**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ЮРИДИЧНИЙ ФАКУЛЬТЕТ**

**кафедра адміністративного та господарського права**

**Кваліфікаційна робота**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_магістра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(рівень вищої освіти)

на тему Актуальні проблеми правового регулювання відносин обігу конфіденційної інформації в ІТ сфері в Україні та зарубіжних країнах: компаративний аналіз.

Виконав: студент магістратури, групи\_\_\_\_\_\_

спеціальності

спеціальності 081 право

Яковенко Є.Є.

Керівник доцент, к.ю.н. Кукурудз Р.О.

Рецензент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя – 2020

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

Факультет\_\_\_юридичний \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кафедра\_\_адміністративного та господарського права \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рівень вищої освіти\_\_\_магістр\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Спеціальність \_\_\_\_\_081 право\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(шифр і назва)

**ЗАТВЕРДЖУЮ**

Завідувач кафедри\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_року

**З А В Д А Н Н Я**

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Яковенко Єлизавета Євгенівна\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище, ім’я, по батькові)

1. Тема роботи (проекту) Актуальні проблеми правового регулювання відносин обігу конфіденційної інформації в ІТ сфері в Україні та зарубіжних країнах: компаративний аналіз.

керівник роботи Кукурудз Р.О.,

доцент кафедри адміністративного та господарського права, к.ю.н.

затверджені наказом ЗНУ від «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_\_року №\_\_\_\_\_\_\_\_\_\_\_\_

1. Строк подання роботи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Вихідні дані до роботи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Консультанти розділів роботи

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  консультанта | Підпис, дата | |
| завдання  видав | завдання  прийняв |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Дата видачі завдання\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №  з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
| 1. | Затвердження теми роботи в результаті опрацювання та обговорення з науковим керівником у відповідності до магістерської програми |  |  |
| 2. | Узгодження проекту плану та завдання до магістерської роботи |  |  |
| 3. | Збір та вивчення джерел інформації для написання дипломної роботи; |  |  |
| 4. | Складання плану дипломної роботи |  |  |
| 5. | Написання першого розділу |  |  |
| 6. | Попередній звіт керівника і студента про хід виконання завдання на дипломну роботу на кафедрі |  |  |
| 7. | Складання схематичних матеріалів |  |  |
| 8. | Збір статистичних даних |  |  |
| 9. | Написання вступу, висновків |  |  |
| 10. | Виправлення зауважень |  |  |
| 11. | Підготовка презентації та захист роботи |  |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

Керівник роботи (проекту) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

**Нормоконтроль пройдено**

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Яковенко Є.Є. Актуальні проблеми правового регулювання відносин обігу конфіденційної інформації в ІТ сфері в Україні та зарубіжних країнах: компаративний аналіз. Запоріжжя. 2020. 94 с.

Кваліфікаційна робота складається зі 94 сторінок, містить 98 джерел використаної інформації.

Стрімкий розвиток IT-сфери передбачає вдосконалення форм та методів регулювання трудових відносин з IT компаніями. Постає питання про способи захист конфіденційної інформаціїї, що використовується найманими співробітниками компанії у ході робочого процесу та поза його меж. Одним з таких способів форм захисту інформації, який нині застосовується та набуває все більшої актуальності – Договір про неразголошення конфіденційної інформації.

Як показує зарубіжний досвід, важливість даного Договору в умовах високої конкуренції в IT-сфері незаперечно потребує детального вивчення і саме активне використання даних договорів зумовлює актуальність обраної теми та необхідність проведення глибокого аналізу правового регулювання конфіденційної інформацї в IT-сфері як в Україні, так і в зарубіжних країнах і вироблення на основі цього рекомендацій та пропозицій щодо вдосконалення законодавства, яке регулює дане питання.

Метою кваліфікаційної роботи є порівняльний аналіз та детальне дослідження особливостей захисту конфіденційної інформації в IT сфері в Україні та зарубіжних країнах, розгляд таких аспектів, як правове регулювання сфери інформаційних технологій в розрізі збереження конфіденційної інформації та окреслити перспектив розвитку даної індустрії в Україні та зарубіжних країнах.

Об’єктом кваліфікаційної роботи є захист конфіденційної інформації в IT сфері в Україні та зарубіжних країнах.

Предметом правові норми в Україні та зарубіжних країнах, що регулюють обіг конфіденційної інформації, її захист в Україні та зарубіжних країнах.

Методологічнуоснову роботи складають сукупність загальнонаукових принципів і підходів та спеціально-наукових класифікацій конфіденційної інформації, законодавча база України, використання яких дало змогу отримати науково-обґрунтовані результати. Для проведення дослідження будуть застосовані такі загальнонаукові методи як: аналіз і порівняння.

Теоретико-методологічною основою дослідження в роботі є компаративний аналіз та класифікування, застосування яких сприяло розглянути актуальність правового регулювання обігу конфіденційної інформації в Україні та зарубіжних країнах, виокремити та детально проаналізувати комерційну таємницю, як підвид конфіденційної таємниці. Аналіз і порівняння дозволили вивчити питання неразголошення кофіденційної інформації в IT-сфері та договору про конфіденційність в Україні та зарубіжних країнах.

Конфіденційна інформація, it-право, комерційна таємниця, Договір про конфіденційність, інформаційна безпека, Сфера інформаційної безпеки, NON DISCLOSURE AGREEMENT, НЕДОБРОСОВІСНА КОНКУРЕНЦІЯ, ПОЛОЖЕННЯ ПРО НЕКОНКУРЕНЦІЮ.

SUMMARY

Yakovenko Y.Y. Actual problems of legal regulation of relations of the circulation of confidential information in the IT field in Ukraine and foreign countries: comparative analysis. Zaporozhye. 2020. 94 p.

Qualifying work consists of 94 pages, contains 98 sources of information used.

The rapid development of the IT sphere implies the improvement of forms and methods of regulation of labor relations with IT companies. The question is how to protect sensitive information used by employees of the company during the workflow and beyond. One such form of protection of information that is currently in use and is becoming increasingly relevant is the Non-Disclosure Agreement.

As foreign experience shows, the importance of this Agreement in the highly competitive IT sphere undoubtedly requires detailed study and the active use of these Agreements determines the relevance of the chosen topic and the need for a thorough analysis of the legal regulation of confidential information in the IT sphere, both in Ukraine and in the foreign countries, and developing on this basis recommendations how to improve the legislation governing this issue.

The aim of the thesis is a comparative analysis and a detailed study of the features of protection of confidential information in the IT sphere in Ukraine and foreign countries, consideration of such aspects as the legal regulation of the sphere of information technologies in the context of the preservation of confidential information and to outline the prospects of the development of this industry in Ukraine and foreign countries.

The object of study of this work is the protection of confidential information in the IT sphere in Ukraine and abroad.

The methodological basis of set up of the general scientific principles and approaches and special scientific classifications of confidential information, the legislative base of Ukraine and the studied foreign countries, the use of which has allowed to obtain scientifically sound results. For the study will be used such as general scientific methods: analysis and synthesis.

Theoretical and methodological basis of the study is in a comparative analysis and classification, the use of which helped to consider the relevance of legal regulation of the circulation of confidential information in Ukraine and foreign countries, to separate and analyze in detail trade secrets as a subspecies of confidential secrecy. The analysis and comparisons made it possible to examine the issues of non-disclosure of confidential information in the IT sphere and of the confidentiality agreement in Ukraine and abroad.

CONFIDENTIAL INFORMATION, IT-LAW, COMMERCIAL SECRET, NON-DISCLOSURE AGREEMENT, INFORMATION SECURITY, UNFAIR COMPETITION, NON-COMPETE CLAUSE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ…………………………………………………9

РОЗДІЛ 1 ПОЯСНЮВАЛЬНА ЗАПИСКА………………………………………….10

РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА………………………………………………...22

2.1. Поняття та види конфіденційної інформації як об'єкта правового регулювання в Україні та зарубіжних країнах………………………………..22

2.2. Стан інформаційної безпеки в Україні та зарубіжних країнах………………………………………………...………………………...35

2.3. Система органів, які здійснюють контроль над дотриманням збереження

конфіденційної інформації в Україні та зарубіжних країнах……………………………………………….…….……………………41

2.4. Заходи спрямовані на захист конфіденційної інформації та комерційної таємниці у сфері IT в Україні та зарубіжних країнах………………………..45

2.5. Договір про нерозголошення конфіденційної інформації (Non‑disclosure agreement) в українському  IT та зарубіжних країнах: порівняльний аналіз……………………………………………………………57

2.6. Проблема збереження конфіденційності та надійності захисту даних в Україні та зарубіжних країнах………………………………………………...72

ВИСНОВКИ…………………………………………………………………………...80

ПЕРЕЛІК використаних джерел……………………………………………..85

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРУ Верховна Рада України

КМУ Кабінет Міністрів України

п. пункт

р. рік

ст. стаття

КМУ Кабінет Міністрів України

РОЗДІЛ 1 ПОЯСНЮВАЛЬНА ЗАПИСКА

*Актуальність теми.* На сьогоднішній день в нашій країні, як і у всьому світі, відбувається поступове становлення інформаційного суспільства, економічною основою якого є створення та вдосконалення технічних і технологічних способів і засобів виробництва, отримання та поширення інформації на основі створення та використання інформаційно-комунікаційних технологій, які можуть розглядатися в якості найважливішої ознаки сучасної інформаційної епохи. Щорічно ІТ-індустрія України демонструє зростання в 20%, що випереджає середні темпи розвитку галузі в світі. Мова йде як про фінансові показники, так і кількість фахівців. За підсумками 2018 року ІТ стала другою найбільшою галуззю з експорту послуг. Підвищення економічної складової інформаційно-комунікаційних технологій вимагає створення і відповідної правової основи їх виробництва та використання. Для країн, що розвиваються, одним із актуальних напрямків розвитку зовнішньоекономічної діяльності є аутсорсинг інформаційних технологій. Завдяки аутсорсингу країни, що розвиваються, можуть брати активну участь у торгівлі на світовому ринку інформаційних послуг і співпрацювати з розвинутими державами на умовах взаємовигоди й обміну досвідом. Україна також бере активну участь у світовому ринку аутсорсингу інформаційних технологій, що є однією із небагатьох галузей української економіки, яка в умовах важкої економічної та політичної ситуації в країні успішно розвивається.

Одним із пріоритетних напрямків державної політики є розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя, що задекларовано Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», Пoстанoвoю КМУ «Прo запровадження Нацioнальнoї системи iндикатoрiв рoзвитку iнфoрмацiйнoгo суспiльства», Рoзпoрядженням Кабінету Міністрів України «Прo схвалення Стратегiї рoзвитку iнфoрмацiйнoгo суспiльства».

Головні тенденції в розвитку сучасної зарубіжної інформатизації – стійке зростання обсягу ринку інформаційних технологій, зростання інвестицій в інформатизацію і зростання прибутків від продуктів інформаційної технології. Домінуюча тенденція полягає в тому, що розвиток індустрії інформаційних технологій у майбутні роки так чи інакше пов'язаний з розвитком і застосуванням комп’ютерної мережі Інтернет.

Наявність системи забезпечення захисту інформації уможливлює надійне забезпечення національної безпеки країни через забезпечення інформаційної безпеки, захисту інформації, інформаційних технологій.

Сучасні темпи розвитку інформаційних технологій перевершили всі очікування і спростували навіть найсміливіші прогнози. Справа в тому, що окремі підсистеми обробки інформації (операційні системи, мережі) розвиваються швидше, аніж інфраструктура, в якій їм визначено працювати. Можливості апаратури зростають зараз набагато швидше, аніж очікувалося в численних прогнозах десятирічної давності.

Наразі, компанії повинні вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб. Компанії все частіше передають на збереження третім особам свої бази даних, а натомість отримують можливість доступу до них без обмежень на місце і час. Отримані переваги перевищують небезпеку ризику їх втрати чи розкриття конфіденційності інформації.

Переважна більшість положень законів України та інших нормативно-правових акті, які мають безпосереднє відношення до інформаційних відносин, спрямовані саме на захист інформації. Однак, проблема інформаційної безпеки українських і зарубіжних IT компаній та продукту, що такі виробляють, залишається недостатньо дослідженою.

*Об’єктом кваліфікаційної роботи* захист конфіденційної інформації в IT сфері в Україні та зарубіжних країнах.

*Предметом* правові норми в Україні та зарубіжних країнах, що регулюють обіг конфіденційної інформації, її захист в Україні та зарубіжних країнах.

*Мета роботи* полягає в порівняльному аналізі та детальному дослідженні особливостей захисту конфіденційної інформації в IT сфері в Україні та зарубіжних країнах, розгляд таких аспектів, як правове регулювання сфери інформаційних технологій в розрізі збереження конфіденційної інформації та окреслити перспектив розвитку даної індустрії в Україні та зарубіжних країнах.

Зазначені мета та об’єкт роботи зумовили наступні *завдання дослідження*, які мають бути вирішені в роботі:

* проаналізувати поняття та види конфіденційної інформації як об'єкта правового регулювання в Україні та зарубіжних країнах;
* дослідити стан інформаційної безпеки в Україні та зарубіжних країнах;
* охарактеризувати система органів, які здійснюють контроль над дотриманням збереження конфіденційної інформації в Україні та зарубіжних країнах;
* проаналізувати заходи спрямовані на захист конфіденційної інформації та комерційної таємниці у сфері IT в Україні та зарубіжних країнах;
* порівняти договір про нерозголошення конфіденційної інформації (Non‑disclosure agreement) в українському  IT та зарубіжних країнах;
* проаналізувати проблему збереження конфіденційності та надійності захисту даних в Україні та зарубіжних країнах.

*Ступінь наукової розробки проблеми.* У цьому напрямі дослідження здійснювали свої розробки провідні представники інформаційно-правової науки, наприклад, А. І. Марущак, який аналізує інформацію як об’єкт доступу до неї громадян. Інформаційно-правові питання державного управління в інформаційній сфері розкриває Ю. П. Бурило, правовий режим конфіденційної інформації як нетипового об’єкта цивільного права А. Г. Дідук, а загальнотеоретичні аспекти щодо особливого суб’єкта інформаційних правовідносин визначає О. С. Рождественська. Поняття конфіденційної інформації та комерційної таємниці досліджено у працях.

Однак зазначені та інші дослідники не розкривають питання класифікації інформації згідно з останніми змінами інформаційного законодавства України. З огляду на викладене, можна стверджувати, що існує необхідність наукового дослідження видової класифікації інформації.

*Опис проблеми, що досліджується.* У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп’ютерної злочинності тощо. Тому Конституція України забезпечення інформаційної безпеки відносить до найважливіших функцій держави.

Необхідно зазначити, що в науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека підприємства», що є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій і супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Таким чином, під інформаційною безпекою розуміється захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі.

Деякі керівники комерційних структур у своїй підприємницькій діяльності не приділяють належної уваги інформаційній безпеці підприємства, що дозволяє зловмиснику використовувати недоліки захисту інформаційних автоматизованих систем й обчислювальної техніки. Одним із шляхів усунення цих недоліків у сфері підприємництва є проектування організаційно-функціональної підсистеми інформаційної безпеки підприємства і її ресурсного забезпечення. Сфера інформаційної безпеки потребує оцінювати вчинки зловмисників, які модифікують, знищують або сприяють крадіжці інформації. Виходячи з аналізу конкретної ситуації, а також технології обробки та захисту даних в інформаційних системах, враховуючи засоби і методи негласного зняття інформації, це роблять порушники правового режиму безпеки інформації.

Питання впровадження концепції забезпечення міжнародної інформаційної безпеки вже розглянуто в дослідженнях, хоча сама концепція не була визначена. Ллойд розглядав акти ООН, Ради Європи, ОЕСР та Азіатсько-Тихоокеанського співтовариства під час вирішення питань конфіденційності, передусім розглядаючи акти «м'якого права». Оглядаючи проблеми кіберзлочинності, цей автор дає короткий огляд Конвенції Ради Європи про кіберзлочинність, Керівних принципів ОЕСР щодо безпеки інформаційних систем та актів ЄС.

З переходом нашої держави до ринкових відносин в українському законодавстві з'явились притаманні ринковій економіці поняття – «конфіденційна інформація», «комерційна таємниця», «ноу-хау», активне використання яких обумовлює необхідність розкриття і уточнення їх змісту. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» визначає впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя одним з пріоритетних напрямів державної політики, реалізація якого потребує удосконалення захисту прав інтелектуальної власності, зокрема і прав на комерційну таємницю. За цих обставин найбільш ефективним способом захисту конфіденційної інформації є договір про нерозголошення, заснований на взаємній зацікавленості сторін.

Аналіз наукових досліджень зазначених вище науковців показує, що їхні праці присвячені, в основному, правовим аспектам комерційної таємниці (право власності на комерційну таємницю, її отримання, використання, зберігання і поширення, правові засади захисту), однак комерційна таємниця з точки зору економічної безпеки первинної ланки господарювання не досліджувалась, а враховуючи динамічний характер розвитку інформаційних технологій (ІТ) потреби вдосконалення захисту комерційної таємниці у суб’єктів господарювання виникають постійно.

Становлення ринкових відносин в Україні проходить під впливом негативних чинників, серед яких найбільше значення мають: загострення конкурентної боротьби; збільшення монополізації ринку; встановлення контролю кримінальних структур над певними галузями економіки підприємства; зростання державного регулювання економіки і посилення тиску на суб’єкти господарювання з боку державних органів, недосконалість чинного законодавства в сфері економічних відносин, зокрема відсутність правових норм, які б конкретно регламентували питання організації і управління безпекою підприємства і, як наслідок, повна незахищеність підприємницьких структур перед зазначеними вище чинниками.

Право підприємців на захист своїх законних інтересів та своєї власності, в тому числі комерційної таємниці, є конституційним правом кожного громадянина України. У ст.ст. 31, 32, 34, 41, 42, 54 Конституції України встановлені базові правові рамки, в межах яких особа вправі реалізовувати свої права на комерційну таємницю та відстоювати власні законні інтереси у забезпеченні конфіденційності інформації. Конституція України стала основою для наступного розгалуження та наповнення нормативним змістом законодавства України щодо комерційної таємниці, розвиток відбувався у таких основних напрямках, як: конкретизація і спеціалізація положень Закону України «Про інформацію» щодо комерційної таємниці, врегулювання доступу органів влади до комерційної таємниці, забезпечення збереження комерційної таємниці в контексті захисту від недобросовісної конкуренції, врегулювання питань відповідальності за правопорушення, пов’язані з комерційною таємницею.

Поняття захисту інформації і конкретні види заходів щодо захисту інформації були введені тільки в січні 2011 року Законом України «Про інформацію» в новій редакції, в якому зазначено, що захист iнформацiї – це сукупнiсть правових, адмiнiстративних, організаційних, технiчних та iнших заходiв, що забезпечують збереження, цiлiснiсть iнформацiї та належний порядок доступу до неї.

Існують різноманітні визначення поняття комерційної таємниці як на законодавчому рівні, так і на науковому. Так, поняття комерційної таємниці зазначені в статтях 420, 505 Цивільного кодексу України. Також, відповідне визначення міститься в Господарському кодексі Україні, а саме в статтях 36, 162 тощо. Тобто окрім поняття, дані вищенаведені статті визначають об’єкт комерційної таємниці, його регулювання тощо.

Неналежний рівень правового регулювання відносин, пов’язаних з комерційною таємницею суб’єктів господарювання, сприяє поширенню комерційного шпигунства, безперешкодному використанню окремими особами незаконно отриманих наукомістких технологій, програмних продуктів та іншої інформації, що належить до комерційної таємниці. Розглядаючи питання визначення ролі правового інституту у системі права, слід звернути увагу на думку С. С. Алєксєєва стосовно того, що природу та правові особливості інституту можна правильно спів ставити лише в тому разі, «якщо виходити з того, що це – така спільність норм приписів, яка в свою чергу, є елементом наступного, головного підрозділу – галузі права. Юридичні норми створюють відповідну галузь права не опосередковано, а через інститути.

Варто погодитися, що відсутність загальновідомості полягає в тому що інформацією яка складає комерційну таємницю володіє обмежене коло осіб хоча й не обов’язково одна особа. Однаковою або аналогічною інформацією можуть одночасно володіти декілька осіб, але визначальним є те що коло цих осіб обмежене. Саме не загальновідомість є вихідною для встановлення охорони змісту об’єкту, яким є комерційна таємниця за відсутності його спеціальної реєстрації не загальнодоступність означає відсутність вільного доступу до інформації на законній підставі. Особи які допущені до таємниці повинні бути зобов’язані не розголошувати її саме з цією ознакою пов’язують вимогу до суб’єкта права на комерційну таємницю вживати заходів для збереження її секретності не загальновідомості та конфіденційності. Здатність об’єкту перебувати в цивільному обороті передбачає його комерційну цінність. тобто можливість отримання економічної вигоди від введення його в оборот. Передумовами оборотоздатності є не загальновідомість та не загальнодоступність. Особливість наведених умов охороно спроможності комерційної таємниці полягає в тому що перевірка їх наявності здійснюється не в порядку спеціальної попередньої процедури а лише тоді коли право суб’єкта на комерційну таємницю порушується або заперечується.

За неофіційними даними, в Україні – близько 4 тисяч компаній, більшість із яких мають до 80 співробітників, однак чимало фахівців працюють у фірмах, що налічують понад 80 осіб персоналу. З них кількість компаній, активних на ринку праці – 2 309. Базуючись на вибірці, можна припустити, що приблизно 70% –  надають ІТ-послуги широкому колу клієнтів. Оскільки за правилами більшості IT компаній при прийомі у штат, неохідно підписати Договір про конфіденційність та неконкурування, саме тому на данний момент існує нагальна потреба у вивченні Договору про конфіденційність (Non-disclosure agrement).

Законодавчий інститут, який регулює відносини в сфері комерційної таємниці можна віднести до інституту інтелектуальної власності, тобто сукупності виключних прав на нематеріальні об’єкти, що є результатом інтелектуальної діяльності, у тому числі творчої, та інших прирівняних до них об’єктів.

Ні вітчизняне законодавство, ні наявна практика не виробили на сьогоднішній день ефективних превентивних заходів щодо попередження витоку інформації або способів захисту правовласників після того, як відомості, що є комерційною таємницею було розголошено. Труднощі виникають вже на етапі визначення кола відомостей, які підлягають охороні, та й довести факт незаконного поширення таких відомостей під час судового розгляду часом буває неможливо, так само як і чітко розрахувати і обґрунтувати розмір завданих збитків та, тим більше, упущеної вигоди. У зв'язку з цим є інтерес дослідників до закордонного досвіду вирішення такого роду проблем. Наприклад, в більшості юрисдикцій США комерційна таємниця охороняється законом. У 42 штатах та окрузі Колумбія суди застосовують ту чи іншу редакцію Уніфікованого закону про комерційну таємницю (Unіfоrm Tradе Sесrеts Aсt).

Даний акт визначає комерційну таємницю як інформацію, в тому числі формулу, зразок, компіляцію, програму, пристрій, метод, техніку або процес, яка має самостійну економічну цінність, дійсну або потенційну, в силу того, що не є загальновідомою або легкодоступною з використанням необхідних засобів для осіб, які можуть отримати економічну вигоду від її розкриття або використання, і є предметом заходів охорони, що є розумними при відповідних обставинах для збереження її секретності.

Крім чіткого визначення характеристик, якими наділена комерційна таємниця, з метою її захисту і регулювання цього інституту в зарубіжному праві широко застосовується інститут договорів про уникнення конкуренції (non-compete agreements), що укладаються з працівниками або підрядниками. Джерелом даного інституту є англійське право XVIII століття, а в даний час ці угоди часто застосовуються у відношенні топ-менеджерів і технічних працівників. На відміну від країн з англо-саксонською системою права, в країнах Європи правове регулювання комерційної таємниці на законодавчому рівні почало розвиватися лише на початку 90-х років минулого століття. Виключення складає лише Франція, де цей правовий інститут законодавчо врегульований з 1884 року. Разом з тим, розвиток Європейського Союзу потребує уніфікації законодавства країн-членів та приведення його до єдиних стандартів. Отже, цілком логічно передбачити можливість та необхідність вироблення єдиної для ЄС нормативноправової бази в сфері регулювання комерційної таємниці та внесення змін в законодавство окремих країн ЄС відповідно до неї.

Питання законодавчого визначення можливості укладати договори про неконкуренцію в сфері трудових відносин з метою належного захисту прав роботодавців та забезпечення міжнародних стандартів вже давно обговорюється як у наукових, так і в практичних сферах юриспруденції. Як зазначає О. М. Рим, укладення угоди про неконкуренцію з метою запобігання неправомірному використанню відомостей, що є комерційною таємницею, тобто договірне регулювання цих відносин якнайбільше відповідає існуючим економічним та соціальним умовам. Однак, такі угоди не можуть використовуватись для повного обмеження господарської та професійної діяльності працівника, а тільки для захисту трудових та майнових прав роботодавця.

Відсутність правової конструкції для регулювання неконкуренції у трудових відносинах зумовлює пошуки різних шляхів для захисту своїх інтересів роботодавцем. Наприклад, є випадки, коли при прийнятті на роботу угоду про неконкуренцію “маскують” під фіктивний договір позики, беручи від працівника розписку про отримання певної суми коштів з попередженням про її застосування у разі переходу до конкурентів. Однак, такий спосіб, крім того, що є не зовсім чесним і законним, є ненадійним з погляду правозастосовної практики. Суди під час розгляду справ про стягнення боргу за такими розписками, з’ясувавши реальні обставини справи, часто стають на бік працівників, визнаючи договір позики фіктивним і, відповідно, недійсним. Так, рішенням Сакського міськрайонного суду Автономної Республіки Крим було відмовлено в позові ОСОБА 1 до ОСОБА 2 про стягнення грошового боргу за договором позики, оскільки відповідачу, що працював у позивача – фізичної особи-підприємця без офіційного оформлення трудових відносин, вдалось довести, що розписки відбирались у працівників під психологічним примусом з метою недопущення переходу до конкурентів, а реального передання грошей не було.

Угоди про неконкуренцію в межах цивільно-правових та господарсько‑правових відносин також не мають належного законодавчого регулювання. Незважаючи на принцип свободи договору, конституційне право кожної особи на працю та підприємницьку діяльність вважається таким, що не може бути обмежено інакше як згідно з законом чи за рішенням суду. Відповідно, відсутність законодавчої можливості обмежити неконкуренцію, зокрема, у сферах розроблення програмного забезпечення та інших інформаційних послуг, не дає змоги встановлювати такі обмеження у договорах за згодою сторін.

Слід наголосити, що немає жодного законодавчого акту, який би зобов’язував працівників підписувати договір про нерозголошення комерційної таємниці. Такий договір у рамках трудових відносин не є обов’язковим. Тим більше, що на працівників у рамках цих відносин покладається обов’язок своєчасно та чітко виконувати розпорядження власника або уповноваженого органу, і якщо робота з конкретною інформацією входить до обов’язків працівника, він мусить дотримуватись розпоряджень керівництва щодо захисту комерційної таємниці.

Відповідно до Кодексу України про адміністративні правопорушення передбачена відповідальність за отримання або розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця. У такому випадку на правопорушника накладається штраф.

При складанні політики охорони комерційної таємниці важливо врахувати відмінності в розумінні терміну «комерційна таємниця» в різних країнах. В Україні захист прав інтелектуальної власності (іншими словами, конкретний обсяг прав і обов’язків осіб щодо якогось об’єкта інтелектуальної власності) підлягає праву держави, де потрібен такий захист. В силу цього різниця між розумінням цього терміна в законодавстві різних країн може істотно обмежити власника такої інформації в його можливості захистити свій головний бізнес-актив при виході на міжнародні ринки – відомості можуть підлягати обов’язковому оприлюдненню або ж не зважати об’єктом інтелектуальної власності, а захищатися в рамках зовсім іншого інституту.

Ефективність охорони права інтелектуальної власності залежить від багатьох факторів, найголовнішим з яких є наявність досконалого законодавства та дієвих механізмів його застосування, в тому числі при захисті прав. Питанням вдосконалення правового поля в сфері інтелектуальної власності приділялася особлива увага за останні декілька років, особливо в контексті європейської інтеграції та вступу України до Світової організації торгівлі. Державні органи України, до компетенції яких належить охорона права інтелектуальної власності, поступово здійснюють відповідні кроки по вдосконаленню правозастосовної практики, орієнтуючись на стандарти ЄС. Особливо це стосується механізму захисту прав інтелектуальної власності у судовому порядку, який використовується в Європейському Союзі вже понад три десятиліття.

З огляду на те, що ІТ-ринок в Україні вважає за краще модель працевлаштування за Кодексом Законів про Працю, часто складання ряду документів, заточених переважно під працівників, не має дійсної практичної користі. У такій особливості розподілу виконавців є свої переваги і недоліки: хоча довести витік інформації і знайти справжнього порушника-працівника буде простіше, але саме підрядника легше притягнути до відповідальності за втрату можливого прибутку компанії в разі порушення конфіденційності.

У різних країнах світу, де використовуються інформаційні об’єкти, які являють собою комерційну цінність, на жаль, ще не вироблений єдиний підхід до визначення поняття такої інформації. Питання актуальності дослідження захисту конфіденційної інформації в Україні та порівняльний аналіз з зарубіжним досвідом сьогодні потребує більш детального вивчення у звязку із активним розвитком сфери інформаціних технологій.

*Апробація результатів дослідження.* Результати кваліфікаційної роботи були обговорені на засіданнях кафедри адміністративного та господарського права Запорізького національного університету. Положення даної магістерської роботи були враховані автором в ході підготовки наукових статей для опублікування в українській наукові періодиці, під час участі у роботі наукових конференцій: Міжнародна науково-практична конференція «Розвиток сучасного права в умовах глобальної нестабільності» м. Одеса, 13-14 вересня 2019 р., Міжнародна науково‑практична конференція «Розвиток державності та права в Україні: реалії та перспективи» м. Львів, 20-21 вересня 2019 р., Міжнародна науково-практична конференція «Юридична наука України: історія, сучасність, майбутнє» м. Харків, 1‑2 листопада 2019 р.

РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА

2.1. Поняття та види конфіденційної інформації як об'єкта правового регулювання в Україні та зарубіжних країнах

У сучасному суспільстві інформація відіграє вирішальну роль, а інформаційні ресурси стають в один ряд з найважливішими ресурсами держави – природними, трудовими, фінансовими та іншими, що становлять його потенціал. Вважається установленою виключна значимість інформації в сучасних соціально-економічних процесах.

Особливий напрям дослідження інформаційного права України пов’язаний із з’ясуванням правової сутності інформації як основного об’єкта інформаційних відносин. Науково-теоретичного та практичного значення набуває питання класифікації інформації. Адже від цього залежить обсяг прав та обов’язків учасників інформаційних відносин. Питання видової класифікації інформації актуалізувалося з набранням чинності законів України «Про доступ до публічної інформації» та «Про внесення змін до Закону України «Про інформацію».

Розпочати необхідно з визначення інформації, наведеного у ст. 1 Закону України «Про інформацію»: інформація − будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Деякі вчені підкреслюють властивості інформації як товару. Інформація набуває основних рис товару – особливого різновиду, якості якого (споживча вартість, відчуження у формі купівлі-продажу тощо) проявляються поза залежністю від кількості потраченої на її вироблення розумової праці. Інформацію виділяють також як об'єкт міжнародного торговельного обороту. При цьому відзначається, що інформація може бути об'єктом міжнародного торговельного обороту як складова частина результатів інтелектуальної діяльності.

Згідно з ч. 2 ст. 28 Закону України «Про інформацію» за режимом доступу до інформації (передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації) інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Частина 1 ст. 30 Закону зазначає, що інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну та таємну.

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. Конфіденційна інформація поряд з службовою та таємною належить до інформації з обмеженим доступом.

**Інформація** - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

Інформація з обмеженим доступом:

Відкрита інформація

* Конфіденційна;
* таємна;
* службова.
* Є інформація про фізичну особу;
* інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень

На думку С. І. Семилетова, конфіденційна інформація (обмеженого доступу) поділяється на:

* службову інформацію;
* інформацію про комерційну і службову таємницю (у тому числі усі види професійної таємниці і ноу-хау);
* інформацію про громадян (персональні дані).

В. Н. Лопатін вважає, що конфіденційна інформація має містити в собі такі об'єкти: комерційну таємницю, банківську таємницю; професійну таємницю; персональні дані; службову таємницю.

Комерційну таємницю слід вважати видом конфіденційної інформації, яка визначена в ч. 2 ст. 30 Закону України «Про інформацію» як відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Незважаючи на різні критерії і види, запропоновані класифікації поєднує те, що комерційна таємниця виділена в окремий вид, що означає визнання вченими, незважаючи на розбіжності в поглядах, самостійності категорії комерційної таємниці.

Деякі вчені вважають комерційну таємницю різновидом професійної таємниці. При цьому професійну таємницю визначають як певний комплекс конфіденційної інформації, у тому числі і тієї, що становить комерційну таємницю, яку за умови її нерозголошення отримує особа в результаті своєї професійної діяльності.

Комерційною таємницею можуть бути **відомості технічного, організаційного, комерційного, виробничого та іншого характеру**, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (стаття 505 (2) ЦК).

У свою чергу, ст. 162 Господарського кодексу України визначає, 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.

**Комерційна таємниця** – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

**Ознаки комерційної таємниці:**

• інформаційність комерційної таємниці (в тому розумінні, що комерційна таємниця – це інформація);

• конфіденційність;

• комерційна цінність;

• захищеність інформації, яка становить комерційну таємницю.

Майнові права інтелектуальної власності на комерційну таємницю:

* 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.

Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною таємницею, якщо інше не встановлено договором.

Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства. Відомості, які не можуть становити комерційну таємницю, визначено постановою Кабінету Міністрів України від 9 серпня 1993 року № 611 «Про перелік відомостей, що не становлять комерційної таємниці».

Так, комерційну таємницю не становитимуть:

* установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;
* інформація за всіма встановленими формами державної звітності;
* дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
* відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
* документи про сплату податків і обов'язкових платежів;
* інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
* документи про платоспроможність;
* відомості про підприємницьку діяльність;
* інформація, яка згідно з Законом України «Про інформацію» підпадає під режим таємної (державна таємниця);
* відкрита інформація (правила страхування, розроблені страховиком) (див. Закон України «Про страхування»);
* відомості, щодо яких в законодавстві міститься пряма заборона на поширення на них режиму обмеженого доступу (інформація про стан довкілля, про якість харчових продуктів і предметів побуту);
* регламент сертифікованою складу (ЗУ «Про сертифіковані товарні склади та прості і подвійні складські свідоцтва»);
* фінансова звітність підприємств (ЗУ «Про бухгалтерський облік та фінансову звітність в Україні»).

Практично в усіх законах про доступ (свободу) до інформації зарубіжних країн втілений принцип максимального оприлюднення: «вся інформація, якою володіють публічні органи, підлягає розкриттю. Винятки повинні бути максимально обмежені, визначені законом і публічні органи повинні довести виникнення та правомірність таких винятків». Доступ лише до інформації, яка підпадає під такі винятки, може бути обмежений.

Порядок захисту комерційної таємниці визначається її власником і має передбачати:

• склад та обсяг інформації, що становить комерційну таємницю;

• порядок надання та зняття грифу обмеження доступу до документа “Комерційна таємниця”;

• умови доступу осіб до комерційної таємниці;

• форму обліку осіб, які отримують доступ до комерційної таємниці;

• порядок оформлення, використання, обліку, збереження документів та інших матеріальних носіїв комерційної таємниці;

• порядок прийняття зобов’язань для сторін щодо збереження комерційної таємниці при здійсненні цивільно-правових, трудових та інших правовідносин.

За недотримання режиму роботи з інформацією, що є комерційною таємницею, працівник суб’єкта підприємницької діяльності може бути притягнений до дисциплінарної відповідальності. Для правомірного застосування санкцій за правопорушення, пов’язані з комерційною таємницею у межах трудових правовідносин, підприємець повинен мати такі документи:

1. Документ, який встановлює перелік відомостей, що становлять комерційну таємницю. Це може бути затверджене суб’єктом господарювання Положення про комерційну таємницю, в якому має чітко зумовлюватися перелік відомостей, що становлять комерційну таємницю, порядок віднесення інформації до комерційної таємниці, умови зберігання, а також коло працівників підприємця, які мають право передавати зазначені відомості представникам органів влади.
2. Посадові інструкції, в яких має бути визначено коло повноважень працівників підприємця та відомості, що становлять комерційну таємницю і з якими вони повинні працювати, а також порядок роботи з ними. Із зазначеними документами працівник має ознайомлюватися до початку своєї трудової діяльності у цього суб’єкта господарювання. Факт ознайомлення повинен фіксуватися письмово, із зазначенням дати ознайомлення.
3. Трудовий договір або контракт, в якому мають зазначатися обов’язки працівника дотримуватися встановлених правил збереження комерційної таємниці та наслідки недотримання цього обов’язку. Можливе також складання окремого документа – зобов’язання про нерозголошення комерційної таємниці, яке підписується представником роботодавця та працівником. У договорі (контракті) за порушення режиму комерційної таємниці можуть передбачатися такі дисциплінарні санкції як догана, звільнення.

Сьогодні законодавство ЄС з охорони комерційної таємниці головним чином включає норми угоди ТРІПС, зокрема розділ 7 «Нерозкрита інформація», що був включений до Угоди у зв’язку з суттєвою роллю комерційної таємниці в міжнародній торгівлі.

Так, згідно зі статтею 39 Угоди ТРІПС, «фізичні та юридичні особи повинні мати можливість перешкоджати тому, аби інформація, яка законно перебуває під їхнім контролем, розголошувалася, збиралася або використовувалася іншими особами без їхньої згоди у такий спосіб, який суперечить чесній комерційній практиці, протягом часу, поки ця інформація:

* є секретною у тому значенні, що вона як єдине ціле або у точній сукупності та поєднанні її компонентів не є загальновідомою або легкодоступною (readily accessible) для осіб у колах, що зазвичай мають справу з вказаним видом інформації;
* має комерційну цінність, оскільки є секретною;
* є об’єктом достатніх для даних обставин заходів із збереженням її у секреті особою, котра законно здійснює контроль за інформацією».

У розвинутих країнах Європи охорона конфіденційної комерційної інформації має свою довгу історію, хоча підходи різняться залежно від країни. Найрозвинутішу систему охорони має Об’єднане королівство, що пов’язано з промисловою революцією та традицією прецедентного права. Саме з англійської системи бере початок відповідне законодавство США. У Великобританії відсутній законодавчий захист комерційної таємниці, відповідно, не існує легального визначення цієї таємниці. Натомість, правове регулювання цих відносин розвивалось упродовж останніх століть на основі судових прецедентів і отримало назву конфіденційного права (law of confidence). Отже, охорона комерційної таємниці ґрунтується на концепції “порушення довіри”. У рішенні Seager v. Copydex LTD вона сформульована так: “Право, що застосовується до цього випадку, не залежить від якоїсь угоди. Воно залежить від широкого принципу справедливості, що полягає в тому, що той, хто отримав інформацію конфіденційно, не повинен недобросовісно здобувати з неї вигоду. Він не повинен використовувати її на шкоду тому, хто передав йому цю інформацію, якщо останній не дав своєї згоди”. Отже, керівним принципом є довіра між законним власником таємниці й отримувачем конфіденційної інформації.

Законодавство Франції містить поняття промислових або виробничих секретів (secret de fabrique) та комерційної таємниці (secret de commerce). Перша категорія походить від французького кримінального кодексу та включає конфіденційну інформацію, що має виробниче застосування та може становити комерційну цінність. Комерційна таємниця прямо не визначається законодавством, але відображає ширше, порівняно з виробничими секретами, поняття й може належати до організаційної структури підприємства, списку постачальників, особистих справ персоналу, контрактів з іншими організаціями, списків клієнтів, планів розвитку бізнесу, схеми дистрибуції тощо. Виробничі й комерційні секрети не вважаються власністю у Франції і отримують захист як делікти з недобросовісної конкуренції та договірних зобов’язань.

**Комерційна таємниця Сполучених штатів Америки**

**4 основні елементи режиму комерційної таємниці в США:**

1939 р. – Перший Звід права деліктів – 1 спроба “кодифікації” права конфіденційної таємниці.

1. Інформація повинна бути “обмежена”, яку можна відрізнити від загальновідомих знань і навичок.

2. Елемент “секретності” – інформація не є добре відомою або такою, яку можна легко отримати.

1993 р. – Третій Звід права деліктів – закріплено сучасний підхід права комерційної таємниці.

3. Інформація повинна мати економічну цінність, що полягає в наданні певної конкурентної переваги.

4. Власник повинен вжити розумних зусиль для того, щоб зберегти інформацію в таємниці.

Охорона комерційної таємниці відбувається в межах делікту незаконного заволодіння комерційною таємницею, який, є складовою делікту недобросовісної конкуренції.

Законодавство Канади про комерційну таємницю також, за винятком Квебеку, ґрунтується на прецедентному праві, центральним принципом якого, як і в Англії, є порушення довіри. Підставами для позову в результаті делікту є:

* секретність інформацій;
* те, що її було надано конфіденційно;
* те, що особою, якій її було надано, використано зі зловживанням.

Наприклад, у справі Three Savers Int’l LTD v. Savoy колишні працівники позивача визнані відповідальними за використання списку клієнтів їхнього працедавця для ведення бізнесу конкурента, що складено працівниками після того, як вони залишили свою попередню роботу.

|  |  |
| --- | --- |
| Визначення комерційної таємниці підприємства в різних країнах | |
| Німеччина | У Німеччині діє «Закон проти недобросовісної конкуренції», який виділяє два види комерційної таємниці: виробничу і комерційну. До виробничої таємниці відноситься інформація організаційного і технічного характеру (спосіб виробництва, технології, відкриття, винаходи та ін. До комерційної таємниці віднесена інформація про торговельні відносини фірми, організації та розмірі обороту, стан ринків збуту і споживачів, банківських операціях і ряд інших. Порушення комерційної таємниці розглядається законодавством Німеччини як факт недобросовісної конкуренції. Кримінальна відповідальність за злочини, пов'язані з порушенням комерційної таємниці передбачені в Німеччині в Законі про недобросовісну конкуренцію. Для кваліфікації відповідних злочинів повинні бути встановлені наявність охоронюваної законом таємниці та її розголошення, неправомірного використання. Умисел злочинця може бути спрямований як на отримання вигоди, так і на заподіяння шкоди власнику інформації. Кримінальна відповідальність настає лише в тому випадку, якщо інформація, яка є складовою комерційної таємниці, отримана з допомогою незаконних, недобросовісних дій. |
| Китай | Китай, вивчивши досвід роботи США і деяких інших країн щодо захисту ноу-хау, спочатку ввів загальнодержавне «Положення про комерційну службу безпеки (1988 рік) а потім «Закон про недобросовісну конкуренцію» (1993 рік). Під комерційними секретами в Законі розуміється: технічна і господарська інформація, яка невідома широким колам публіки, яка може принести економічну вигоду її власникам і яка представляє практичну цінність для інших, у зв'язку з чим власники цієї інформації приймають заходи для збереження її секрету. Комерційні служби безпеки працюють за контрактами з державними і приватними організаціями, спільно з власниками визначають секрети виробництва конкретних фірм, що організують необхідну роботу щодо їх захисту, а також здійснюють її координацію з державними та недержавними організаціями. У Китаї комерційна таємниця відноситься до сфери цивільного права. Розкрадання і незаконне використання комерційної інформації трактується як порушення закону «Про незакону конкуренцію», який набрав чинності в грудні 1993 року. Згідно із законодавством Китаю поняття комерційної таємниці визначається як технічна й управлінська інформація конфіденційного характеру, яка є ознакою економічної та практичної цінності, і щодо якої вжиті запобіжні по захисту секретності. Юридичний захист встановлюється відносно промислових «ноу-хау», що містяться в будь-яких документах, дизайнерських проектах, схемах та кресленнях. Закон забороняє вчинення дій, пов'язаних з отриманням комерційної таємниці шляхом розкрадання, незаконного примусу або іншими неправомірними способами. Також закон встановлює заборону на розголошення та використання інформації, складової комерційної таємниці, отриманої незаконними способами і з порушенням умов використання відомостей, передбачених угодою між сторонами. Власник комерційної таємниці, законні інтереси якого були порушені, має право звернутися до суду з позовом про відшкодування завданих збитків. |
| Великобританія | Немає спеціального законодавства з питань захисту комерційної таємниці в Англії. Відносини, пов'язані з комерційною таємницею регулюються в основному договорами між роботодавцем і найманим працівником в рамках цивільно-правових відносин застосовуються угоди про конфіденційність між контрагентами. Державні службовці, наприклад, податкові інспектори, поліцейські, як правило зобов'язуються не розголошувати інформацію, яка стала їм відома в силу виконання службових обов'язків. Покладання такого обов'язку здійснюється шляхом підписання державним службовцям спеціального угоди. |
| США | У 1996 році в США був прийнятий закон «Про економічне шпигунство», що заклав сучасні основи федеральної системи захисту комерційної інформації. Розкрадання відомостей, що становлять комерційну таємницю, прирівнюється законом до федеральних злочинів. Винні в ньому можуть бути засуджені до 10 років тюремного ув’язнення і 2,5 мільйонів доларів штрафу. Закон розширив поняття комерційної таємниці, включивши в нього нові технології, за допомогою яких здійснюється створення та зберігання відомостей, складових комерційної таємниці. До комерційної таємниці віднесено види і форми фінансової, комерційної, наукової, технічної і економічної інформації, включаючи моделі, креслення, програми, формули, ідеї, прототипи, методики, технології, процедури фбо коди, що зберігаються будь-яким способом, за умови, що власник вжив розумних заходів для збереження конфіденційності, а інформація має самостійну економічну цінність в силу відсутності доступу до неї інших осіб. |

Отже, у зв’язку з активним розвитком інформаційних технологій, їх використанням у повсякденному житті та надання IT послуг, виникає потреба у такому понятті як конфіденційна інформація, та її підвид – комерційна таємниця. Критерії визначення комерційної інформації в Україні та зарубіжних країнах ґрунтуються на різних принципах. Одними з суміжних понять, які переплітаються з конфіденційною інформацією в законодавствах України та зарубіжних країн, котрі були розглянуть у даному підрозділі, це елемент секретності інформації, комерційна цінність та інформаційність комерційної таємниці.

2.2. Стан інформаційної безпеки в Україні та зарубіжних країнах

Розвиток та впровадження новітніх інформаційно-телекомунікаційних технологій призвів до науково-технічної революції, що сприяла виникненню інформаційних відносин та як наслідок виокремленню самостійної галузі права – інформаційного права. На сучасному етапі інформаційні відносини в Україні урегульовані значною кількістю нормативно-правових актів різної юридичної сили. Водночас інформаційне законодавство України є неефективним, оскільки характеризується безсистемністю, фрагментарністю, колізійністю норм права та домінуванням підзаконних нормативно-правових актів щодо законів.

Рівень інформаційної безпеки держави, значною мірою, зумовлений рівнем її інформаційної інфраструктури. На жаль, як зазначає науковець В. Петрик, низький загальний рівень інформаційної інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації. Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його неконкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу іноземним інформаційним програмам.

Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека – це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію (або дані) можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм.

На сьогодні в Україні немає чітко врегулювання вимог до інформаційної безпеки на підприємствах. При цьому є вимоги які ставляться до компаній, які працюють з персональними даними громадян Європейського союзу відповідно до вимог [General data protection regulation](https://legalitgroup.com/gdpr-novi-yevropejski-tendentsiyi/) (GDPR), та деяких інших нормативних актів.

Останні тенденції нормотворення, зокрема, проект Постанови НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків», окремі норми Закону України «Про основні засади забезпечення кібербезпеки України» та деякі інші, вказують на те, що в близькому майбутньому нас чекає чітке законодавче регулювання з жорсткими вимогами до Політик інформаційної безпеки підприємств. Правову  основу  забезпечення  інформаційної  безпеки  України  становлять також Конституція України, закони України, “Про інформаційну безпеку України”, “Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”, “Про доступ до публічної інформації, інші закони та інформативно правові акти, а також ратифіковані або парафовані Україною Договір про безпеку і співробітництво в Європі, Договір “Відкрите небо”, Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов’язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання  та споживання отриманої інформації в національних інтересах.

Закони і нормативні акти орієнтовані на всіх суб’єктів інформаційних відносин незалежно від іх організаційної приналежності (це можуть бути як юридичні, так і фізичні особи) в межах країни (міжнародні коніенції мають навіть ширшу область дії), адміністративні захди – на всіх субєктів в межах організації, процедурні – на окремих людей (або невеликі категорії субєктів), програмно-технічні – на устаткування і програмне забезпечення.

Інформаційну безпеку доцільно розглядати у контексті комплексу дій, що пов’язаний із забезпеченням прав на захист інформації, а також права власності на інформацію, права на захист від інформації та інформаційних впливів, а також права на інформацію та свободу інформаційної діяльності. З цього приводу, на думку деяких дослідників в сфері інформаційної безпеки, вона представлена трьома структурними компонентами.

Структурні компоненти інформаційної безпеки

Інформаційно-технічна безпека

Інформаційно-психологічна безпека

Інформаційна безпека в сфері прав і свобод людини і громадянина

Реалізація прав громадян на доступ до інформації, дотримання основних принципів інформаційних відносин

Захист від інформаційних впливів, що носять негативний характер

Захист інформації з обмеженим доступом згідно законодавства

Одночасно з розвитком технологій постає питання безпеки в інформаційно-телекомунікаційних мережах. З точки зору забезпечення безпеки найбільш важливими властивостями мереж є: конфіденційність (використання інфраструктури або її частини); цілісність (інфраструктури); доступність (служб та сервісів); cпостереженість (за використанням інфраструктури або її частини); прихованість (використання та управління інфраструктурою).

Захист інформації це діяльність, яка спрямована на забезпечення безпеки оброблюваної в інформаційно-телекомунікаційних систем інформації та інформаційно-телекомунікаційних систем в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз. Основним завданням захисту інформації є протидія порушенню таких властивостей як: конфіденційність інформації; цілісність інформації; доступність використання інформаційно-телекомунікаційних систем та оброблюваної інформації; спостережність за діями користувачів та керованість інформаційно-телекомунікаційних систем.

На даний час, відповідно до Закону визначені основні поняття. Кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Закон набуває чинності через шість місяців з дня його опублікування. З точки зору забезпечення безпеки найбільш важливими властивостями кіберінфраструктури є: конфіденційність (використання інфраструктури або її частини); цілісність (інфраструктури); доступність (служб та сервісів); cпостереженість (за використанням кіберінфраструктури або її частини); прихованість (використання та управління кіберінфраструктурою). Якщо для захисту інформації найбільш важливими заходами є запобігання загрозам конфіденційності та цілісності, то в кіберпросторі основні зусилля повинні бути направлені на запобігання загрозам доступності служб (в кіберпросторі атаки з метою порушення доступності реалізуються простіше) та cпостереженість за використанням інфраструктури (або її частини).

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

* протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
* порушення встановлених регламентів збору, обробки та передачі інформації;
* навмисні дії та ненавмисні помилки персоналу інформаційних систем;
* помилки в проектуванні інформаційних систем;
* відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо.

Також необхідно враховувати, що загроза інформаційним системам підприємства може настати з боку наступних суб’єктів:

* працівники підприємства, що використовують своє службове становище (коли законні права за посадою використовуються для незаконних операцій з інформацією);
* працівники підприємства, що не мають права в силу своїх службових обов’язків, але здійснили несанкціонований доступ до конфіденційної інформації;
* особи, які не пов’язані з підприємством трудовою угодою (контрактом).

Всі методи забезпечення інформаційної безпеки підприємства можна об’єднати у три групи: правові, організаційні та програмно-технічні.

Правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов’язані з використанням інформації в діяльності підприємства. З розвитком правового регулювання процесів інформаційного обміну набагато простіше встановлювати партнерські стосунки, шукати контрагентів, реалізовувати і закуповувати продукцію, стали доступніші нові «види бізнесу» – нові форми здійснення підприємницької діяльності. Захист інформації є невід’ємної складової бізнесу.

Необхідність наукового аналізу форм і методів інформаційної безпеки, захисту населення від негативних впливів як у воєнний час, так і в мирний, що використовується США, дозволить критично оцінити американський досвід у побудові інформаційної стратегії, в цілому розглянути її систему, роль і повноваження різних відомств з урахуванням специфіки їх діяльності. Ураховуючи те, що США мають значний фінансовий, технологічний, науково-технічний та воєнний потенціал, а також приділяють велику увагу посиленню національної безпеки, захисту громадянських прав та інтересів бізнесу, досвід цієї держави у сфері управління інформаційною безпекою є найбільш важливим для вивчення.

Оскільки США в XX столітті стали лідером у розвитку інформаційних технологій, соціально-економічні, воєнні та політичні наслідки інформаційної революції найбільш відчутні в цій державі. Америка раніше за інші країни зіткнулася з інформаційними загрозами національної безпеки. В результаті цього США стали першими, хто розпочав розроблення державної політики у сфері інформаційної безпеки. У США була створена система державного регулювання в інформаційній сфері, що забезпечує ефективне використання сучасних інформаційних технологій для прискорення американської економіки.

Пріоритетами національної інформаційної політики США визначено: підтримку досліджень і розробок у галузі інформації і комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудову та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудову глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформація як суспільне благо, інформація як товар, інформація як невіддільний компонент існування держави (необхідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин); недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; творення урядової політики в галузі інформації і комунікації.

Американський досвід державної політики у сфері інформаційної безпеки може бути актуальним для багатьох питань української зовнішньої та внутрішньої політики. Насамперед необхідно звернути увагу на такі аспекти американського досвіду в сфері забезпечення інформаційної безпеки, як: найбільш ефективний підхід до регулювання ринку інформаційних технологій в умовах ринкової економіки. Україна має достатній потенціал для того, щоб бути повноправним учасником інформаційного суспільства. Зазначимо, що ефективність державної політики грає не менш важливу роль порівняно з рівнем технологічного розвитку. Хоча відставання України від світових лідерів у інформаційній сфері в останні роки скорочується, зберігається наша залежність від іноземних інформаційних технологій та програмного забезпечення. Це створює суттєву загрозу національній безпеці України. Україні, як і іншим державам, необхідно виробити виважену політику держави в цій сфері.

Зважаючи, що інформаційна проблематика є транснаціональною, особливе значення для розвитку правової системи України має узгодження з міжнародними стандартами у цій сфері, що також потребує внесення змін та доповнень до чинного вітчизняного інформаційного законодавства. Інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації. Крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність.

Інформаційні системи можна розділити на три частини:  програмне забезпечення, апаратне забезпечення та комунікації з метою цільового застосування (як механізму захисту і попередження) стандартів інформаційної безпеки. Самі механізми захисту реалізуються на трьох рівнях або шарах: фізичному, особистісному та організаційному. По суті, реалізація політик і процедур безпеки покликана надавати інформацію адміністраторам, користувачам і операторам про те як правильно використовувати готові рішення для підтримки безпеки.

Безпека і захист інформаційної системи має будуватись з урахуванням комплексного відходу до структури системи захисту, що передбачає об’єднання в єдиний комплекс відповідних заходів та засобів захисту інформації на всіх рівнях системи інформаційного забезпечення.

2.3. Система органів, які здійснюють контроль над дотриманням збереження

конфіденційної інформації в Україні та зарубіжних країнах

Орган державної влади або місцевого самоврядування, юридична або фізична особа, яка відповідно до законодавства України може бути учасником відносин, що регулюються нормами інформаційного права, є суб’єктами інформаційного права. Так, згідно зі ст. 7 Закону України “Про інформацію” суб’єктами інформаційних відносин є громадяни України, юридичні особи та держава. Суб’єктами інформаційних відносин можуть бути також інші держави, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства. Проте, щоб стати учасником інформаційних правовідносин, суб’єкт повинен мати інформаційну правосуб’єктність, яка складається з інформаційної право- та дієздатності. Інформаційна правоздатність – це можливість конкретного суб’єкта набувати інформаційних прав і обов’язків і нести юридичну відповідальність за їх практичну реалізацію. Кожний, хто наділений правами та обов’язками в інформаційній сфері, може розглядатися як суб’єкт інформаційного права. Однак такий суб’єкт інформаційного права може стати суб’єктом інформаційних правовідносин лише за наявності другого елемента правосуб’єктності – інформаційної дієздатності, тобто здатності суб’єкта своїми діями набувати прав, створювати для себе юридичні обов’язки, а також нести відповідальність за свої дії в інформаційній сфері.

Джерелом інформаційного права виступають норми інформаційного законодавства, що забезпечують регулювання відносин в інформаційній сфері. Ці джерела можуть бути скласифіковані в кілька груп:

1. Норми Конституції України – закріплюють інформаційні права і свободи, встановлюють права і обов’язки суб’єктів інформаційних відносин з приводу створення та поширення інформації певного виду, а також встановлюють обмеження обігу інформації в державі та суспільстві.
2. Галузі законодавства – присвячені питанням інформаційного права. До них належать:

* законодавство про засоби масової інформації;
* законодавство про формування інформаційних ресурсів, інформаційних продуктів, надання інформаційних послуг (про правову інформацію, персональні дані, бібліотечну справу, архіви, музеї, рекламу, видавничу діяльність, статистичну інформацію, міжнародний обмін інформацією тощо);
* законодавство, що регламентує порядок реалізації права на пошук, отримання, передачу та використання інформації;
* законодавство про створення та використання інформаційних систем, їх мереж, інших інформаційних технологій і засобів їх забезпечення;
* законодавство про інформаційну безпеку.

1. Окремі інформаційно-правові норми – входять до складу інших галузей права України. Ці норми включаються в:

* нормативні акти, що регламентують правовий статус відповідних структур (Конституція України, конституційні та звичайні закони, які визначають статус органів державної влади);
* нормативні акти цивільного законодавства, які розглядають питання реалізації права власності на інформацію;
* нормативні акти, що регулюють відносини в різних галузях господарської діяльності (законодавство про землю, надра, охорону природи тощо), які супроводжуються створенням інформації певного виду та призначення;
* нормативні акти про відповідальність за правопорушення в інформаційній сфері.

Практично в усіх зарубіжних країнах діють спеціальні інституції, відповідальні за реалізацію права на доступ до інформації. В одних країнах – це тимчасові органи, спеціально створені після прийняття законів про доступ до інформації і уповноважені здійснювати контроль за виконанням цих законів. В інших країнах – це постійні інституції, спеціально уповноважені забезпечувати реалізацію права на доступ до інформації. У країнах, де немає спеціального закону про доступ до інформації, а таке право закріплено у конституції, вказані функції покладено на парламенти, омбудсмени та суди. Так, досвід зарубіжних країн свідчить про такі моделі спеціальних інституцій:

1. Cпеціальний орган контролю за забезпеченням права на доступ до інформації в рамках виконавчої влади (Бельгія, Ісландія, Естонія, Польща, Таїланд, Японія тощо).
2. Cпеціалізований омбудсмен з питань інформації або колегіальний орган, що буде здійснювати незалежний парламентський контроль за охороною та захистом права на доступ до інформації (Великобританія, Ірландія, Угорщина, Словенія, Німеччина, Сербія, Канада тощо).
3. Уповноважений з прав людини або службовий підрозділ чи спеціальний представник для здійснення контролю за забезпеченням конституційного права на інформацію у межах апарату уповноваженого з прав людини (Швеція, Данія, Бельгія, Фінляндія, Австрія, Нідерланди, Польща тощо).

Орган контролю, який формально створюється при уряді або парламенті, але до його складу входять представники законодавчої, виконавчої, судової гілки влади, представники від громадськості та органів місцевого самоврядування (Франція, Португалія тощо).

За останні роки в Чехії реалізовано комплекс заходів із удосконалення забезпечення її інформаційної безпеки. Розпочато формування бази правового забезпечення інформаційної безпеки, прийнято низку законів, розпочато створення механізмів їхньої реалізації. Здійснюються певні заходи із забезпечення захисту інформації в органах державної влади, на підприємствах, в установах і організаціях усіх форм власності. Запроваджується створення захищеної інформаційно-телекомунікаційної системи спеціального призначення в інтересах органів державної влади.

Основним документом, що регламентує діяльність органів, які забезпечують інформаційну та державну безпеку, є «Стратегія Національної безпеки Чеської Республіки». Головним органом, що забезпечує інформаційну безпеку Чехії є Служба інформаційної безпеки (Bezpečnostní informační služba (BIS), яку було утворено 1 січня 1993 року. Діяльність зазначеної служби регламентується законами Чеської Республіки «Про розвідувальні служби Чеської Республіки», «Про інформаційну безпеку» та «Про захист секретної інформації». Діяльність Служби інформаційної безпеки не є публічною, але здійснюється із суворим дотриманням законів, у тісній співпраці із поліцією, розвідкою, чеськими правоохоронними органами та правоохоронними органами країн-партнерів.

Проаналізувавши міжнародне законодавство та законодавство деяких зарубіжних країн про охорону комерційної таємниці, можна зробити висновок, що на сьогодні український законодавець ще недостатньо приділяє уваги як специфіці, так і окремим видам правового забезпечення захисту комерційної таємниці. Крім того, треба відзначити, що чинне законодавство встановлює тільки загальні правила у сфері виявлення, збору, аналізу та передачі інформації, яка зазначена як комерційна.

2.4. Заходи спрямовані на захист конфіденційної інформації та комерційної таємниці у сфері IT в Україні та зарубіжних країнах

Порушення прав на комерційну таємницю тягне за собою дисциплінарну, цивільно-правову, адміністративну, кримінальну відповідальність згідно із законодавством України. Так, особа, яка в результаті трудових відносин із власником комерційної таємниці – роботодавцем володіє комерційною таємницею, у випадку умисного або необережного її розголошення за відсутності у цих діях складу злочину, несе дисциплінарну або цивільно-правову відповідальність.

Цивільно-правова відповідальність. Згідно зі ст. 1166 Цивільного кодексу України майнова шкода, завдана неправомірними рішеннями, діями чи бездіяльністю особистим немайновим правам фізичної або юридичної особи, а також шкода, завдана майну фізичної або юридичної особи, відшкодовується в повному обсязі особою, яка її завдала.

Моральна шкода, завдана фізичній або юридичній особі неправомірними рішеннями, діями чи бездіяльністю відшкодовується особою, яка її завдала, за наявності її вини (ст. 1167 Цивільного кодексу України). У разі порушення встановленого режиму комерційної таємниці завдана моральна шкода може виражатися в приниженні честі, гідності, а також ділової репутації фізичної або юридичної особи, а розмір грошового відшкодування моральної шкоди визначатиметься судом залежно від характеру правопорушення, ступеня вини особи, яка завдала моральної шкоди, а також з урахуванням інших обставин, які мають істотне значення.

Підставою для відшкодування матеріальної і моральної шкоди є рішення суду. Адміністративно-правова відповідальність. Законом України “Про захист від недобросовісної конкуренції” встановлюється відповідальність за неправомірне збирання комерційної таємниці та її розголошення, неправомірне використання та схиляння до розголошення комерційної таємниці (ст. 16-19). Відповідно до законодавства ці правопорушення визнаються недобросовісною конкуренцією. У свою чергу, згідно з Господарським кодексом України неправомірним збиранням відомостей, що становлять комерційну таємницю, вважається добування протиправним способом зазначених відомостей, якщо це завдало чи могло завдати шкоди суб’єкту господарювання. Розголошенням комерційної таємниці є ознайомлення іншої особи без згоди уповноваженої на те особи, з відомостями, що відповідно до закону становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв’язку з виконанням службових обов’язків, якщо це завдало чи могло завдати шкоди суб’єкту господарювання. Схилянням до розголошення комерційної таємниці є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв’язку з виконанням службових обов’язків відомості, що відповідно до закону становлять комерційну таємницю, до їх розкриття, якщо це завдало чи могло завдати шкоди суб’єкту господарювання. Неправомірним використанням комерційної таємниці є впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до закону комерційну таємницю. За неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею, винні особи несуть відповідальність, встановлену законом.

Так, згідно зі ст. 164–3 Кодексу України про адміністративні правопорушення отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця тягне за собою накладення штрафу від дев’яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян.

Кримінально-правова відповідальність. Законодавством передбачена і кримінальна відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю та за її розголошення. Так, згідно зі ст. 231 Кримінального кодексу України умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності, – караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п’яти років, або позбавленням волі на термін до трьох років. Згідно зі ст. 232 Кримінального кодексу України умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв’язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб’єкту господарської діяльності, – карається штрафом від двохсот до п’ятисот неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на термін до трьох років, або виправними роботами на термін до двох років, або позбавленням волі на той самий термін. При цьому шкода вважається істотною, якщо вона в триста і більше разів перевищує неоподаткований мінімум доходів громадян.

У сфері інформаційних технологій інформація, що представляє собою велике значення для функціонування кожної конкретної компанії, напрацювання співробітників таких компаній, що виявляють конкурентні переваги однієї компанії над іншою, вирізняють компанії поміж компаній-конкурентів зберігаються на комп’ютерах, жорстких дисках та у хмарному сховищі. При захисті комп’ютерних систем від несанкціонованого доступу треба враховувати специфіку їх використання. Як, правило, окремим комп’ютером користується обмежена кількість користувачів. ПК можуть функціонувати як в автономному режимі, так і у складі локальних мереж, підключатися до глобальної мережі Internet тощо.

**Захист ПК від несанкціонованого доступу**

Засоби захисту обчислювальних ресурсів (використання парольної ідентифікації)

Застосування різноманітних методів шифрування інформації

Засоби захисту від копіювання комерційних програм

Захист від комп’ютерних вірусів

Для захисту конфіденційної інформації за допомогою парольної ідентифікації можна використати апаратні засоби встановлення паролю на запуск операціїної системи за допомогою установок в CMOS Setup. Однак, використання такої парольної ідентифікації не є надійним, для подолання такого захисту достатньо, наприклад, ввести універсальний пароль (AWARD\_SW) або відключити акумуляторні батарею комп’ютера.

Щодо судових справ у вирішенні питань порушення комерційної таємниці, яскравим прикладом є справі №1355/12 ПП. «Н-ВФ «Лад» звернувся до Соснівського районного суду м. Черкас з позовом до фізичної особи про відшкодування збитків, завданих розголошенням відомостей, що складають комерційну таємницю. З тексту рішення випливає, що відповідач працював в ПП «ЛАД» на посаді інженера-системотехніка. Під час роботи мав доступ до технічної документації по технології виробничого процесу нанесення вакуумного покриття нітриду титану на підкладку листової нержавіючої сталі. Будучи співробітником, підписав договір про нерозголошення комерційної таємниці, до якої роботодавець відніс документацію з технології вказаного процесу. Після звільнення, відповідач створив конкуруюче підприємство ТОВ «НПФ «Покров», одним з основних видів діяльності якого також є нанесення вакуумного покриття нітриду титану на підкладку листової нержавіючої сталі. Суд дійшов висновку що способом захисту прав на комерційну таємницю – є подання позову про відшкодування збитків завданих розголошенням відомостей, що складають комерційну таємницю. В якості розрахунку збитків суд прийняв суму отриманого товариством «Покров» прибутку у розмірі 26 620 грн. Визначивши, що відповідач порушив письмове зобов’язання «Про нерозголошення комерційної таємниці» Суд вирішив позов задовольнити, а також стягнув на користь приватного підприємства «Науково-виробнича фірма «Лад» збитки, завдані розголошенням відомостей, що складають комерційну таємницю в розмірі 26 620 грн.

Проте, 19 березня 2014 рішення суду першої інстанції скасовано Ухвалою Вищого господарського суду України. Касаційний суд, зокрема, зазначив, «задовольняючи позовні вимоги та стягуючи збитки, завдані розголошенням відомостей, що складають комерційну таємницю, в розмірі 26 620,00 грн., керуючись при цьому положеннями ст. 22 ЦК України, суди не обґрунтували застосування вказаної норми до правовідносин, що виникли між сторонами та не визначились з нормою закону, яка визначає таку відповідальність. Крім того, суди не визначили, якими доказами підтверджується наявність причинно-наслідкового зв’язку між діями відповідача та заподіянням збитків позивачу саме у розмірі доходу, отриманого новоствореним підприємством відповідача, яке проводить власну комерційну діяльність».

Не вдалося відшкодувати майнові збитки й в іншому аналогічному випадку. Суть справи № 6-14136СВ13 полягала в тому, що ТОВ «АЙЛІС» (далі – Товариство) звернулося до Комінтернівського районного суду м. Харкова з позовом до двох фізичних осіб-підприємців, які були працівниками даного Товариства, про стягнення завданих майнових збитків у вигляді упущеної вигоди від витоку, розголошення і незаконного використання комерційної таємниці та дій з недобросовісної конкуренції.

На підставі трьохстороннього договору між позивачем та відповідачами було укладено Угоду про нерозголошення комерційної таємниці, відповідно до якої користувачі комерційної інформації, в тому числі працівники, про яких йде мова, зобов’язалися не розголошувати інформацію: про місце, дату та вартість виготовлення спідньої (нижньої) білизни конкретної торгівельної марки, інформацію про підрядні організації, що займаються виготовленням спідньої (нижньої) білизни цієї торгівельної марки та інформацію про існуючі цивільно-правові відносини цих підрядних організацій, посередників та кінцевих споживачів продукції, товарів та послуг, а також іншу інформацію комерційного характеру.

Посилаючись на те, що відповідачі вступили у протиправну змову про наміри та дії щодо державної реєстрації власної торгової марки та Інтернет сайту, а також спільну організацію власного виробництва без відповідної державної реєстрації на основі бази ТОВ «АЙЛІС» з протиправним отриманням, розголошенням комерційної таємниці та конфіденційної інформації та використанням у своїй діяльності заходів та методів недобросовісної конкуренції, що призвело до зниження продажу товару, позивач просив суд стягнути з в солідарному порядку з відповідачів на свою користь майнові збитки у вигляді упущеної вигоди від витоку, розголошення і незаконного використання комерційної таємниці та дій з недобросовісної конкуренції у розмірі 668 386,00 гривень 25 копійок. Рішенням районного суду позов було задоволено.

Проте, скасовуючи рішення суду першої інстанції та ухвалюючи нове про відмову у задоволенні позову, апеляційний суд Харківської області вірно виходив з того, що позивачем не надано доказів зниження обсягу продажу товару та настання прямих майнових збитків внаслідок дій відповідачів. Крім того, апеляційний суд дійшов висновку про безпідставність посилання позивача на Закон України «Про захист від недобросовісної конкуренції», як на підставу відповідальності відповідачів, оскільки даний Закон застосовується до відносин, у яких беруть участь суб’єкти господарювання, яким один з відповідачів не є, а вимоги до іншого відповідача, як суб’єкта підприємницької діяльності, повинні розглядатися в суді господарської юрисдикції.

​ Проте, як і в попередньому випадку, справа дійшла до вищої судової інстанції – касаційну скаргу Товариства на рішення апеляційного суду року суд відхилив.

У задоволені позовних вимог фізичної особи-підприємця до іншої фізичної особи-підприємця про стягнення збитків завданих розголошенням відомостей, що становлять комерційну таємницю в розмірі 136 930,00 грн. відмовив і Господарський суд Волинської області у справі № 903/1027/16. На думку суду, не доведеним є той факт, що відповідач був ознайомлений з положенням позивача «Про комерційну таємницю та правила її зберігання», а також позивачем не доведено факту (не надано суду належних та допустимих доказів) саме розголошення відповідачем відомостей, що становлять комерційну таємницю, зокрема щодо бази даних і кому саме.

Проте, сторона, що позивається, може також вимагати стягнення з винної сторони штрафу за розголошення інформації, який, до речі, є мірою відповідальності за договором NDA і ви ж самі можете його прописати. Прикладом такої ситуації є судове рішення від 21.02.2017 в справі № 760/9029/16-ц Апеляційний суд м. Києва.

ТОВ «ГУД ПАРТНЕРС» звернулося до суду з позовом до колишнього працівника, в якому, просило стягнути з останнього на свою користь штраф розмірі 50 000 грн. та витрати на правову допомогу розмірі 20 300 грн. Будь-яких інших доказів, окрім двох листів, отриманих від третіх осіб, в яких відповідач наче б то звернувся з пропозицією подальшої співпраці та замовлення у нього як постачальника товарів, аналогічних товарам позивача та за меншою ціною аніж ціна позивача, про розповсюдження такої інформації позивач не надав.

Суд з’ясував, що листи не містили інформації, яку нібито стороннім особам повідомив відповідач та яка є конфіденційною. У зазначених листах також не зазначено про яку собівартість товарів і послуг повідомив відповідач, який розмір цін та який рівень прибутку має позивач. Відтак, відмовляючи в задоволенні позовних вимог, суд першої інстанції виходив з недоведеності позивачем факту розголошення відповідачем конфіденційної інформації та передання відповідачу такої інформації позивачем. Окрім того, доказів про перерахування коштів у розмірі 20 300 грн. за надання правової допомоги позивач також не мав. Апеляційний суд м. Києва Рішення Солом’янського районного суду м. Києва від 13 жовтня 2016 року вирішив залишити без змін.

Правова охорона комерційної таємниці в Сполучених Штатах Америки ґрунтується, головним чином, на законодавстві кожного штату окремо. Єдиним видом правової охорони комерційної таємниці, що існує в даний час на федеральному рівні, є встановлення кримінальної відповідальності за крадіжку та незаконне присвоєння відомостей, які становлять комерційну таємницю, а також за «економічне шпигунство». Закон, котрий часто називається як «Акт про економічне шпигунство» (Economic Espionage Act), міститься в частині 18, §1831 – 1839 Кодексу законів США.

У цілому, законодавство штатів забороняє незаконне присвоєння секретних відомостей, що становлять комерційну таємницю. Визначення комерційної таємниці, наведене в Законі, включає нові технології, за допомогою яких здійснюється створення і зберігання комерційної таємниці. Так, до комерційної таємниці відносяться всі види і форми фінансової, комерційної, наукової, технічної та економічної інформації, включаючи моделі, креслення, програми, формули, ідеї, прототипи, методики, технології, процедури або коди, що зберігаються будь-яким способом, за умови, що власник вжив розумних зусиль для збереження секретності, а інформація має самостійну економічну цінність завдяки відсутності до неї доступу з боку інших осіб.

Обов’язок зберігати комерційну таємницю в секреті може встановлюватися контрактом, наприклад, угодою про конфіденційність, або передбаченим законом зобов’язанням зберігати відомості, що становлять комерційну таємницю, в секреті у зв’язку із зайняттям відповідальної посади. Крім прямих правопорушень суди приймають до розгляду позови про співучасть (vicarious infringement) і відповідальність за дії інших осіб. Таким чином, особа, яка підбурює іншу особу порушити чиїсь права, або особа, яка надає допомогу в такому правопорушенні, несуть однакову відповідальність.

Оскільки в результаті несанкціонованого використання або розголошення відомості, що становлять комерційну таємницю, можуть втратити свою цінність, найважливішими способами збереження таємниці за законодавством США є судові заборони з метою запобігання потенційного або фактичного незаконного присвоєння комерційної таємниці. Способи захисту прав на комерційну таємницю, що містяться в законодавстві США, включають мінімальні стандарти захисту прав, передбачені Угодою про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС), серед яких – судові заборони, відшкодування збитків, відшкодування витрат на послуги адвоката та судові витрати, вилучення товарів, з якими пов’язані правопорушення, або їх знищення.

|  |  |
| --- | --- |
| **Захист прав та відшкодування збитків у США за порушення комерційної таємниці або незаконе присвоєння інформаціїї, що є комерційною таємницею** | |
| Судові заборони (Injunctions) | Тимчасові, попередні або остаточні заборони можуть бути видані судом на тих умовах, які він вважатиме виправданими, для запобігання або припинення фактичного чи потенційного незаконного присвоєння відомостей, що становлять комерційну таємницю. |
| Відшкодування збитків у грошовій формі (Money Damages) | Відповідач може відповідати за фактичні збитки власника прав на комерційну таємницю у зв’язку з незаконним присвоєнням відомостей, що її становлять, а також за одержання прибутків або економічної переваги в результаті такого незаконного присвоєння, які не бути враховані при розрахунку збитків власника прав на комерційну таємницю. У випадку умисного або злочинного незаконного присвоєння відомостей, що становлять комерційну таємницю, суди присуджують виплату штрафних санкцій у сумі, яка не перевищує подвійної суми фактичних збитків. |
| Гонорар адвокатів і судові витрати | суд може також винести рішення про відшкодування стороні, на користь якої винесено рішення, судових витрат, а також витрат на послуги адвоката. Під «винятковими» випадками зазвичай маються на увазі умисні або злочинні правопорушення. У справах про недобросовісне присвоєння відомостей, що становлять комерційну таємницю, також присуджується, як правило, відшкодування витрат на послуги адвоката. |
| Вилучення предметів, що порушують права | Суд може розпорядитися про вилучення всіх предметів, які, як стверджується, порушують права на комерційну таємницю. До числа таких предметів відносяться матеріальні носії, які містять відомості, а також майстер-файли, товари тощо, що містять комерційну таємницю або вироблені з її використанням. |
| Знищення | Суд може також винести рішення про знищення всіх предметів, що порушують права на комерційну таємницю, та/або повернення матеріальних носіїв, які містять відомості, що становлять комерційну таємницю, відповідачу або під його контроль. |
| Відповідальність за дії інших осіб (vicarious liability) та співучасть (contributory infringement) | Особи, які свідомо і навмисно сприяють правопорушенням або заохочують до їх вчинення, несуть відповідальність нарівні з безпосереднім правопорушником і підпадають під такі ж самі покарання. Такі особи відповідають за сприяння у правопорушенні (якщо вони знали про правопорушення або мали підстави знати про набуття відомостей, що становлять комерційну таємницю, неналежними засобами), а також спонукання, заохочення або матеріальну підтримку такої діяльності. |
| Застава і гарантії | За законодавством США суд може вимагати від правовласника внести заставу в розумних розмірах, щоб гарантувати компенсацію відповідачу у випадку, коли арешт буде визнаний неправомірним. |

У законодавстві Франції комерційну таємницю визначено як інформацію, що використовується компанією та є основою її конкурентоспроможності, а також зберігається в конфіденційності. Законодавство Франції включає такі напрями захисту комерційної таємниці:

1. В рамках трудових відносин на працівника покладається обов’язок підтримувати режим конфіденційності інформації, працівник не має права конкурувати з роботодавцем після звільнення.
2. Передбачена цивільно-правова відповідальність за «зловживання довірою», тобто розголошення комерційної таємниці особою, якій вона довірена володарем.
3. Передбачена кримінальна відповідальність для державних службовців та посадових осіб контролюючих органів за розголошення конфіденційної інформації.

У Швецарії суди тлумачать поняття комерційної таємниці як технічну або комерційну інформацію, що впливає на комерційні результати діяльності підприємства, яка не є добре відомою та загальнодоступною, яку власник не відкриває, зважаючи на власні законні інтереси. Злочином є розкриття комерційної інформації закордонній державі фбо фірмі, а також використання переваг від відомостей, які є комерційною таємницею, або зловживання ними та забороняє всі методи конкуренції, повязані з використанням комерційної таємниці, одержаної шляхом порушення умов конфіденційності. За такі дії передбачається накладання штрафів. У ст.4 цього Закону заборонено спонукання працівника до розголошення комерційної таємниці, що є деліктом, як і розкриття технічної або торговельної таємниці, одержаної незаконно. Деліктом так само є використання відомостей третьоє стороною, якщо вона знає, що вони одержані неправомірно. Якщо будь-який з наведених деліктів був учинений особою свідомо або навмисно, то вона підлягає кримінальній відповідальності.

Законодавство Німеччини встановлює обов’язок посадових осіб державних контролюючих органів дотримуватися режиму конфіденційності інформації та передбачає відповідальність за її розголошення, аж до кримінальної. Процесуальне законодавство Німеччини передбачає гарантії збереження конфіденційності ноу-хау в процесі судового розгляду. Суть їх полягає у вилученні з принципу гласності розгляду справ судом: «Слухання справи в закритому засіданні допускається ... при задоволенні судом клопотання особи, що бере участь у розгляді та посилається на необхідність збереження комерційної та іншої таємниці». Кримінальне покарання, передбачене процесуальним законодавством Німеччини за розголошення торгового секрету, варіюється від штрафу до позбавлення волі до 1 року, що не виключає також відшкодування завданих збитків.

В англійському праві використовуються три принципи, які застосовуються до будьякого порушення конфіденційності:

* якщо інформація передається на умовах конфіденційності, то особа, що одержала її, не має права використовувати або розкривати цю інформацію з метою створення конкуренції власнику інформації;
* якщо доведено, що відповідач умисно або ненавмисно розкрив конфіденційну інформацію без згоди власника, він визнається винним у порушенні прав власника інформації;
* особа, що отримала конфіденційну інформацію, не має права використовувати її раніше, ніж власник інформації, для заняття найбільш вигідних позицій, навіть якщо зміст цієї інформації був опублікований або може бути встановлений третіми особами шляхом власних досліджень. Передбачається, що власник конфіденційної інформації повинен мати певну перевагу перед всією рештою осіб і бути упевненим, що не запізниться на старті в умовах жорсткої конкуренції.

У разі порушення конфіденційності до порушника застосовуються такі заходи:

* винесення ухвали суду, яка може мати «проміжну» (слугує лише для запобігання подальшому спричиненню шкоди до прийняття остаточного рішення по справі) або «постійну» дію;
* взяття відповідачем зобов’язання під присягою передати позивачу або знищити фізичні об’єкти, в які втілені ноу-хау або торговий секрет (позивач може на свій розсуд вибрати ту або іншу міру);
* компенсація за збитки або упущену вигоду, які стали результатом порушення зобов’язань про конфіденційність.

Третя міра полягає у відшкодуванні збитків, викликаних порушенням конфіденційності.

2.5. Договір про нерозголошення конфіденційної інформації (Non‑disclosure agreement) в українському  IT та зарубіжних країнах: порівняльний аналіз

Кожна людина, з моменту народження, а кожна юридична особа з моменту заснування набувають певну інформацію, яка, в майбутньому, розширяючись, складає нематеріальну основу їх діяльності. Юридичні та фізичні особи набувають інформацію затрачуючи час, фінансові засоби та інтелектуальний потенціал. Тому безспірною є ідея про те, що рівним захистом повинна користуватися як сама людина чи організація, так і всі їх складові, в тому числі й інформаційні. Розглянемо особливості та специфічні риси договору про нерозголошення конфіденційної інформації (комерційної таємниці). Варто розпочати аналіз з загальних теоретичних положень щодо договору в цивільному праві.

Договір – це домовленість двох і більше осіб, спрямована на встановлення, зміну або припинення цивільних прав та обов’язків. Поняття договору розкривається через поняття угоди. Договори – це дво – або багатосторонні угоди. Треба згадати, що договір у цивільному праві являє собою угоду, яка вчиняється на підставі погодження волі сторін з приводу певних прав і обов’язків. Воля сторін у договорі повинна бути взаємною і погодженою, тобто збігатися як за обсягом, так і за змістом.

Договір про нерозголошення конфіденційної інформації – це угода між правовласником та зацікавленою стороною про дотримання конфіденційної інформації (комерційної таємниці), за розголошення якої передбачена відповідальність. Договори про нерозголошення конфіденційної інформації як правило визначають, що конкретно є конфіденційною інформацією. В цьому контексті можна сказати, що Договір знімає один рівень захисту, так як тепер нова особа проінформовано, що саме цінне й захищається в компанії.

Об’єктом даного договору є конфіденційна інформація (комерційна таємниця), тому слід проаналізувати чинне законодавство та доктринальні розробки для з’ясування одного з провідних питань даної роботи: що відноситься до комерційної таємниці. Необхідно визнати, що в країнах світу, де використовуються інформаційні об’єкти, які представляють комерційну цінність, не має єдиного підходу до визначення поняття такої інформації. Застосовують різні визначення: «ділові секрети», «виробничі секрети», «торгівельні секрети», «конфіденційна інформація», «комерційна таємниця» тощо. Питання щодо змісту інформації, яка становить комерційну таємницю завжди викликало багато дискусій. Наприклад, щодо кореляції понять комерційної таємниці (конфіденційної інформації та інформації взагалі) та інтелектуальної власності. Інформація, згідно з законодавством України, є об’єктом права власності, але вона одночасно може бути і об’єктом права інтелектуальної власності. Закон України «Про інформацію» під поняттям «інформація» розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

За своєю природою договори про конфіденційність є цивільноправовими, оскільки їх об‘єктом є інформація, яка відповідно до статей 177, 200 ЦК України є об‘єктом саме цивільних прав, хоча можуть укладатись і в тих сферах, де превалюючим є регулювання іншої галузі права, наприклад у сфері трудових відносин. Маючи цивільно-правову природу, договір про конфіденційність, однак не має свого окремого спеціального законодавчого врегулювання. Законним підґрунтям його укладання є ч.1 ст.6 ЦК України, згідно якої сторони мають право укласти договір, який не передбачений актами цивільного законодавства, але відповідає загальним засадам цивільного законодавства.

Договір є двостороннім, реальним. Природа Договору зумовлена також прагненням учасників правовідносин попередити негативні наслідки з боку робітників, партнерів чи третіх осіб. Такої стратегії, наприклад дотримуються володільці веб – ресурсів і інформаційних продуктів, коли попереджають про відповідальність за незаконне використання контента чи інформаційної бази даних. Далі, при порушенні зобов’язанні діє популярна конструкція відповідальності, яку ще часто називають концепцією розумної людини, відома у вітчизняній юриспруденції під конструкцією особи, яка «знала та повинна була знати» про порушення. Договір в значній мірі дозволяє уникнути розголошенню конфіденційної інформації та наступних судових засідань. Договір про нерозголошення (NDA) актуальний для таких індустрій:

* торгівля (приховати інформацію про постачальників, про скрипти продажу товарів тощо);
* сільське господарство (приховати інформацію про способи обробки земельних ділянок, про технічні інструменти тощо);
* ІТ (тут спектр комерційної таємниці дуже широкий: програмний код, програмний застосунок, не запатентована інформація, моделі роботи тощо);
* сфера послуг (туризм, ресторанна справа тощо);
* виробництво (секрет виробництва продукції, секрет компонентів виробу тощо.

Природа Договору зумовлена також прагненням учасників правовідносин попередити негативні наслідки з боку робітників, партнерів чи третіх осіб. Такої стратегії, наприклад дотримуються володільці веб – ресурсів і інформаційних продуктів, коли попереджають про відповідальність за незаконне використання контента чи інформаційної бази даних. Договір в значній мірі дозволяє уникнути розголошенню конфіденційної інформації та наступних судових засідань.

Практика діяльності ділового товариства показує, що договір про нерозголошення конфіденційної інформації можна заключати в спрощеній формі. При цьому відсутні в ньому положення можуть бути доповнені диспозитивними нормами законодавства. Тим паче, суттєві умови договору, під загрозою його недійсності все-таки повинні бути окреслені. Припускається, що суттєві умови Договору крім обов’язкової (предмет договору) повинні включати: термін конфіденційності, обов’язок нерозголошення, відповідальність сторін. Також це можуть бути випадкові умови договору, тобто такі, які не містяться в договорах певного виду, проте можуть бути внесені за згодою сторін.

Аналоги і адаптації non-disclosure agreement (NDA) під правову систему України зустрічаються під такими назвами: Договір про нерозголошення конфіденційної інформації; Договір про нерозголошення інформації, що становить комерційну таємницю (зовсім не те саме, що конфіденційна інформація); Угода про конфіденційність; Угода про нерозголошення та інші. Умови, які можуть бути розглянуті при укладенні Договору наступні:

* чітке окреслення конфіденційної інформації та строку початку й закінчення конфіденційності. Повинно бути вказано, що зобов’язання конфіденційності існує як в період дії договору так й після неї;
* переконатися в тому, що мета, для якої конфіденційна інформація передана чітко розписана, та отримавши сторона не може використовувати інформацію для інших цілей;
* переконатися в тому, що не має ніякої підрозуміваємої ліцензії на інтелектуальну власність в конфіденційній інформації;
* захистити себе від будь-якої потенційної відповідальності за конфіденційну інформацію.

Важливою умовою при укладенні Договору є строк чинності права інтелектуальної власності на комерційну таємницю. Відповідно до Ст. 508 ЦК України строк чинності права інтелектуальної власності на комерційну таємницю обмежується строком існування сукупності ознак комерційної таємниці, встановлених ч.1 ст. 505 ЦК України.

Розглянемо структуру типового Договору про нерозголошення. Окрім назв розділів Ви знайдете короткі коментарі, які допоможуть Вам зорієнтуватись і прийняти правильне рішення при вивченні або підписанні non-disclosure agreement, складеного відповідно до вимог законодавства України. Отже, типова структура Угоди про **нерозголошення виглядає наступним чином:**

1. **Предмет договору – цей розділ розміщується одразу за преамбулою Угоди про нерозголошення. Предмет договору (угоди) кратко і чітко виражає суть угоди, вказує на відносини, які виникають між сторонами, обов’язки сторін.**
2. Права і обов’язки сторін – даний розділ угоди містить деталізований виклад прав і обов’язків сторін. Для non-disclosure agreement (NDA) зазвичай притаманна ситуація, коли обов’язки носять переважно однобічний характер (лише одна сторона бере на себе обов’язок утримуватись від розголошення і розкриття конфіденційної інформації). Якщо Ви та сторона, яка приймає на себе такий обов’язок, радимо уважно поставитись до відповідних положень угоди і визначити чи зможете Ви виконати взяті на себе обов’язки після того, як Ваші відносини з контрагентом або роботодавцем за основним договором будуть припинені.
3. Допустиме розкриття інформації – даний розділ містить так би мовити виключення з основних положень Угоди про нерозголошення. Тобто випадки, коли допустимо відступити від взятих на себе зобов’язань, не порушуючи умов угоди в цілому. Наприклад, це може бути розкриття (надання) інформації, яка захищена угодою, на запит правоохоронних та інших компетентних органів (суди, органи досудового розслідування Національної поліції, Служби безпеки України тощо).
4. Відповідальність сторін – назва цього розділу говорить сама за себе. Рекомендуємо вкрай уважно ставитись до положень цього розділу угоди. Така порада стосується обох сторін. Відсутність адекватного рівня відповідальності у разі несанкціонованого розкриття інформації не зможе забезпечити належну ефективність роботи Угоди про нерозголошення.
5. Особливі умови (або Додаткові положення). Наповнення даного розділу багато в чому залежить від сфери основних відносин (основного договору) в яких перебувають сторони Угоди про нерозголошення.
6. Форс-мажор та обставини непереборної сили. Типовий розділ будь-якого договору, який не має вкрай суттєвих особливостей для Угоди про нерозголошення або інших варіацій non-disclosure agreement.
7. Дія договору (угоди) – радимо вказати чіткий строк дії угоди. Саме в цьому розділі зазначаються підстави та порядок припинення дії угоди (у тому числі з ініціативи однієї та/або обох сторін). Цей розділ може містити деталізовані наслідки припинення дії угоди у тому чи іншому випадку.
8. Порядок вирішення спорів. Враховуючи особливість NDA і окремі правові прогалини, рекомендуємо окрім судового порядку вирішення спорів передбачити процедуру медіації.
9. Заключні положення і визначення термінів. Угода про нерозголошення не відрізняється особливими відмінностями в частині змісту розділу “Заключні положення”. Доцільно передбачити вказівку на те, що визнання окремих положень угоди недійсними не тягне за собою недійсність угоди в цілому.
10. Визначення термінів – розділ (або підрозділ) Угоди про нерозголошення, який вимагає відповідального підходу. Нетиповість аналогів NDA для правової системи України і відносно нова сфера відносин, де застосовуються такі угоди, обумовлюють необхідність детального розкриття окремих термінів. Визначення термінів зазвичай наводиться на початку або, навпаки, наприкінці угоди.
11. Реквізити і підписи сторін. З цим розділом немає виникати питань. Єдина порада – перевіряйте повноваження особи, яка підписує угоду від імені Вашої компанії. Трапляються випадки, коли підписантом виступає менеджер, який немає повноважень ні за статутними документами компанії, ні за відповідної довіреністю.

Основні права володільців комерційної таємниці такі:

* суб'єкт права на комерційну таємницю може використовувати всі допустимі законом засоби для забезпечення секретності інформації;
* правоволоділець має право вимагати від інших осіб утримуватися від незаконного володіння інформацією, що становить комерційну таємницю;
* володілець комерційної таємниці має право розпоряджатися належним йому об'єктом інтелектуальної власності (розголошувати перед публікою, продавати, перевідступати іншим способом). Суб'єкт права на комерційну таємницю може давати іншим особам дозвіл на використання конфіденційної інформації у власній сфері. Тобто допускають видачу іншим особам ліцензій, які, у свою чергу, можуть мати виключний або невиключний характер.

Правила щодо форми цивільно-правових договорів поширюються і на договори у сфері інтелектуальної власності. Проте з цього загального правила є винятки, передбачені законом. Усі договори, що укладаються у сфері інтелектуальної діяльності, мають укладатися у письмовій формі. Чинне цивільне законодавство України не передбачає обов'язкового нотаріального засвідчення зазначених договорів. Проте за бажанням сторони можуть свій договір засвідчити нотаріально. Отже, договір про нерозголошення має укладатися тільки в письмовій формі і за бажанням посвідчуватися нотаріально.

Умови дійсності договорів у сфері інтелектуальної діяльності - це ті ж самі умови дійсності, дотримання яких обов'язкове при укладенні будь-якого цивільно-правового договору. Передусім зміст, умови, форма, порядок укладення таких договорів мають відповідати вимогам ЦК України. Як і у будь-якому договорі, основним має бути законність змісту.

Зміст договору - це ті умови, на яких сторони погодилися укласти договір. Це в основному права й обов'язки сторін, визначені договором. За своїм юридичним значенням усі умови договору прийнято поділяти на істотні, звичайні та випадкові. До істотних належать такі умови, без яких договір не може набрати чинності. Безперечно, істотні умови договору визначаються за волевиявленням обох сторін. Без такого визначення об'єкта (предмета) договір не виникає. Очевидно, що до істотних умов договору у сфері інтелектуальної діяльності слід також віднести умову про обсяг використання об'єкта.

Звичайними умовами договору визнаються ті, що передбачені нормативними актами й автоматично набувають чинності при укладенні договору. Вони не потребують погодження сторін, але це не означає, що такі умови діють проти їх волі, вони також опираються на угоду сторін. Це означає, що сторони, укладаючи договір, погоджуються на такі визнані, усталені й звичайні для такого виду договору, умови. Передбачається, що сторони, які згодилися укласти такий договір, погоджуються його укласти на таких звичайних умовах.

Договір про нерозголошення комерційної таємниці як цивільноправова угода є досить нетрадиційним, по крайній мірі, ЦК не передбачає такого виду договорів (угод). У вітчизняній правовій науці такі конструкції майже не досліджувалися, а, отже, вони рідко використовувалися на практиці. Цього не скажеш про західну теорію і практику, яким дуже добре відомі договори про захист комерційної таємниці. Але можна сміливо сказати, що договори про нерозголошення мають право на існування, адже як передбачено ч. 1 ст. 6 ЦК, сторони мають право укласти договір, який не передбачений актами цивільного законодавства, але відповідає загальним засадам цивільного законодавства.

Типовий NDA в українських IT компаніях виглядає наступним чином:

***Зразок***

**ДОГОВІР**

**про конфіденційність і нерозголошення інформації NDA**

м. \_\_\_\_\_\_\_                                                              «\_\_\_»  \_\_\_\_\_\_\_\_2019 року

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , надалі іменується сторона «СТОРОНА, ЯКА РОЗКРИВАЄ»  в особі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, що діє на підставі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  з однієї сторони та \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  надалі іменується  «СТОРОНА, ЯКА ОДЕРЖУЄ» в особі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  які спільно іменуються  «Сторони», уклали договір про наступне:

**1.ПРЕДМЕТ ДОГОВОРУ**

1.1. Сторони підтверджують, що:

1.1.1. СТОРОНА, ЯКА РОЗКРИВАЄ, передала з метою належного виконання Договору №\_\_\_ від «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_ року, укладеного між \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ та \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (надалі іменується «Основний договір»), СТОРОНІ, ЯКА ОДЕРЖУЄ, інформацію, визначену Основним договором, а також наступну інформацію:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(надалі – Конфіденційна інформація).

Конфіденційною є також інформація про умови цього договору та Основного договору, в т.ч. відомості технічного, організаційного, комерційного, виробничого та іншого характеру.

Конфіденційною є також інформація, крім вказаної вище, про конфіденційність якої Сторона, яка розкриває прямо повідомила Сторону, яка одержує  в момент її передання.

1.1.2. СТОРОНА, ЯКА ОДЕРЖУЄ отримала названу інформацію виключно для виготовлення товару (надання послуг) за замовленням СТОРОНИ, ЯКА РОЗКРИВАЄ, та не має право використовувати її для будь-яких інших цілей.

1.1.3. Будь-яка інформація, передання якої мало місце на підставі Основного договору та визначена Сторонами у п. 1.1.1. цього Договору, вважається конфіденційною за цим Договором і щодо неї діє режим комерційної таємниці згідно чинного законодавства та цього договору.

1.1.4. Передання інформації від СТОРОНИ, ЯКА РОЗКРИВАЄ, до СТОРОНИ, ЯКА ОДЕРЖУЄ обумовлене взаємовигідним співробітництвом Сторін і прагненням Сторін інтенсифікувати та спільно скоординувати свої подальші ділові відносини.

**2. ОБОВ'ЯЗКИ СТОРІН**

2.1. Сторони підтверджують розуміння ними важливості договірного врегулювання відносин із забезпечення режиму комерційної таємниці та погоджуються взяти на себе наступні обов'язки:

2.1.1. З дня набрання чинності цим Договором СТОРОНА, ЯКА ОДЕРЖУЄ, зобов'язується:

2.1.1.1. не розголошувати конфіденційної інформації, отриманої нею від СТОРОНИ, ЯКА РОЗКРИВАЄ, будь-яким іншим третім особам, включаючи органи державної влади, підприємства, установи, організації усіх форм власності та підпорядкування, і не буде використовувати названу інформацію для своєї власної вигоди, за винятком використання такої інформації відповідно до цілей, визначених у пп. 1.1.2. цього Договору. Вказаний обов’язок діє також протягом п’яти років після закінчення цього договору.

2.1.1.2. дотримуватися такого ж ступеня секретності з метою уникнення розголошення або використання цієї інформації іншим особами, якого СТОРОНА, ЯКА ОДЕРЖУЄ, дотримувалася б в розумній мірі стосовно своєї власної конфіденційної інформації аналогічного ступеня важливості.

2.1.2. СТОРОНА, ЯКА ОДЕРЖУЄ, зобов’язується вжити всіх необхідних заходів для збереження конфіденційної інформації, в тому числі:

2.1.2.1. забезпечити доступ до конфіденційної інформації обмеженій кількості працівників, і тільки тим працівникам, які безпосередньо  використовують зазначену інформацію у зв’язку з виконанням службових обов’язків, попередньо отримавши від зазначених працівників письмові Зобов'язання про нерозголошення відомостей, що становлять конфіденційну інформацію (як під час виконання ними відповідних виробничих функцій, так і у випадку їх звільнення з роботи, або відсторонення від виконання замовлення СТОРОНИ, ЯКА РОЗКРИВАЄ) та письмово попередити про кримінальну, адміністративну чи цивільно-правову відповідальність за розголошення відомостей, що становлять комерційну таємницю та конфіденційну інформацію. При цьому відповідальність перед СТОРОНОЮ, ЯКА РОЗКРИВАЄ за порушення умов щодо конфіденційності такими працівниками буде нести СТОРОНА, ЯКА ОДЕРЖУЄ;

2.1.2.3. заборонити у відповідних договорах (контрактах) використання знань, отриманих в процесі роботи з конфіденційною інформацією, своїм працівникам протягом п’яти років після звільнення;

2.1.2.4. здійснювати реєстрацію доступу своїх працівників до конфіденційної інформації і надавати щомісяця до п’ятого числа інформацію про такий доступ, який повинен включаючи прізвище працівника, матеріали, з якими він ознайомлений, ґрунтовне підтвердження необхідності ознайомлення, дату і час їх отримання і повернення відповідних матеріалів;

2.1.2.5. не робити копій документів в більшій кількості, чим це необхідно для виконання працівниками  службових обов’язків,  забезпечити достовірний облік всіх копій і місць, де вони де вони зберігаються та знищити копії, якщо в цьому не буде необхідності;

2.1.2.6. забезпечити захищену обробку конфіденційної інформації на технічних засобах, не підключених до мережі Інтернет і доступ до яких дозволений тільки авторизованим користувачам;

2.1.2.7. забезпечити надійне зберігання інформації, яке не дозволить отримати доступ до неї неавторизованим особам, в тому числі поза робочим часом;

2.1.2.8. призначити осіб, відповідальних за розробку і практичне здійснення заходів по забезпеченню конфіденційності інформації.

2.1.2.9. За письмовим запитом СТОРОНИ, ЯКА РОЗКРИВАЄ, (який може бути зроблений в будь-який час) СТОРОНА, ЯКА ОДЕРЖУЄ, зобов’язана:

- у випадку, якщо носії конфіденційної інформації є власністю СТОРОНИ, ЯКА ОДЕРЖУЄ – знищити конфіденційну  інформацію з таких носіїв, або самі носії до ступеня неможливості відновлення;

- у випадку, якщо носії конфіденційної інформації є власністю СТОРОНИ, ЯКА РОЗКРИВАЄ – забезпечити повернення всіх таких носіїв. У кожному такому випадку СТОРОНА, ЯКА ОДЕРЖУЄ зобов’язана проінформувати СТОРОНУ, ЯКА РОЗКРИВАЄ, про виконання своїх обов’язків у письмовій формі.

Термін виконання СТОРОНОЮ, ЯКА ОДЕРЖУЄ обов’язків по цьому пункту складає 10 днів з моменту подання СТОРОНОЮ, ЯКА РОЗКРИВАЄ такого запиту.

2.1.2.10. не схиляти до розголошення зазначеної інформації будь-яких інших осіб, яким така інформація є відомою з тих чи інших причин.

2.1.3. У разі виникнення потреби в розкритті інформації третім особам, в т.ч. у разі отримання запиту (письмового, усного, по електронній пошті) на інформацію, яка становить комерційну таємницю та конфіденційну інформацію від контрагентів, клієнтів і будь-яких державних органів, СТОРОНА, ЯКА ОДЕРЖУЄ зобов'язана:

а) з'ясувати у контрагента, клієнта або представника державного органу необхідність отримання такої інформації (з чим пов'язаний такий запит; обсяг інформації, яка повинна міститися у відповіді);

б) негайно повідомити про такий запит СТОРОНУ, ЯКА РОЗКРИВАЄ;

в) отримати згоду СТОРОНИ, ЯКА РОЗКРИВАЄ на надання такої інформації;

г) погодити з СТОРОНОЮ, ЯКА РОЗКРИВАЄ, зміст і обсяг інформації, яка буде надаватися;

2.1.2.2. СТОРОНА, ЯКА ОДЕРЖУЄ, зобов’язана надати перелік працівників, які будуть використовувати зазначену інформацію для виробничих потреб.

ґ) у разі запиту правоохоронних органів направити копію зазначеного запиту СТОРОНІ, ЯКА РОЗКРИВАЄ, та отримати відповідні інструкції щодо конкретного запиту. Надати відповідь на запит лише в разі письмової згоди СТОРОНИ, ЯКА РОЗКРИВАЄ, за винятком випадків коли невиконання такого обов’язку, відповідно до чинного законодавства є підставою для притягнення СТОРОНИ, ЯКА ОДЕРЖУЄ, до адміністративної або кримінальної відповідальності.

2.1.4. СТОРОНА, ЯКА ОДЕРЖУЄ після закінчення дії цього Договору або у випадку реорганізації чи ліквідації зобов’язується негайно повернути всю отриману конфіденційну інформацію і копії, зроблені з неї.

2.1.5. СТОРОНА, ЯКА ОДЕРЖУЄ  зобов’язана при виявленні фактів, які свідчать про інформованість третіх осіб про конфіденційну інформацію, навіть в тому випадку, якщо така інформованість не є наслідком порушення умов цього Договору СТОРОНОЮ, ЯКА ОДЕРЖУЄ, повідомити про такі факти СТОРОНУ, ЯКА РОЗКРИВАЄ в найкоротші терміни, але не пізніше 5 (п’яти) днів з моменту виявлення.

2.1.6. СТОРОНА, ЯКА РОЗКРИВАЄ залишає за собою право проводити аналіз заходів по захисту конфіденційної інформації, вжитих СТРОНОЮ, ЯКА ОДЕРЖУЄ. При відмові надати інформацію про заходи щодо захисту конфіденційної інформації  чи виявленні недостатності вжитих заходів по захисту конфіденційної інформації СТОРОНА, ЯКА РОЗКРИВАЄ, має право відмовитись в наданні конфіденційної інформації чи розірвати договір достроково.

**3. ВІДПОВІДАЛЬНІСТЬ СТОРІН І ВИРІШЕННЯ СПОРІВ**

3.1. У випадку невиконання або неналежного виконання своїх зобов’язань за цим Договором СТОРОНА, ЯКА ОДЕРЖУЄ, зобов’язується протягом 3 (трьох) днів з дати отримання відповідного повідомлення від СТОРОНИ, ЯКА РОЗКРИВАЄ, сплатити штраф в розмірі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ за кожне таке порушення. При цьому сплата штрафу не звільняє винну сторону від належного виконання своїх зобов’язань згідно цього Договору і повного відшкодування завданих збитків (включаючи упущену вигоду).

3.2. Усі спори, що виникають з цього Договору або пов'язані із ним, вирішуються шляхом переговорів між Сторонами. Якщо відповідний спір неможливо вирішити шляхом переговорів, він вирішується в судовому порядку відповідно до чинного в Україні законодавства.

3.3. СТОРОНА, ЯКА ОДЕРЖУЄ, визнає, що несе повну відповідальність за будь-які дії чи бездіяльність своїх співробітників, посадових осіб, членів колегіальних органів управління (включаючи без обмеження осіб, які раніше виконували вказані функції чи займали посади), які прямо чи побічно призвели до розголошення чи розкриття конфіденційної інформації іншим особам.

**4. РОЗКРИТТЯ ІНФОРМАЦІЇ**

4.1. Якщо третя сторона пред'явить позов або вчинить іншу юридичну дію з вимогою розкрити будь-яку конфіденційну інформацію, СТОРОНА, ЯКА ОДЕРЖУЄ зобов'язана негайно повідомити про це СТОРОНУ, ЯКА РОЗКРИВАЄ і забезпечить їй в розумних межах таку допомогу, якої СТОРОНА, ЯКА РОЗКРИВАЄ, буде вимагати для запобігання розголошенню.

4.2. Жодна із сторін зобов’язується не розголошувати факт існування цього Договору та Основного договору без попередньої письмової згоди другої сторони.

4.3. Жодна із сторін не може передавати чи іншим шляхом уступати повністю чи частково, свої права и обов’язки по цьому договору без попередньої письмової згоди на це іншої сторони.

4.4. СТОРОНА, ЯКА ОДЕРЖУЄ, лише з письмової згоди СТОРОНИ, ЯКА РОЗКРИВАЄ може надати доступ до конфіденційної інформації, але не передачу такої інформації третій стороні, яка виступає в якості виконавця (субпідрядника), в цьому випадку СТОРОНА, ЯКА ОДЕРЖУЄ, несе повну відповідальність перед СТРОНОЮ, ЯКА РОЗКРИВАЄ за дотримання третьою стороною режиму конфіденційності стосовно розкритої інформації за правилами розділу  4.

4.5. Вся конфіденційна інформація за цим договором є виключною власністю СТОРОНИ, ЯКА РОЗКРИВАЄ.

**5. ДІЯ ДОГОВОРУ**

5.1. Цей Договір вважається укладеним і набирає чинності з моменту його підписання Сторонами та його скріплення печатками Сторін.

5.2. Строк цього Договору починає свій перебіг у момент, визначений у п. 5.1 цього Договору та закінчується через 5 років після закінчення строку дії Основного договору.

5.3. Закінчення строку цього Договору не звільняє Сторони від відповідальності за його порушення, яке мало місце під час дії цього Договору.

5.4. Якщо інше прямо не передбачено цим Договором або чинним в Україні законодавством, зміни у цей Договір можуть бути внесені тільки за домовленістю Сторін, яка оформлюється додатковою угодою до цього Договору.

5.5. Зміни у цей Договір набирають чинності з моменту належного оформлення Сторонами відповідної додаткової угоди до цього Договору, якщо інше не встановлено в самій додатковій угоді, цьому Договорі або у чинному в Україні законодавстві.

**6. ПРИКІНЦЕВІ ПОЛОЖЕННЯ**

6.1. Усі правовідносини, що виникають з цього Договору або пов'язані із ним, у тому числі пов'язані із дійсністю, укладенням, виконанням, зміною та припиненням цього Договору, тлумаченням його умов, визначенням наслідків недійсності або порушення Договору, регламентуються цим Договором та відповідними нормами чинного в Україні законодавства, а також застосованими до таких правовідносин звичаями ділового обороту на підставі принципів добросовісності, розумності та справедливості.

6.2. Після підписання цього Договору всі попередні переговори за ним, листування, попередні договори, протоколи про наміри та будь-які інші усні або письмові домовленості Сторін з питань, що так чи інакше стосуються цього Договору, втрачають юридичну силу, але можуть братися до уваги при тлумаченні умов цього Договору.

6.3. Сторони несуть повну відповідальність за правильність вказаних ними у цьому Договорі реквізитів та зобов'язуються своєчасно у письмовій формі повідомляти іншу Сторону про їх зміну, а у разі неповідомлення несуть ризик настання пов'язаних із ним несприятливих наслідків.

6.4. Додаткові угоди та додатки до цього Договору є його невід'ємними частинами і мають юридичну силу у разі, якщо вони викладені у письмовій формі, підписані Сторонами та скріплені їх печатками.

6.5. Всі виправлення за текстом цього Договору мають силу та можуть братися до уваги виключно за умови, що вони у кожному окремому випадку датовані, засвідчені підписами Сторін та скріплені їх печатками.

6.6. Всі повідомлення, враховуючи повідомлення про зміну фактичної і/чи юридичної адреси, повинні бути в трьохденний термін відправлені у письмовій формі рекомендованим листом з повідомленням  на адресу іншої СТОРОНИ.

6.7. Якщо одне або більше положень цього Договору будуть визнані судом, незаконними, недійсними або неможливими до застосування, Договір повинен вважатися дійсним, як ніби такі незаконні, недійсні або неможливі до застосування положення ніколи не існували. При цьому Сторони погоджуються зустрітися та, в дусі доброї волі, обговорити внесення необхідних змін до Договору, щоб відобразити первісні наміри Сторін цього Договору.

6.8. Цей Договір складений при повному розумінні Сторонами його умов та термінології українською мовою у двох автентичних примірниках, які мають однакову юридичну силу, по одному для кожної із Сторін.

### 

**7. МІСЦЕЗНАХОДЖЕННЯ ТА РЕКВІЗИТИ СТОРІН**

Правова система ЄС надає охорону інформації, що становить комерційну таємницю, у вигляді охорони “ноу-хау”, яка міститься в Європейській патентній конвенції. Під “ноу-хау” розуміється цілісна технічна інформація, що є секретною, зафіксованою в матеріальному об’єкті та може бути встановлена у будь-який можливий спосіб. “Секретний” означає “такий, що не є загально відомим або легко доступним”.

У зв’язку з тим, що в Україні IT компанії використовують приклад Договору про нерозголошення конфіденційної інформації практики США, яскравим прикладом різниці у договорах двух країн виявлено:

**Severability.** If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as to best to effect the intent of the parties.

Якщо суд визнає будь-яке положення цієї Угоди недійсним або не підлягає виконанню, решта цієї Угоди тлумачиться так, щоб найкращим чином здійснити наміри сторін.

**Waiver**. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

Невикористання будь-якого права, передбаченого цією Угодою, не може бути відмовою від попередніх або наступних прав.

**Notice of Immunity [OPTIONAL].** Employee is provided notice that an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual (i) files any document containing the trade secret under seal; and (ii) does not disclose the trade secret, except pursuant to court order.

Може включатися у Договір ДОДАТКОВО. Працівник отримує повідомлення про те, що фізична особа не несе кримінальної чи цивільної відповідальності за будь-яким федеральним чи державним законом про комерційну таємницю за розголошення комерційної таємниці, яка робиться в довіру до посадової особи федерального, штатного чи місцевого самоврядуванняпрямо чи опосередковано, або до адвоката; та виключно з метою повідомлення або розслідування підозр на порушення закону; або подається у скарзі чи іншому документі, поданому в судовому порядку або іншому провадженні, якщо така подача робиться під печаткою. Особа, яка подає позов про відплату роботодавцем за повідомлення про підозру про порушення закону, може розголосити комерційну таємницю адвокату фізичної особи та використовувати інформацію про комерційну таємницю в судовому процесі, якщо особа подає будь-який документ, що містить комерційну таємницю під печаткою; та не розголошує комерційну таємницю, за винятком наказу суду.

Тож загалом питання, чи варто укладати договір про неконкуренцію, не є однозначним не лише в Україні. Між іншим, попри світову практику та право більшості штатів США, у Каліфорнії (де розташована всесвітньо відома Кремнієва долина, де знаходяться більшість ІТ-компаній США) неконкуренція під забороною як прямо, так і через визначення неконкуренції через договір про нерозголошення. Як приклад наводять “експеримент”, який здійснив Марк Херд – керівник Hewlett-Packard (HP). Впродовж усієї роботи у Каліфорнії він підписав чимало NDA контрактів, при звільненні ще раз у договорі підтвердив свої зобов’язання не розголошувати конфіденційної інформації. А потім перейшов на роботу у відому компанію Oracle, що є прямим конкурентом HP. Розпочався судовий процес, і юристи HP намагалися довести, що під час роботи у конкурента він однозначно використає конфіденційні напрацювання, що Херд отримав за роки роботи виконавчим директором HP. Тим не менше, вони уклали угоду про примирення, умови якої не розголошуються, але як зазначають експерти, все одно Марк Херд вийшов із цієї ситуації переможцем. Отже, навіть у США можна не дотримуватися положення про неконкуренцію (хоча лише у штаті Каліфорнія).

2.6. Проблема збереження конфіденційності та надійності захисту даних в Україні та зарубіжних країнах

Серед головних причин недостатнього рівня ефективності охорони інтелектуальної власності українських фізичних і юридичних осіб фахівці найчастіше називають такі:

* відсутність у держави засобів на патентування і здійснення реєстраційних процедур за кордоном;
* низький рівень правової культури в країні;
* відсутність належних знань та інформації про порядок захисту інтелектуальної власності за межами України;
* законодавчу неврегульованість в Україні питань трансферу технологій, у т.ч. у випадках виїзду українських фахівців на роботу за кордон.

У сфері законодавчого регулювання системи охорони інтелектуальної власності слід вирішити проблемні питання щодо володіння і управління правами на об’єкти інтелектуальної власності, які створюються за рахунок державного бюджету; колективного управління авторськими і суміжними правами; передачі прав на об‘єкти інтелектуальної власності на комерційній основі; забезпечення розвитку франчайзингу, трансферу технологій; захисту комерційної інформації підприємств, а також ноу-хау; обліку об‘єктів інтелектуальної власності та оцінки вартості нематеріальних активів; охорони раціоналізаторських пропозицій, порід тварин та сортів рослин, а також охорони фольклору, народних художніх промислів і традиційних знань.

Слід акцентувати увагу на впровадженні сучасних технологій управління процесами охорони інтелектуальної власності. Цьому сприяло б створення централізованого комп‘ютерного банку даних щодо фірмових найменувань, зареєстрованих на території України; впровадження новітніх інформаційних технологій, зокрема, щодо патентної бібліотеки загального користування. Необхідно також розробити заходи з узгодження національної статистики щодо інтелектуальної власності із міжнародними стандартами в цій сфері. Разом з цим, зарубіжний досвід свідчить, що створити ефективну систему охорони інтелектуальної власності, спираючись виключно на державні структури, практично неможливо. Через це власникам інтелектуального продукту (юридичним і фізичним особам), а також творчим союзам України важливо активізувати процес створення недержавних організацій з питань охорони інтелектуальної власності, а також вивчити питання входження у відповідні міжнародні недержавні організації.

Одна з основних проблем полягає в тому, що згідно зі ст. 9 КЗпП, умови договорів про працю, які погіршують становище працівників порівняно з законодавством України про працю, є недійсними. З одного боку, Конституція України прямо передбачає право на працю, що включає можливість заробляти собі на життя працею, яку людина вільно обирає і на яку вільно погоджується, тому застереження про неконкуренцію справді можуть бути визнані недійсними в Україні. З іншого боку, дотримуючись норм ст. 9 Кодексу законів про працю України, необхідно аналізувати кожне застереження про неконкуренцію індивідуально на предмет того, чи справді таке застереження погіршує становище працівників порівняно з законодавством України про працю.

Цивільне законодавство України теж не передбачає жодних умов про врегулювання неконкуренції між двома суб’єктами господарювання договірним шляхом.

В англійському праві, а також у законодавстві ряду країн ЄС, положення про неконкуренцію вважаються легітимними і такими, що можуть бути виконані в примусовому порядку при дотриманні ряду вимог. Перш за все, потрібно довести, що положення про неконкуренцію спрямоване безпосередньо на захист законних інтересів, а не тільки на обмеження або усунення конкуренції з боку третіх осіб. Тут має значення оцінка того, наскільки конкуренція колишнього працівника/підрядника, може мати істотний вплив на діяльність Замовника або ІТ компанії.

При цьому, беремо за приклад поширену модель співпраці іноземних замовників або аутсорсингових IT компаній та українських розробників, де замовник знаходиться за кордоном, а розробник знаходиться в Україні. Згідно норм Закону України «Про міжнародне приватне право», зокрема статті 5 «Автономія волі», сторони договору можуть вибрати право держави, яке має бути застосоване. Також, Закон України «Про Міжнародне приватне право» передбачає такий правовий інститут, як застосування конкретного права держави не до цілого договору, а до окремих його положень (це не стосується трудових договорів).

Ще одна регулятивна особливість, яка передбачена Законом України «Про міжнародне приватне право» – це можливість обрання підсудності, тобто можливість обрати який саме суд і де буде розглядати такий спір. Хоча, тут існують певні нюанси.

Наприклад, іноземна компанія уклала з українським розробником договір про розробку ПЗ, в якому зазначено, що спір підсудний українському суду, але право, яке буде застосовуватися – право іноземної держави. В такому випадку, відповідно до статті 8 Закону України «Про міжнародне приватне право» при застосуванні права іноземної держави суд чи інший орган встановлює зміст його норм згідно з їх офіційним тлумаченням, практикою застосування і доктриною у відповідній іноземній державі. Тому, суд має звернутися або до уповноваженого органу іноземної держави або України для офіційного тлумачення норм права іноземної країни. На практиці такий процес може затягнутися на декілька місяців, що істотно знижує його ефективність для заявника.

Інший варіант – якщо судовий спір виник між тими самим сторонами, але підсудність договором визначена в іноземній державі, а його виконання буде відбуватись на території України. Процес виконання рішень іноземних судів передбачений цивільним процесуальним та господарським процесуальним законодавством. Зокрема, згідно статті 462 ЦПК України, рішення іноземного суду (суду іноземної держави, інших компетентних органів іноземних держав, до компетенції яких належить розгляд цивільних справ) визнаються та виконуються в Україні, якщо їх визнання та виконання передбачено міжнародним договором, згода на обов’язковість якого надана Верховною Радою України, або за принципом взаємності.

Суд України може відмовити за наступних обставин: 1) якщо рішення іноземного суду за законодавством держави, на території якої воно постановлено, не набрало законної сили; 2) якщо сторона, стосовно якої постановлено рішення іноземного суду, була позбавлена можливості взяти участь у судовому процесі через те, що їй не було належним чином і вчасно повідомлено про розгляд справи; 3) якщо рішення ухвалене у справі, розгляд якої належить виключно до компетенції суду або іншого уповноваженого відповідно до закону органу України; 4) якщо раніше ухвалене рішення суду України у спорі між тими самими сторонами, з того самого предмета і на тих самих підставах, що набрало законної сили, або якщо у провадженні суду України є справа у спорі між тими самими сторонами, з того самого предмета і на тих самих підставах, яка порушена до часу відкриття провадження у справі в іноземному суді.

Не секрет, що в Україні працівники абсолютно несерйозно ставляться до підписання NDA (Non-disclosure agreement). Для сторін договір про нерозголошення, в першу чергу, є попередженням, а не дієвим механізмом захисту. Саме тому більшість договорів такого типу люди беруть з інтернету і, в кращому випадку, трохи змінюють формулювання або доповнюють за змістом - на цьому вся юридична частина закінчується.

Для того, щоб краще з цим розібратися, пропонуємо розглянути практичну ситуацію. Маленька IT-компанія бере на роботу нового співробітника, з яким звичайно ж підписують NDA - це обов'язкова умова прийому на роботу, особливо в IT-компаніях. І все начебто добре, але раптом керівництво компанії якимось чином (не заглиблюючись в деталі) дізнається, що їх новий співробітник передає інформацію їх головним конкурентам - інший маленької IT-компанії. Співробітника відразу ж звільняють. Навіть незважаючи на це керівництву здається, що це занадто легке для нього покарання – вирішують засудити людину, адже підписано NDA. Компанія наймає хороших юристів, витрачає на них купу грошей, але результату немає - суд програно.

Основне питання полягає в наступному: чому виходить так, що більшістю підписаних NDA можна просто скласти на полицю? Нижче перераховані причини, які можуть спростити процес складання NDA і значно вплинути на його «життєздатність»:

1. Узагальненість. У договорах про нерозголошення, в основному, прописують загальні положення про конфіденційну інформацію або цитують розмиті норми із законів. Це спочатку є неправильним підходом. Замість того, щоб наповнювати документ безглуздими положеннями, варто досконально описати, що є конфіденційною інформацією конкретно у випадку окремої компанії, і що є порушенням порядку поводження з конфіденційною інформацією.
2. Відірваність від реальності. Відсутність підв'язки NDA до реальних правовідносин означає, що документ лише формальність, яка немає юридичної сили. Щоб уникнути цього, договір варто підписувати або на період роботи над проектом (якщо це проектна робота), вказуючи при цьому назву проекту і приблизні терміни його існування, або як додаткову угоду до основного договору (якщо це трудові відносини), посилаючись при цьому на основний договір. У плані трудових відносин трохи простіше. Усередині компанії завжди можна розробити локальні акти, які регулюють питання конфіденційності.
3. Термін. Для NDA немає специфічних вимог до терміну дії договору. У цьому контексті все залежить від типу інформації, якою ділиться із співробітником компанія, її цінность і галузь діяльності. Найпоширеніші терміни - це 1, 3 або 5 років. Існує альтернативний варіант - складання безстрокового договору, який залишається в силі до тих пір, поки одна зі сторін не захоче його розірвати. В даному контексті дуже цікавим видається кейс Orthofix, Inc. vs. Hunter. Проаналізувавши обставини справи, суд першої інстанції штату Іллінойс виявив порушення договору, але в зв'язку з тим, що не було територіальних і часових обмежень в договорі, він був визнаний недійсним. Для того, щоб було більше шансів перед опонентом в суді, NDA повинен включати чіткі терміни, мало того - ці терміни повинні бути виправдані. Це стосується не тільки терміну дії самого договору, це також поширюється і на обов'язок зберігати конфіденційність після його розірвання.
4. Застереження. Кожен договір про нерозголошення повинен включати в себе застереження про те, що не є розголошенням. В українському законодавстві в загальних рисах зазначено, що не відноситься до конфіденційної інформації, але недостатньо просто взяти і відобразити це в договорі. Кожен раз, складаючи NDA, варто враховувати специфіку правовідносин, в яких він підписується. Крім ситуацій, прямо прописаних в національному законодавстві, варто передбачити ситуації в яких було б несправедливо або занадто обтяжливо зберігати конфіденційність інформації. Це можуть бути винятки, що стосуються відносин з правоохоронними органами або застереження про інформацію з публічного доступу.
5. Способи передачі інформації. Іноді просто фізично неможливо вичерпно прописати конфіденційну інформацію. У таких випадках конфіденційність інформації можливо зв'язати зі способами її передачі. Тобто, в договорі може бути прямо вказано, що на час співпраці сторони ведуть всю ділову переписку через певні поштові скриньки, створені для цієї мети. Вся інформація, відправлена ​​з такою пошти, є конфіденційною. Як варіант, сторона може надати інший доступ до свого хмарного сховища. Це значно спростить контроль за інформацією, адже до хмари зможе отримати доступ тільки авторизований користувач, а всі його дії будуть відображатися і фіксуватися в журналі, тобто істрії праці з даною інформацією. На практиці часто зустрічаються формулювання такого типу: «вся інформація, яка передана способами, зазначеними в пункті 2.28 договору, є конфіденційною», або такі: «в пункті 2.28 договору зазначено вичерпний перелік способів передачі конфіденційної інформації, його порушення - є порушенням договору». Йдеться навіть не про ефективність цих формулювань, а скоріше про те, що необхідно вказувати і деталізувати стандартні способи передачі (месенджери, пошту, телефон тощо).
6. Режим інформації. Залежно від важливості підписаного договору і серйозності намірів сторін, можливо розглянути варіант із встановленням режимів інформації та / або призначення відповідальних осіб. У цьому плані не потрібно вигадувати велосипед, вже давно існує посада «information officer», в обов'язки якого входить розробка політик інформаційної безпеки та моніторинг за інформаційної гігієною в компанії. У книзі «Information Security Management: Concepts and Practice» приведена досить загальна класифікація інформації. Якщо її доопрацювати/змінити, можна впевнено застосувати до приватноправових відносин. Умовно, інформацію можна розділити на три класи: для внутрішнього використання; конфіденційна; строго конфіденційна. І вже виходячи з цієї класифікації варто опрацьовувати способи зберігання і передачі, умови отримання доступу до інформації, а також відповідальність за її розголошення (неправомірне поводження).
7. Відповідальність. В якійсь мірі відповідальність - це одна з найважливіших частин договору про нерозголошення. Для того, щоб зробити цю частину ще й ефективною, необхідно пов'язати відповідальність за розголошення з усіма попередніми умовами, а точніше їх невиконанням. У цьому контексті, важливо розмежовувати відповідальність за невиконання умов, які призвели до розголошення інформації, і які не привели до наслідків у вигляді розголошення, але мали місце (наприклад, не передбачений спосіб передачі). Так, якщо були передбачені конкретні заходи зберігання, а сторона їх порушила і допустила витік інформації – штраф відповідному розмірі, а якщо умови були порушені, але розголошення не було – штраф у відповідному розмірі.

Підводячи підсумок, слід сказати, що в плані захисту конфіденційної інформації національне законодавство значно відстає від європейського і, тим більше, від законодавства США. Трапляються ситуації, в яких договір складений за всіма юридичними канонами України, але в зв'язку з відсутністю дієвого механізму підтвердження самого факту розголошення інформації, в судовому процесі не вдається відстояти свою позицію.

Необхідно враховувати вже сформовану світову практику, особливо - судову. Аналізуючи її, не складно зрозуміти, що краще застосовувати іноземне законодавство до договорів про нерозголошення. Якщо фінансове становище компанії дозволяє реалізувати це – можна розглянути такий варіант. Але в такому випадку необхідно розуміти, що судовий процес буде проходити відповідно до чинного законодавства. Якщо було визначено, що договір регулюється законодавством штату Делавер - ви повинні бути готові до додаткових витрат, які будуть потрібні для судового розгляду в США. Якщо договір підписано з іноземними співробітниками, це того варте.

ВИСНОВКИ

В процесі комплексного аналізу питання правового регулювання обігу конфіденційної інформації в IT сфері, розгляду правової сутності поняття комерційної таємниці, дослідження Договору про конфіденційність (NDA) в Україні та зарубіжних країнах, сформульовано ряд висновків, пропозицій і рекомендацій, спрямованих на удосконалення чинного галузевого законодавства в досліджуваній сфері.

1. Для забезпечення достатнього рівня інформаційної безпеки компанії потрібно розробляти Політику інформаційної безпеки з урахуванням того, що вона є складовою системи безпеки підприємства, і пам’ятати, що вона повинна бути орієнтованою на кожного працівника, а також не навантажувати головний документ інформацією, направленою на окремих працівників. Для цього потрібно розробляти документи нижчого рівня.
2. Часто ІТ компанії пропонують підписати договір про нерозголошення (NDA) своїм працівникам. Цю практику поступово використовують і в інших сферах бізнесу, де використовується інтелектуальна праця. Проте, підписати договір – ще не означає, що він має юридичну силу. Здебільшого, ці договори характерні для США, їх перекладають на українську мову, вносять певні правки і все. Проте, не враховують найважливішого – нормативного регулювання України. Підписавши цей договір із працівником, навіть якщо він розголосить комерційну таємницю Вашого бізнесу, у Вас не буде правових засобів впливу та Ви не зможете виграти судову справу проти такого працівника. Відповідно, не зможете стягнути компенсації за розголошення. Для того, щоб підписати договір про нерозголошення потрібна спеціальна правова конструкція, про яку буде йтись далі.
3. Охорона комерційної таємниці від незаконного використання здійснюється за допомогою різних правових заходів. Деякі держави прийняли спеціальні акти про охорону комерційної таємниці, інші забезпечують її охорону на підставі положень законів про недобросовісну конкуренцію. Окремі держави забезпечуюь охорону таємниці в межах загальної системи про цивільно-правовий делікт. Досить часто права особи на комерційну тамницю охороняються засобами кримінального права, проте така охорона передбачає доведення проінформованості правопорушника про таємний характер інформації та наявність його умислу щодо вчинення дій з розголошення комерційної таємниці. Тому, як правило, більш ефективним є цивільно-правовий захист прав особи на комерційну таємницю, що може забезпечуватися як загальними нормами цивільного законодавства, так і нормативними положеннями щодо боротьби з недобросовісною конкуренцією.
4. Договір про нерозголошення комерційної таємниці направлений на запобігання неправомірному використанню чи розголошенню комерційної таємниці підприємства. Зневажливе ставлення до питання захисту комерційної таємниці може негативно вплинути на економічний розвиток суб'єкта господарювання. З огляду на це, слід привітати пропозицію Комітету Верховної Ради України з питань науки і освіти про створення робочої групи з розробки законопроекту «Про комерційну таємницю», до якої має бути залучено фахівців Державного департаменту інтелектуальної власності, Антимонопольного комітету України, Служби безпеки України та представників інших центральних органів виконавчої влади. Адже участь широкого загалу фахівців, які опікуються проблемами захисту прав суб’єктів інформаційних відносин, є необхідною передумовою створення якісної законодавчої бази в цій сфері.
5. Нині в чинному законодавстві України лише формується система законодавчої охорони суб’єктивних прав на комерційну таємницю, а особливості її правового режиму є предметом окремих наукових досліджень у вітчизняній цивілістиці. Норми, що спрямовані на забезпечення правової охорони комерційної таємниці, закріплені переважно в положеннях глави 46 Цивільного кодексу України, а також у законодавстві про інформацію. Охорона прав суб’єкта на комерційну таємницю здійснюється також засобами адміністративного та кримінального права (Законом України «Про захист від недобросовісної конкуренції») і статтями 231, 232 Кримінального кодексу України.
6. Договір про конфіденційність - відомий також як Договір про нерозголошення конфіденційної інформації або договір про секретність - це договір, який укладається між двома сторонами, в якому вони погоджуються на захист конфіденційної інформації, що розкривається під час здійснення підприємницької діяльності. У сфері IT конфіденційною інформацією можуть вважатися спільні бізнес-ідеї, коди, бази даних, документація, засоби і методи розробки, методи обробки інформації та багато іншого.
7. На ефективність захисту комерційної таємниці істотний вплив має документальне оформлення. Факт укладення договору про нерозголошення не є достатнім для захисту комерційної таємниці. Необхідно врегулювати пов’язані з захистом такої інформації питання на рівні Статуту, локальних актах (положенні про комерційну інформацію), встановити спеціальний режим для роботи з вказаною інформацію, здійснювати облік (реєстрацію) доступу до вказаної інформації, позначати носії конфіденційної інформації, тощо. Умови про використання та захист комерційної таємниці бажано регулювати в договірному порядку не лише з працівниками, а й учасниками та контрагентами.
8. Договір про конфіденційність може бути охарактеризовний як різновид лінцензійного договору про надання прав на інформацію, згідно з яким одна сторона (ліцензіат, конфіденціал) повинна дотримуватися обумовленного договором режиму інформації, набутої від іншої сторони (ліцензіара, конфідента), і зобов’язується не надавати права на інформацію іншим особам. Таке розуміння договору про конфіденційність дає змогу поширити на правове регулювання його умов положення законодавства про форму й істотні умови ліцензвйного договору з урахуванням специфіки притаманних такому виду договірних зобов’язань.
9. Загалом питання, чи варто укладати договір про неконкуренцію, не є однозначним не лише в Україні. Між іншим, попри світову практику та право більшості штатів США, у Каліфорнії (де розташована всесвітньо відома Кремнієва долина, де знаходяться більшість ІТ-компаній США) неконкуренція під забороною як прямо, так і через визначення неконкуренції через договір про нерозголошення.
10. Угоди про неконкуренцію в межах цивільно-правових та господарсько-правових відносин також не мають належного законодавчого регулювання. Незважаючи на принцип свободи договору, конституційне право кожної особи на працю та підприємницьку діяльність вважається таким, що не може бути обмежено інакше як згідно з законом чи за рішенням суду. Відповідно, відсутність законодавчої можливості обмежити неконкуренцію, зокрема, у сферах розроблення програмного забезпечення та інших інформаційних послуг, не дає змоги встановлювати такі обмеження у договорах за згодою сторін.
11. Судовий захист права інтелектуальної власності також зустрічає перешкоди і у недосконалості судової системи України (тобто у деяких прогалинах та колізіях в законодавстві, що регулює судову систему). Наприклад проблеми підсудності справ, що випливають із захисту права інтелектуальної власності: справи. Те, що стосуються кваліфікації об’єкта промислової власності – прерогатива адміністративного суду, а те, що стосуються порушення прав, підтверджених охоронними документами, – прерогатива господарського суду. Тобто, два дуже близьких по суті спори мають розглядатися різними судовими органами. Таких випадків неточності українського законодавства ще є багато, що значним чином впливає на якість забезпечення захисту права інтелектуальної власності в цілому
12. Для Євросоюзу і для України пріоритетною є розробка нормативноправової бази, яка сприятиме більш ефективному застосуванню відповідних правових положень у разі порушення прав на комерційну таємницю, формуванню цивілізованого конкурентного середовища серед виробників товарів і послуг на європейській арені, що в цілому забезпечить зростання рівня безпеки та надійності європейської економіки.
13. В Україні використання на практиці норм про неконкуренцію під питанням. Тим не менше, все ж таки варто для роботодавців (в ІТ-сфері зазвичай “наймають” працівників, укладаючи з ними цивільно-правові договори як з фізичними особами-підприємцями, а відтак, можуть вносити це застереження) та замовників програмних послуг включати положення про неконкуренцію у контракти, враховуючи, що, по-перше, це має превентивно-психологічний вплив, по-друге, практика застережень про неконкуренцію є звичайною та нормальною у цій сфері відносин у розвинених країнах світу, а по-третє, євроінтеграційні процеси свідчать про акцепт значної частини правових норм розвинутих правових систем. Також в Україні склалося доволі потужне лобі ІТ-галузі, що дозволяє припускати можливу імплементацію законодавства про неконкуренцію в Україні.

ПЕРЕЛІК використаних джерел

1. [Bel G. Raggad](https://www.google.com/search?rlz=1C1CHBD_ruUA843UA843&sxsrf=ACYBGNTBHi5ZfkxBShhA231cWuoR2I_ZdQ:1577413678389&q=information+security+management:+concepts+and+practice+bel+g.+raggad&stick=H4sIAAAAAAAAACXKMQ7CMAwAwAmJBQZmBouRgSiMmfkHcl03hBI7uK4K3-GlIDGedOvtbhNyiLFb2tPv_fnw5xDt1XKMx_1IKXSqY1isuLNcF7Ux4ew3tc_qUmRQq-hFBSam-ZfeUFEwc2XxBKRC3HwClB6aIXkhho4fkE9gmDP2XzFzrsGFAAAA&sa=X&ved=2ahUKEwi0gtvv49TmAhXLaVAKHXrvDCoQmxMoATARegQIEBAM) Information Security Management: Concepts and Practice. CRC Press, 2010. 871 р.
2. GDPR. Official Journal of the European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
3. Lloyd I. J. Information Technology Law. Oxford: Oxford University Press, 2008. 584 p.
4. Seager v. Copydex Limited. Reports of Patent, Design and Trade Mark Cases. Volume 84. Issue 14. 1967. P. 349–374. URL: <https://academic.oup.com/rpc/article/84/14/349/1639209>.
5. Talimonchik P. V. Legal Aspects of International Security. Ethics, Laws, and Policies for Privacy, Security, and Liability. 2018. URL: <https://www.intechopen.com/online-first/legal-aspects-of-international-information-security>.
6. Trade-Related Aspects of Intellectual Property Rights (TRIPS). URL: <http://www.wto.org/english/docs_e/legal_e/legal_e.htm>.
7. Unіfоrm Tradе Sесrеts Aсt. URL: httр://dеlсоdе.dеlawarе.gоv/tіtlе6/с020/.
8. Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны. Київ : Видавничий дім «Ін Юре», 2000. 398 с.
9. Андрощук Г. О. Захист комерційної таємниці в США: протидія економічному шпигунству. Наука та інновації. 2013. №1. С. 80-95. URL: <http://intellect21.cdu.edu.ua/wp-content/uploads/2015/10/Combating-Economic-Espionage-UKR-1.pdf>.
10. Бачинський Т. В. Положення про не конкуренцію у ІТ-сфері та чинність цих положень загалом за законодавством України. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки : збірник наукових праць.* 2015. № 824. С. 169–173. URL: <http://www.pravoznavec.com.ua/period/article/72328/%D2>.
11. Бурило Ю. П. Організаційно-правові питання державного управління в інформаційній сфері : дис. …канд. юр. наук : 12.00.07 / Киїівський національний економічний університет Вадима Гетьмана. Київ, 2008. 216 с.
12. Виноградова Г. В. Інформаційне право України: навч. посіб. Київ : МАУП, 2006. 144 с.
13. Гелич Ю. О. Види інформації за законодавством України. *Правничий вісник Університету «КРОК»*. Київ, 2011. №10. С. 84-88.
14. Голод К. Інформаційна безпека США: сучасний стан та уроки для України. *Геополітика України: історія і сучасність.* № 2 (19). 2017. С. 91‑107. URL: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/Інформаційна%20безпека%20США.pdf>
15. Гороховська О. В. Семенюк І. С. Захист комерційної таємниці в міжнародному праві та законодавстві зарубіжних країн. *Держава та регіони. Серія: Право.* 2016. №1. С. 86-91. URL: <http://nbuv.gov.ua/UJRN/drp_2016_1_18>.
16. Господарський кодекс України від 16.01.2003 № 436-IV. *Відомості Верховної ради України.* URL: <http://zakon2.rada.gov.ua/laws/436-15>.
17. Гриджук Г. С. Систематизація методів інформаційної безпеки підпримства. URL: <http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf>.
18. Громов Г. NDA-эксперимент, который поставил Mark Hurd. URL: http://www.netvalley.com/silicon\_valley/ Hurd\_NDA\_HP\_ru.html
19. Гузь Д. Сильное заявление: Как (не)работает NDA в Украине. URL: <https://ain.ua/2017/05/25/kak-rabotaet-nda>.
20. Демкова М. Прозорість влади – умова належного урядування (аналіз та рекомендації). Київ, 2008. 50 с. URL: [https://www.pravo.org.ua/img/books/files/prozorist‑vlady‑demkova‑2008.pdf](https://www.pravo.org.ua/img/books/files/prozoristvladydemkova2008.pdf).
21. Дзьобань О. П., Мануйлов Є. М. Інформаційна безпека в контексті інформаційної культури. *Інформація і право.* 2017. №1. С. 74-81. URL: [http://nbuv.gov.ua/UJRN/Infpr\_2017\_1\_10](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Infpr_2017_1_10).
22. Дідук А. Г. Аналіз закордонного законодавства щодо конфіденційної інформації, комерційної таємниці. *Вісник Національного університету внутрішніх справ.* 2002. № 20. С. 320-325.
23. Дідук А. Г. Поняття «інформації» у цивільному праві. *Проблеми правознавства та правоохоронної діяльності: збірник наукових праць.* 2003. № 2. С. 174-181.
24. Дідук А. Г. Правовий режим конфіденційної інформації: цивільно-правовий аспект : дис. … канд. юр. наук: 12.00.03 / Харківський національний університет внутрішніх справ. Харків, 2008. 232 с.
25. Договір про нерозголошення конфіденційної інформації NDA. URL: <https://vreshetov.com/ua/obrazcy-dokymentov/drugie-dogovora/165-dogovor-o-konfidencialnosti>.
26. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2012 рік. Київ. 2012. URL: <https://old.e.gov.ua/sites/default/files/skachannye_fayly.pdf>.
27. Єдиний державний реєстр судових рішень. Справа № 2-0117-1531/11. URL: http://www.reyestr.court.gov.ua/Review/ 16982351.
28. Зусев Г. Ю. Інформаційні основи трансформації теперішньої економіки. *Економіка і право*. 2002. № 1. С. 28-33.
29. Іващенко В. А. Закономірності та тенденції розвитку законодавства у сфері інтелектуальної власності в Україні : дис. … д-ра юр. наук. : 12.00.03. Черкаси, 2018. 477 с.
30. Івченко Т. В. Цивільно-правова охорона комерційної таємниці як об’єкта права інтелектуальної власності в Україні. *Держава і право: юридичні і політичні науки : зб. наук. праць*. 2008. № 42. С. 401-408.
31. Ільницька У. Інформаційна безпека України: сучасний виклик, загрози та механізм протидії негативним інформаційно-психологічним впливам. *Політичні науки.* Львів, 2016. №1. С. 27-32. URL: [http://science.lpnu.ua/sites/default/files/journal‑paper/2017/jun/4352/ilnicka0.pdf](http://science.lpnu.ua/sites/default/files/journalpaper/2017/jun/4352/ilnicka0.pdf).
32. Капіца Ю. Захист комерційної таємниці в європейських країнах та Україні. *Підприємництво, господарство і право.* 2006. №1. С. 16-21.
33. Капіца Ю. М. Право інтелектуальної власності ЄС та законодавство України. Київ : Видавничий Дім «Слово», 2006. 360 с.
34. Кодекс законів про працю України від 10.12.1971 №322-VIII. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/322-08>.
35. Кодекс України про адміністративні правопорушення від 07.12.1984 №8073-X. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/80732-10>.
36. Колесніков Б. П. Стан та перспективи розвитку інформаційного суспільства в Україні. *Державне управління та місцеве самоврядування.* 2012. №3. С. 37-45. URL: <http://www.dridu.dp.ua/vidavnictvo/2012/2012_03(14)/12kbpisu.pdf>.
37. Колобов Л. Порівняльний аналіз складників комерційної таємниці та її захисту у вітчизняному законодавстві та законодавстві країн Євросоюзу. *Підприємництво, господарство і право*. 2016. №9. С. 9-13. URL: <http://pgp-journal.kiev.ua/archive/2016/09/3.pdf>
38. Конституція України від 28.06.1996. *Відомості Верховної Ради України.* URL: [https://zakon.rada.gov.ua/rada/show/254%D0%BA/96‑%D0%B2%D1%80](https://zakon.rada.gov.ua/rada/show/254%D0%BA/96%D0%B2%D1%80)
39. Копилов В. А. Інформаційне право : навч. посібник. Москва : Юристь, 2002. 282 с.
40. Костецька Т. А. Особливості формування національних інформаційних відносин та перспективи розвитку інформаційного законодавства. Правова держава: Щорічник наук. праць. 2001. № 12. С. 209-220.
41. Кримінальний Кодекс України від 05.04.2001. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/2341-14>.
42. Кротюк В. Іоффе А. Правові аспекти банківської таємниці. *Право України.* 1998. № 12. С. 62-66.
43. Кукшинова О. О. Правове регулювання доступу до відкритої інформації : автореф. дис. … канд. юрид. наук : 12.00.07. Київ, 2012. 20 с.
44. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес.* 2015. №5. С.87–92. URL: [http://nbuv.gov.ua/UJRN/ecmebi\_2015\_3\_18](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=ecmebi_2015_3_18).
45. Литвинюк А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування. URL: <http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf>.
46. Ліпкан В. А. Залізняк В. А. Систематизація інформаційного законодавства України : монографія / за заг. наук. ред. В. А. Ліпкан. Київ : ФОП О. С. Ліпкан, 2012. 304 с.
47. Логунов, А. Б. Региональная и национальная безопасность: Учебное пособие. Москва : НИЦ ИНФРА-М, 2014. 457 с. URL: <https://znanium.com/catalog/product/406872>.
48. Лонг Д. Патриція Р. Жаров В. О. Шевелева Т. М., Василенко І. Е., Дроб’язко В. С. Захист прав інтелектуальної власності: практ. посіб. Київ, 2015. 465 с.
49. Лопатин В. Н. Правовая охрана и защита служебной тайны. *Государство и право*. 2000. № 6. С. 85-91.
50. Макода В. Є. Правова охорона промислових зразків в Україні. Київ : Юрінком Інтер, 2014. 226 с.
51. Мандрик А. Договори про уникнення розголошення та неконкуренцію: аналіз зарубіжної практики та дійсність за чинним законодавством України. *Історико-правовий часопис.* 2019. №1. С. 127-131. URL: http://nbuv.gov.ua/UJRN/ipch\_2019\_1\_26.
52. Марущак А. І. Інформаційне право: доступ до інформації: навчальний посібник. Київ : КНТ, 2007. 532 с.
53. Матеріали судової практики ЄС у сфері захисту інтелектуальної власності можна знайти на офіційному сайті ЕС EUR-Lex у розділі Case-law. URL: <http://www.eur-lex.europa.eu/JURISIndex.do?ihmlang=en>>.
54. Мешко Н. П., Єфремова М. О. Розвиток IT-аутсорсингу в Україні. *Вісник Дніпропетровського університету.* 2015. № 5. С. 79–85. URL: http://irbis‑nbuv.gov.ua/cgi‑bin/irbis\_nbuv/cgiirbis\_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE\_FILE\_DOWNLOAD=1&Image\_file\_name=PDF/vdumi\_2015\_23\_5\_12.pdf.
55. Нестеренко О. Інформаційний омбудсман в механізмі забезпечення прав людини і основоположних свобод. *Харківська правозахисна група*. 2008. URL: <http://uapp.org/pub_analitics/5111.html>.
56. Нікітіна О. Комерційна таємниця. Ступінь захисту. *Юрист Консультує: інформаційно-довідкова газета.* 2005. №2. URL: <http://www.ts.lica.com.ua/b_text.php?type=3&id=233220&base=1>.
57. Новаківський І. І. Формування ефективних інноваційних адаптивних структур структур управління в умовах інформаційного суспільства. *Тези доповідей V Міжнародної науково-практичної конференції. Управління інноваційним процесом: налагодження взаємодії між учасниками.* Львів, 2014. С. 119-121.
58. Особливості діяльності розвідувальних служб країн Європейського Союзу та США: інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. URL: <http://euinfocenter.rada.gov.ua/uploads/documents/28833.pdf>.
59. Офіційний сайт Служби інформаційної безпеки Чехії: діяльність уряду Чеської Республіки в напрямку інтеграції до НАТО. URL: <http://osvita.ua/vnz/reports/world_history/4787/>.
60. Панаско О. М. Комплексний аспект інформаційної безпеки. *Збірник тез доповідей ІІІ Міжнародної науково-практичної конференції.* Кропивницький : ЦНТУ, 2018. С. 114-116.
61. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал.* 2009. №5. С. 122-134.
62. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства.  *Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації : міжнар. зб. наук. праць*. 2014. №2. С. 165-168. URL: <http://ibo.tneu.edu.ua/index.php/ibo/article/view/124>.
63. Підопригора О. А. Проблеми кодифікації законодавства про інтелектуальну власність. *Українське право.* 2013. С. 61 -80.
64. Подоляга А. Правове регулювання захисту комерційної таємниці. *Право України*. 2011. №4. С. 56-59.
65. Прo запровадження Нацioнальнoї системи iндикатoрiв рoзвитку iнфoрмацiйнoгo суспiльства : Постанова Кабінету Міністрів України від 28.11.2012 р. №1134. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/1134-2012-%D0%BF>.
66. Прo схвалення Стратегiї рoзвитку iнфoрмацiйнoгo суспiльства в Україні : Розпорядження Кабінету Міністрів України від 15.03.2013 р. №386-р. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80>.
67. Право інтелектуальної власності : підручник для студентів вищих навч. закладів / за ред. О. А. Підопригори, О. Д. Святоцького. Київ : Видавничий Дім «Ін Юре», 2002. 624 с.
68. Про банки і банківську діяльність : Закон України від 07.12.2000 №2121-III. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/2121-14>.
69. Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16.07.1999 №996-XIV. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/996-14>.
70. Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» : Закон України від 27.03.2014 №1170‑VII. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/1170-18>.
71. Про державну підтримку розвитку індустрії програмної продукції : Закон України від 16.10.2012. *Відомості Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/5450-17>
72. Про доступ до публічної інформації : Закон України від 13.01.2011 №2939-VI. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/2939-17>.
73. Про захист від недобросовісної конкуренції : Закон України від 07.06.1996. Відомості Верховної Ради України. URL*:* [https://zakon.rada.gov.ua/laws/show/236/96‑%D0%B2%D1%80](https://zakon.rada.gov.ua/laws/show/236/96%D0%B2%D1%80).
74. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/2297-17>.
75. Про інформацію : Закон України від 02.10.1992 №2657-XII. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/2657-12>.
76. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 №2163-VIII. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/2163-19>.
77. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. №537-V. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/537-16>.
78. Про перелік відомостей, що не становлять комерційної таємниці : Постанова Кабінету Міністрів України від 09.08.1993 №611. *Відомості Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF>.
79. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25.02.2017 №47/2017. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/47/2017>.
80. Продіус О. І. Концептуальні основи та функціональні складові економічної безпеки підприємства. *Глобальні та національні проблеми економіки.* Миколаїв, 2016. №10. С. 463-468 URL: <http://global-national.in.ua/archive/10-2016/96.pdf>.
81. Продіус О., Чупріна О., Ющук М. Актуальність економічної безпеки у контексті сталого розвитку підприємства. *Науковий вісник Одеського національного економічного університету.* 2016. № 10. С. 122-134. URL: <http://nbuv.gov.ua/UJRN/Nv_2016_10_11>.
82. Работягова Л.І Організаційно-юридичні засоби захисту прав на конфіденційну інформацію і/або комерційну таємницю. Теоретичні і практичні аспекти економіки та інтелектуальної власності. 2011. Т. 1. С. 194‑199. URL: <http://eir.pstu.edu/bitstream/handle/123456789/331/35.1.pdf?sequence=1>.
83. Рим О. М. Запобігання конкуренції у трудових правовідносинах : автореф. дис. ... канд. юрид. наук : 12.00.05. Львів, 2008. 16 с.
84. Рождественська О. С. Особливий суб’єкт інформаційних правовідносин (загальнотеоретичний аспект) : дис. … канд. юрид. наук : 12.00. Харків, 2009. 315 с.
85. Руколайніна І. Є. Захист інформаційної безпеки як об’єкта забезпечення в діяльності поліції. *Юридичний науковий електронний журнал.* 2016. №2. С. 93‑96 URL: <http://www.lsej.org.ua/2_2016/27.pdf>.
86. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки.* Запоріжжя, 2016. №1. С. 155-161. URL: <http://www.irbis-nbuv.gov.ua/UJRN/Vznu_eco_2016_1_21>.
87. Семилетов С. И. Информация как особый нематериальный объект права. *Государство и право*. 2000. № 5. С. 67-74.
88. Сляднєва  Г. О. Співвідношення категорій інформації та комерційної таємниці. *Актуальні проблеми держави і права.* 2009. № 50. С. 396-403.
89. Сороківська О. А. Особливості формування теоретичних засад економічної безпеки підприємств малого бізнесу. *Глобальні та національні проблеми економіки.* Миколаїв, 2015. №6. С. 486-494 URL: <http://globalnational.in.ua/archive/6-2015/101.pdf>.
90. Тынель А., Функ Я. Курс международного торгового права. Минск : Амалфея, 2000. 704 с.
91. Угода про торговельні аспекти прав інтелектуальної власності : Міжнародний документ від 15.04.1994. *Відомості Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/981_018>.
92. Угоди про заборону конкуренції (NCA) та їх чинність в Україні. URL: <http://www.dominuslegal.com/ugodi-pro-zaboronu-konkurentsiyi-nca-ta-yih-chinnist-v-ukrayini/>
93. Хлапонін Д. Ю. Механізм державного управління створенням та функціонуванням кіберфізичних систем : дис. … канд. наук з державного управління : 25.00.02 / Інститут підготовки кадрів Державної служби зайнятості України. Київ, 2019. 245 с.
94. Хороші зарплати і стабільне зростання: Що з себе представляє українська IT-галузь. URL: <https://ua.112.ua/statji/khoroshi-zarplaty-i-stabilne-zrostannia-shcho-z-sebe-predstavliaie-ukrainska-it-haluz-482651.html> (дата звернення 15.12.2019).
95. Цивільний Кодекс України від 16.01.2003. *Відомості Верховної Ради України.* URL: <https://zakon.rada.gov.ua/laws/show/435-15>.
96. Шакірова О. В. Захист права інтелектуальної власності: законодавчий аспект. *Збірник наукових праць Міжрегіональної фінансово- юридичної академії (економіка, право).* 2014. №1. С. 179-184.
97. Яковлев Д. О. Істотні умови договору про конфіденційність. *Проблемні питання цивільного та трудового права.* Дніпро : Видавечь Біла К. О. 2018. С. 28-30. URL: <http://er.dduvs.in.ua/bitstream/123456789/1453>.
98. Янків Б. Ю. Захист комерційної таємниці бізнесу. URL: <https://advokatura.lviv.ua/nerozholoshennya-komertsiynoyi-tayemnytsi/>