієнтів, технічні рішення, ноу-хау, маркетингові стратегії, фінансові показники тощо.[1] Чим точніше визначено предмет захисту, тим вищий шанс на успішне застосування договору у разі порушення.[1]

Покладання на загальні формулювання або відсутність деталізації істотно ускладнює процес доведення порушення. Для створення юридично стійкого захисту необхідно, щоб перелік відомостей, які становлять КТ, був формально зафіксований у внутрішньому локальному акті підприємства, наприклад, у Положенні про комерційну таємницю. Зазначення складу та обсягу таких відомостей є прямим обов'язком суб'єкта господарювання відповідно до закону.[5] Якщо NDA містить лише загальне посилання на "комерційну таємницю", суд може вимагати від позивача доказів того, що інформація відповідала критеріям КТ на момент розголошення. Натомість, прийняття внутрішніх процедур, визначення кола питань, ознайомлення з положеннями співробітників під підпис[6] та посилання на цей локальний акт у NDA створює потужну презумпцію вжиття "адекватних заходів". Цей "подвійний бар’єр захисту" критично зменшує простір для відповідача оскаржувати статус інформації як таємної у суді.

Строк дії зобов'язань щодо нерозголошення є важливим аспектом NDA. Українське законодавство надає сторонам свободу у його визначенні. На практиці, термін дії договору про нерозголошення зазвичай встановлюється в середньому на 3 роки більше, ніж основний період співробітництва між сторонами.[7] Зобов'язання щодо нерозголошення, як правило, мають залишатися чинними навіть після припинення основних договірних або трудових відносин.[1]

Проте сторони повинні уникати встановлення надмірно тривалих або безстрокових зобов'язань. Судова практика демонструє, що суди можуть визнати такі строки необґрунтованими. Рекомендованим підходом є диференціація строків для різних категорій інформації. Наприклад, для технологічних рішень та ноу-хау, що мають довготривалу цінність, може бути встановлений триваліший строк (3-5 років), тоді як для менш стійких до часу активів, таких як маркетингові плани або фінансові показники, може бути

ISSN 3041-1793 Online

визначений коротший термін (1-2 роки).[1]

Відповідальність за порушення умов NDA може мати кілька форм, включаючи цивільно-правову, дисциплінарну, адміністративну та кримінальну.[8] З погляду цивільно-правового захисту, найефективнішим є комбінований підхід до санкцій, що поєднує фіксований штраф та відшкодування збитків, заподіяних розголошенням.[1]

Фіксований штраф (неустойка) виконує функцію потужного стримуючого фактора і значно спрощує процес стягнення, оскільки вимагає доведення лише факту порушення, а не складного обрахунку розміру збитків та причинно-наслідкового зв'язку.[9] Однак необхідно, щоб розмір штрафних санкцій був розумним та обґрунтованим. Суди мають право зменшити надмірні санкції, якщо вони вважатимуться несправедливими або непропорційними до порушення.[1]

Відшкодування збитків (ст. 22 ЦК України) вимагає доведення факту завдання реальних збитків або упущеної вигоди та прямого причинно-наслідкового зв’язку між розголошенням та шкодою.[8] Цей аспект залишається найскладнішим для доведення в українській судовій практиці, оскільки необхідно довести, що, наприклад, розірвання комерційного договору сталося саме внаслідок розголошення КТ.[9] Окрім фінансових санкцій, в NDA слід передбачати детальні вимоги щодо способів обробки інформації, обмежувати доступ до критичних даних та фіксувати факт ознайомлення з цими політиками підписом кожної сторони.[10]

Створення правового режиму Diia City та ухвалення Закону України «Про стимулювання розвитку цифрової економіки в Україні» (№ 4196-20) запровадило специфічні вимоги до оформлення договірних відносин у сфері IT, включаючи NDA. Цей режим, що замінює традиційне застосування законодавства в сфері господарської діяльності, забезпечує інноваційний підхід до захисту інтелектуальної власності.

Ключовою особливістю режиму Diia City є чітке юридичне розділення гіг-контракту та зобов’язань щодо конфіденційності. Гіг-контракт є змішаним договором, що поєднує ознаки цивільно-правового договору (виконання конкретного завдання) та трудового договору (соціальні гарантії). Відповідно до Закону № 4196-20, договір про нерозголошення (NDA) та Угода про неконкуренцію (NCA) повинні укладатися окремо від гіг-контракту і не можуть бути включені до його змісту.[11]

Це розділення має важливу юридичну мету: воно забезпечує автономність зобов’язань щодо конфіденційності та неконкуренції, відокремлюючи їх від змішаної правової природи гіг-контракту. Таким чином, порушення конфіденційності регулюватиметься незалежно від припинення чинності самого гіг-контракту. Якщо резидент Diia City має намір укласти NDA та/або

ISSN 3041-1793 Online

NCA з гіг-спеціалістом, гіг-контракт повинен містити пряме посилання на те, що положення про нерозголошення та/або неконкуренцію регулюються додатковими, окремими угодами.[11]

Закон про Diia City встановлює спеціальний та чіткий режим щодо інтелектуальної власності: об'єкти прав інтелектуальної власності (ІВ), створені в рамках гіг-контракту, за замовчуванням належать резиденту Diia City (замовнику).[11]

У цьому контексті, NDA відіграє роль додаткового, але незамінного інструмента. Він захищає не самі об'єкти ІВ (авторське право), а ту критично важливу інформацію (ноу-хау, технологічні секрети, бізнес-стратегії), яка супроводжує процес створення ІВ і може не мати формального статусу об'єкта авторського чи патентного права.[3] Спеціальні вимоги Закону 4196-20 щодо NDA/NCA сигналізують судам про пріоритет захисту конфіденційності в ІТ-секторі. Це дозволяє стверджувати, що справи резидентів Diia City, належним чином оформлені відповідно до цього закону, потенційно мають вищі шанси на успіх у судових спорах порівняно з традиційними трудовими чи господарськими суперечками. Режим Diia City є законодавчим актом, що підвищує правову визначеність і вимагає високого рівня договірної дисципліни.

Практична ефективність NDA часто наштовхується на значні перешкоди у процесі судового доведення. Історично суди вимагали довести не лише факт доступу особи до комерційної таємниці (наприклад, через корпоративну систему[7]) або факт передачі файлів, але й необхідність доведення факту неправомірного використання цієї інформації відповідачем у власних цілях.[6]

Особливо складною є проблема стягнення збитків. Хоча неправомірне розголошення, збирання або використання комерційної таємниці може розглядатися як випадок недобросовісної конкуренції (Глава 4 ЗУ "Про захист від недобросовісної конкуренції"), доведення причинно-наслідкового зв'язку є надзвичайно важким. Необхідно довести, що такі негативні обставини, як розірвання комерційного договору чи накладення штрафних санкцій на власника відомостей, відбулися саме внаслідок розголошення.[9] Наприклад, у справі, де співробітник здійснив несанкціонований доступ до комерційної таємниці під час відпустки по догляду за дитиною, суд відмовив у позові через ненадання належного доказу про неправомірне використання відповідачем КТ у власних цілях.[7] Аналогічно, у справі, що розглядалася ВС у 2019 році, касаційну скаргу було залишено без задоволення, оскільки позивач не довів факт розголошення і не надав доказів порушення прав, тобто незаконного використання КТ відповідачем.[6]

Одним із найбільш значущих змінних факторів у судовій практиці щодо NDA є прогресивна еволюція позиції Верховного Суду (ВС) щодо допустимості електронних доказів. Раніше, у справах про порушення конфіден-

ISSN 3041-1793 Online

ційності, апеляційні інстанції могли відмовляти у задоволенні позовів, мотивуючи це тим, що електронні листи або інше листування не містять електронного підпису, що ідентифікує особу, і тому не вважаються належними чи достовірними доказами.[9]

Проте новітня практика Верховного Суду у складі суддів об'єднаної палати Касаційного господарського суду (КГС) демонструє кардинальну зміну. У постанові від 15.07.2022 у справі №914/1003/21 та у справі №910/5408/21, ВС КГС визнав передчасними висновки судів про те, що електронні докази (листування в месенджері Telegram, електронна пошта, відомості з систем управління проектами Jira чи середовища обміну результатами GitLab) не відповідають вимогам належності та допустимості лише через відсутність кваліфікованого електронного підпису (КЕП).[12]

Суд обґрунтував, що чинне законодавство визначає обов'язковість використання КЕП лише для певних офіційних документів, але це не поширюється на комерційне, ділове чи особисте листування між приватними особами (якщо інше не встановлено домовленістю сторін). У таких відносинах презюмується ідентифікація особи, оскільки малоймовірно, що хтось інший, окрім цієї особи, міг отримати чи відповісти на повідомлення з урахуванням його змісту та обговорюваних деталей. Верховний Суд використовував для обґрунтування цієї позиції навіть міжнародні джерела, зокрема Керівні принципи Комітету Міністрів Ради Європи щодо онлайн вирішення спорів.[12]

Ця зміна позиції має прямий вплив на ефективність NDA, особливо в IT-середовищі. Послаблення вимог до КЕП у комерційних спорах збільшує правову силу цифрових слідів. Компанії можуть успішно використовувати дані корпоративних систем та листування як ключові докази порушення. Це вимагає від компаній змістити фокус з суто формальної документації на забезпечення технічної фіксації цілісності даних та метаданих, що підтверджують авторство та час розголошення.[13]

Для забезпечення належності електронних доказів у справах про порушення NDA, позивачу необхідно завчасно подбати про їх правильну фіксацію. Типовими доказами порушення конфіденційності виступають: скріншоти електронного листування, аудіо- чи відеозаписи, а також відомості про витоки даних у загальнодоступних джерелах.[10]

Превентивні заходи для забезпечення доказової бази включають:

Договірне закріплення: Включення до тексту NDA положення про те, що сторони погоджуються визнавати листування у конкретних корпоративних месенджерах, системах управління проектами (Jira, GitLab, корпоративна пошта) як допустимий доказ, незалежно від наявності КЕП.[12]

Технічна фіксація: Регулярне оновлення політик щодо поводження з інформацією та обмеження доступу до критичних даних.[10]

ISSN 3041-1793 Online

Формальне ознайомлення: Фіксація факту ознайомлення з NDA та внутрішніми положеннями про КТ підписом кожної сторони.[10]

Для наочності, ключові аспекти допустимості електронних доказів, згідно з практикою ВС КГС, представлені у таблиці.

Таблиця 1: Аналіз допустимості електронних доказів у справах про порушення NDA (за практикою ВС КГС)

Тип Доказу	Проблема (традиційний підхід)	Актуальна позиція ВС КГС	Практична рекомендація щодо фіксації
Email, Telegram, Jira/GitLab	Відсутність кваліфікованого електронного підпису (КЕП)	Висновки про недопустимість через відсутність КЕП передчасні. Ідентифікація автора презюмується через зміст та обговорювані деталі.[12]	Зафіксувати метадані, цілісність даних. Чітко визначити в NDA ці канали як допустимі засоби комунікації.[12]
Корпоративні файли/доступ до систем	Недоведеність факту використання у власних цілях	Необхідно довести не лише доступ, але й причинно-наслідковий зв'язок між розголошенням та заподіяними збитками.[6]	Встановити технічний контроль (логінги) вивантаження інформації та забезпечити докази подальшого використання чи передачі третім особам.

При порушенні умов NDA позивач може вимагати притягнення відповідача до цивільно-правової відповідальності, яка реалізується переважно у двох формах: стягнення збитків та стягнення штрафу (неустойки).

Стягнення збитків (ст. 22, 1166 ЦК України)[8] вимагає доведення факту та розміру реальних збитків (матеріальної шкоди) або упущеної вигоди. Це найскладніша форма захисту, оскільки вимагає складного економічного обґрунтування та доведення прямого причинно-наслідкового зв'язку між діями порушника та фінансовими втратами компанії.[9]

Фіксований штраф є значно ефективнішим інструментом. Штраф, як форма неустойки, вимагає доведення лише самого факту порушення зобов'язання, незалежно від доведення збитків. Штрафні санкції слугують превентивним заходом і спрощують судовий процес стягнення. Важливо, щоб у NDA було передбачене поєднання стягнення фіксованого штрафу за факт розголо-

ISSN 3041-1793 Online

шення та право на додаткове відшкодування збитків понад суму штрафу, якщо збитки перевищують цю суму. При цьому, розмір штрафу повинен бути розумним, оскільки надмірні санкції можуть бути зменшені судом відповідно до принципу справедливості.[1]

Окрім цивільно-правової, порушення NDA та розголошення КТ може мати інші юридичні наслідки:

Дисциплінарна відповідальність: Застосовується до працівників (ст. 147 Кодексу законів про працю України). Для посадових осіб товариств з обмеженою відповідальністю, порушення конфіденційності може бути підставою для розірвання договору без виплати компенсації, відповідно до частин 7 та 8 статті 42 Закону України «Про товариства з обмеженою та додатковою відповідальністю».[8]

Адміністративна відповідальність: Передбачена за незаконне використання комерційної таємниці, зокрема у формі недобросовісної конкуренції (ч. 3 ст. 164-3 КУпАП).[8]

Кримінальна відповідальність: Кримінальний кодекс України передбачає відповідальність за незаконне збирання, використання або розголошення комерційної або банківської таємниці (ст. 231, ст. 232 КК України).[8]

Для власника КТ критично важливим є не лише стягнення відповідальності, а й негайне припинення подальшого неправомірного використання або розголошення інформації. Власник КТ має виключне право перешкоджати такому неправомірному розголошенню, збиранню чи використанню.[14]

У судовому процесі як забезпечувальний захід може застосовуватися судова заборона (заборона або обмеження певних дій). Це може бути заборона відповідачу використовувати, розголошувати або передавати КТ третім особам до моменту вирішення спору по суті.[14] Такі заходи є особливо актуальними, коли існує ризик незворотної шкоди від продовження розголошення.

Водночас, існує потреба у вдосконаленні процесуального законодавства щодо захисту КТ під час самого судового розгляду. Для запобігання подальшому розголошенню інформації, що є предметом спору, необхідне запровадження правил, спрямованих на обмеження доступу до матеріалів справи, які містять комерційну таємницю, визначаючи вузьке коло осіб, які можуть ознайомитися з такими файлами.[15]

Висновки. Проведене дослідження підтверджує, що договір про нерозголошення (NDA) в Україні є дієвим, хоча й непоіменованим, цивільно-правовим інструментом захисту комерційної таємниці. Проте його ефективність є не автономною, а залежить від трьох ключових факторів:

Якість організаційних заходів: необхідність чіткого визначення КТ у внутрішніх локальних актах (Положеннях), що створює презумпцію вжиття «адекватних заходів» відповідно до національних та європейських стандартів.

ISSN 3041-1793 Online

Договірна індивідуалізація: створення NDA з деталізацією предмета, диференційованими строками дії та розумним поєднанням штрафних санкцій та відшкодування збитків.[1]

Технічна доказова база: здатність позивача зібрати та належним чином зафіксувати цифрові сліди порушення. Прогресивна практика Верховного Суду щодо допустимості електронних доказів (навіть без КЕП) значно підвищила шанси на успіх у справах, де використовуються дані корпоративних систем.[12]

Спеціальний правовий режим, встановлений Законом України № 4196-20 для резидентів Diia City, підкреслює пріоритет захисту конфіденційності в IT-секторі та вимагає формального відокремлення NDA від гіг-контракту, забезпечуючи юридичну стійкість зобов'язань.

Для забезпечення максимальної ефективності захисту комерційної таємниці через NDA рекомендується впровадити комплексну стратегію, що охоплює організаційний, договірний та процесуальний блоки.

Таблиця 2: Рекомендовані істотні умови та заходи для ефективного NDA в IT-секторі

Блок	Ключовий Захід	Юридичне Значення
Організаційний	Затвердження детального Положення про КТ та ноу-хау	Доведення "адекватних заходів" захисту, необхідних для визнання інформації комерційною таємницею.[1]
Організаційний	Ознайомлення співробітників/контрагентів з Положенням про КТ під підпис	Усунення можливості заперечення обізнаності щодо статусу інформації.[6]
Договірний	Чітка індивідуалізація предмета NDA	Зменшення простору для маневру відповідача у суді, уникнення загальних формулювань.[1]
Договірний	Диференціація строків дії зобов'язань	Забезпечення розумності та обґрунтованості термінів, особливо для ноу-хау (3-5 років).[1]
Договірний	Поєднання фіксованого штрафу та відшкодування збитків	Спрощення процесу стягнення відповідальності за факт порушення та збереження права на компенсацію фактичних втрат.[1]

ISSN 3041-1793 Online

Блок	Ключовий Захід	Юридичне Значення
Процесуальний	Закріплення допустимості електронних доказів у договорі	Попереднє погодження використання листування (email, месенджери, Jira) як допустимого доказу, відповідно до практики ВС КГС.[12]
Процесуальний	Впровадження системи логування та фіксації метаданих	Забезпечення належності та достовірності цифрових доказів (ідентифікація автора, час, цілісність).[10]
Процесуальний	Використання судових заборон як забезпечувального заходу	Негайне припинення подальшого розголошення КТ у ході судового розгляду.[14]

Література:

1. NDA в Україні: як ефективно захистити конфіденційну інформацію - RED LAWYERS, 2025, – [Електронний ресурс]. – Режим доступу: https://redlawyers.ua/poslugy/nda-v-ukrayini-yak-efektyvno-zahystyty-konfidentsijnu-informatsiyu/

2. Н. П. Капітаненко. Захист комерційної таємниці промислового підприємства в умовах цифрової трансформації. - Liha-Pres, 2023, – [Електронний ресурс]. – Режим доступу: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/download/225/5504/12235-1?inline=1

3. Порівняльний аналіз понять "ноу-хау" і "комерційна таємниця". 2009. Мего-Інфо — Юридичний портал №1. – [Електронний ресурс]. – Режим доступу: https://mego.info/%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB/%C2%A7-2-%D0%BF%D0%BE%D1%80%D1%96%D0%B2%D0%BD%D1%8F%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7-%D0%BF%D0%BE%D0%BD%D1%8F%D1%82%D1%8C-%D0%BD%D0%BE%D1%83-%D1%85%D0%B0%D1%83-%D1%96-%D0%BA%D0%BE%D0%BC%D0%B5%D1%80%D1%86%D1%96%D0%B9%D0%BD%D0%B0-%D1%82%D0%B0%D1%94%D0%BC%D0%BD%D0%B8%D1%86%D1%8F?page=1

4. Договір про захист комерційної інформації (про конфіденційність). Форма типового документа. Договір. Документ n 0084697-00 від 01.01.2000. Законодавство, Верховна Рада України. URL: https://zakon.rada.gov.ua/rada/show/n0084697-00#Text

5. Комерційна таємниця Вашого бізнесу: як захистити її у відносинах із діловими партнерами - Юридична Газета, 2020. – [Електронний ресурс]. – Режим доступу: https://yur-gazeta.com/dumka-eksperta/komerciyna-taemnicya-vashogo-biznesu-yak-zahistiti-yiyi-u-vidnosinah-iz-dilovimi-partnerami.html

6. Корисні поради при захисті прав на комерційну таємницю - юридична фірма Asters, 2019. – [Електронний ресурс]. – Режим доступу: https://www.asterslaw.com/ua/press_center/publications/useful_tips_for_protecting_trade_secrets_in_ukraine/

7. Чи працює NDA в Україні: розвіюємо міфи - АРМАДА, 2025, – [Електронний ресурс]. – Режим доступу: https://armada.law/blog/chy-pratsyue-nda-v-ukrayini/

ISSN 3041-1793 Online

8. Практичні аспекти захисту комерційної таємниці в діяльності ТОВ: адвокат Надія Тарасова. Вища школа адвокатури НААУ, 2023,– [Електронний ресурс]. – Режим доступу: https://www.hsa.org.ua/blog/prakticni-aspekti-zaxistu-komerciinoyi-tajemnici-v-diialnosti-tov-advokat-nadiia-tarasova

9. Чи можуть IT-компанії покарати співробітників через суд за порушення умов NDA. Розбираємо кілька судових справ. DOU, 2021. – [Електронний ресурс]. – Режим доступу: https://dou.ua/lenta/articles/breach-of-nda/

10. Відповідальність за порушення договору про нерозголошення конфіденційної інформації в Україні. - FastDoc. 2025, – [Електронний ресурс]. – Режим доступу: https://fastdoc.com.ua/ua/post/105_vidpovidalnist-za-porushennya-dogovoru-pro-nerozgoloshennya-konfidenciynoyi-informaciyi-v-ukrayini/

11. Гіг-контракт: що це, особливості та відмінності від ФОПу. АО Бачинський та Партнери, 2025, – [Електронний ресурс]. – Режим доступу: https://legalaid.ua/ua/shho-take-gig-kontrakt/

12. Верховний Суд: відсутність кваліфікованого електронного підпису не зумовлює недостовірність певних даних в електронній формі і недостовірність електронного доказу. Юрлайн. 2022, – [Електронний ресурс]. – Режим доступу: https://jurline.ua/blog/verhovnij-sud-vidsutnist-kvalifikovanogo-elektronnogo-pidpisu-ne-zumovlyuye-nedostovirnist-pevnih-danih-v-elektronnij-formi-i-nedostovirnist-elektronnogo-dokazu

13. Відсутність кваліфікованого електронного підпису не зумовлює недостовірність певних даних в електронній формі і недостовірність електронного доказу, — Верховний Суд. - Територіальне управління Державної судової адміністрації України у Тернопільській області. Судова влада України, 2022, – [Електронний ресурс]. – Режим доступу: https://te.court.gov.ua/tu20/pres-centr/news/1317863/

14. Захист комерційної таємниці підприємства. Бізнес. Ліга.Закон, 2024, – [Електронний ресурс]. – Режим доступу: https://biz.ligazakon.net/analitycs/230936_zakhist-komertsyno-tamnits-pdprimstva

15. Катерина Дюкарєва-Бержаніна. Захист комерційної таємниці в судовому провадженні. 2020, – [Електронний ресурс]. – Режим доступу: http://pgp-journal.kiev.ua/archive/2020/3/4.pdf

References:

1. NDA v Ukraini: yak efektyvno zakhystyty konfidentsiinu informatsiiu (2025). [NDAs in Ukraine: how to effectively protect confidential information] - RED LAWYERS. URL: https://redlawyers.ua/poslugy/nda-v-ukrayini-yak-efektyvno-zahystyty-konfidentsijnu-informatsiyu/ [in Ukrainian]

2. N. P. Kapitanenko., (2023). Zakhyst komertsiinoi taiemnytsi promyslovoho pidpryiemstva v umovakh tsyfrovoi transformatsii. [Protecting the trade secrets of industrial enterprises in the context of digital transformation]. Liha-Pres. URL: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/download/225/5504/12235-1?inline=1 [in Ukrainian]

3. Porivnialnyi analiz poniat "nou-khau" i "komertsiina taiemnytsia". (2009). [Comparative analysis of the concepts of ‘know-how’ and ‘trade secret’] Meho-Info — Yurydychnyi portal №1. URL: https://mego.info/%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB/%C2%A7-2-%D0%BF%D0%BE%D1%80%D1%96%D0%B2%D0%BD%D1%8F%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7-%D0%BF%D0%BE%D0%BD%D1%8F%D1%82%D1%8C-%D0%BD%D0%BE%D1%83-%D1%85%D0%B0%D1%83-%D1%96-%D0%BA%D0%BE%D0%BC%D0%B5%D1%80%D1%86%D1%96%D0%B9%D0%BD%D0%B0-%D1%82%D0%B0%D1%94%D0%BC%D0%BD%D0%B8%D1%86%D1%8F?page=1 [in Ukrainian]

ISSN 3041-1793 Online

4. Dohovir pro zakhyst komertsiinoi informatsii (pro konfidentsiinist). (2000). [Agreement on the protection of commercial information (confidentiality).] Forma typovoho dokumenta. Dohovir. Dokument n 0084697-00 vid 01.01.2000. Zakonodavstvo, Verkhovna Rada Ukrainy. URL: https://zakon.rada.gov.ua/rada/show/n0084697-00#Text [in Ukrainian]

5. Komertsiina taiemnytsia Vashoho biznesu: yak zakhystyty yii u vidnosynakh iz dilovymy partneramy. (2020). [Your business's trade secrets: how to protect them in your dealings with business partners]- Yurydychna Hazeta, URL: https://yur-gazeta.com/dumka-eksperta/komerciyna-taemnicya-vashogo-biznesu-yak-zahistiti-yiyi-u-vidnosinah-iz-dilovimi-partnerami.html [in Ukrainian]

6. Korysni porady pry zakhysti prav na komertsiinu taiemnytsiu. (2019). [Useful tips for protecting trade secret rights] - yurydychna firma Asters. URL: https://www.asterslaw.com/ua/press_center/publications/useful_tips_for_protecting_trade_secrets_in_ukraine/ [in Ukrainian]

7. Chy pratsiuie NDA v Ukraini: rozviiuiemo mify (2025). [Does NDA work in Ukraine: dispelling myths]. - ARMADA, URL: https://armada.law/blog/chy-pratsyue-nda-v-ukrayini/ [in Ukrainian]

8. Praktychni aspekty zakhystu komertsiinoi taiemnytsi v diialnosti TOV: advokat Nadiia Tarasova. (2023). [Practical aspects of protecting trade secrets in the activities of LLCs: lawyer Nadiya Tarasova]. - Vyshcha shkola advokatury NAAU. URL: https://www.hsa.org.ua/blog/prakticni-aspekti-zaxistu-komerciinoyi-tajemnici-v-diialnosti-tov-advokat-nadiia-tarasova [in Ukrainian]

9. Chy mozhut IT-kompanii pokaraty spivrobitnykiv cherez sud za porushennia umov NDA. Rozbyraiemo kilka sudovykh sprav. (2021). [Can IT companies punish employees through the courts for violating the terms of an NDA? We examine several court cases.] - DOU, 2021. URL: https://dou.ua/lenta/articles/breach-of-nda/ [in Ukrainian]

10. Vidpovidalnist za porushennia dohovoru pro nerozgholoshennia konfidentsiinoi informatsii v Ukraini. (2025). [Liability for breach of confidentiality agreements in Ukraine.] FastDoc. URL: https://fastdoc.com.ua/ua/post/105_vidpovidalnist-za-porushennya-dogovoru-pro-nerozgoloshennya-konfidenciynoyi-informaciyi-v-ukrayini/ [in Ukrainian]

11. Hih-kontrakt: shcho tse, osoblyvosti ta vidminnosti vid FOPu. (2025). [Gig contract: what it is, features and differences from an individual entrepreneur] - AO Bachynskyi ta Partnery, URL: https://legalaid.ua/ua/shho-take-gig-kontrakt/ [in Ukrainian]

12. Verkhovnyi Sud: vidsutnist kvalifikovanoho elektronnoho pidpysu ne zumovliuie nedostovirnist pevnykh danykh v elektronnii formi i nedostovirnist elektronnoho dokazu. (2022). [Supreme Court: the absence of a qualified electronic signature does not render certain data in electronic form unreliable or electronic evidence inadmissible]. Yurlain. URL: https://jurline.ua/blog/verhovnij-sud-vidsutnist-kvalifikovanogo-elektronnogo-pidpisu-ne-zumovlyuye-nedostovirnist-pevnih-danih-v-elektronnij-formi-i-nedostovirnist-elektronnogo-dokazu [in Ukrainian]

13. Vidsutnist kvalifikovanoho elektronnoho pidpysu ne zumovliuie nedostovirnist pevnykh danykh v elektronnii formi i nedostovirnist elektronnoho dokazu, — Verkhovnyi Sud. (2022). [The absence of a qualified electronic signature does not invalidate certain data in electronic form or electronic evidence, according to the Supreme Court]. Terytorialne upravlinnia Derzhavnoi sudovoi administratsii Ukrainy u Ternopilskii oblasti. Sudova vlada Ukrainy. URL: https://te.court.gov.ua/tu20/pres-centr/news/1317863/ [in Ukrainian]

14. Zakhyst komertsiinoi taiemnytsi pidpryiemstva. (2024). [Protection of commercial secrets of the enterprise]. Biznes. Liha.Zakon. URL: https://biz.ligazakon.net/analitycs/230936_zakhist-komertsyno-tamnits-pdprimstva [in Ukrainian]

15. Kateryna Diukarieva-Berzhanina., (2020). Zakhyst komertsiinoi taiemnytsi v sudovomu provadzhenni. [Protection of trade secrets in court proceedings]. URL: http://pgp-journal.kiev.ua/archive/2020/3/4.pdf [in Ukrainian]

Дата першого надходження статті до видання: 27.02.2026
Дата прийняття статті до друку після рецензування: 13.03.2026