



Адміністративне право і процес; фінансове право; інформаційне право

УДК 005.94:338.24(477)

DOI <https://doi.org/10.5281/zenodo.15692009>

Конфіденційність комерційної інформації як складова економічної безпеки України

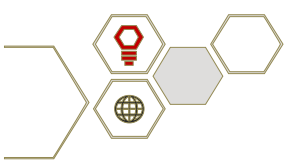
Волинець Віталій Валентинович

доктор юридичних наук, професор кафедри готельно-ресторанної справи,
Київський університет туризму, економіки і права,
вул. Князя Романа Мстиславича, 26, Київ, 02000, Україна,
e-mail: volinets.law@gmail.com, <https://orcid.org/0009-0003-0714-236X>

Прийнято: 03.06.2025 | Опубліковано: 16.06.2025

***Анотація.** Захист інформації є головним чинником забезпечення стабільності та конкурентоспроможності суб'єктів господарювання. Сучасний розвиток суспільства потребує дієвих механізмів збереження конфіденційної інформації, витік якої здатний завдати неоправної шкоди економічному сектору та економічній безпеці держави в цілому. Актуальність дослідження даного питання зумовлена впливом розвитку інформаційно-комунікаційних технологій, спрямованих на захист інформації в контексті забезпечення інформаційної безпеки. Поняття «інформаційна безпека» охоплює захист конфіденційності, гарантування безпеки конституційних прав та свобод громадян. Вона передбачає можливість вільного доступу до інформації та її раціонального використання, водночас актуалізуючи необхідність її захисту. В загальному, система захисту інформації покликана забезпечити її цілісність, достовірність та повноту.*

Метою статті є розгляд правових, організаційних та технічних аспектів забезпечення конфіденційності комерційної інформації як одного з ключових



елементів економічної безпеки України. Методологічну основу дослідження склали метод аналізу, а також порівняльно-правовий та системний підхід, який сприяв виявленню закономірностей у сфері захисту конфіденційної інформації в контексті економічної безпеки України. В процесі дослідження проведено аналіз нормативно-правового регулювання в Україні та виявлено низку проблем, пов'язаних із недостатньою адаптацією законодавства до умов цифрової трансформації економіки. Зроблено акцент на необхідності посилення захисту комерційної таємниці, а також захисту персональних даних. Визначено, що витік конфіденційної інформації може мати як короткострокові, так і довготривалі негативні наслідки - від зниження прибутковості підприємств до загроз для економічної безпеки держави. На основі проведеного аналізу запропоновано вектори вдосконалення політики захисту інформації в умовах цифрової економіки, з урахуванням сучасних викликів. Особливу увагу приділено формуванню ефективної стратегії інформаційної безпеки, яка б поєднувала законодавче регулювання, технічні рішення, а також сприяла б підвищенню інформаційної культури суб'єктів господарювання.

Ключові слова: інформація, конфіденційна інформація, економічна безпека, інформаційно-комунікаційні технології, комерційна інформація.

Confidentiality of commercial information as a component of economic security of Ukraine

Volynets Vitalii Valentynovych

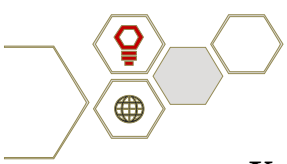
Doctor of Law, Professor, Professor of the Department of Hotel and Restaurant Business, Kyiv University of Tourism, Economics and Law,
26 Knyaz Roman Mstyslavych St., Kyiv, 02192, Ukraine,
e-mail: volynets.law@gmail.com, <https://orcid.org/0009-0003-0714-236X>

Abstract. Information protection is the main factor in ensuring the stability and competitiveness of business entities. The modern development of society requires



effective mechanisms for preserving confidential information, the leakage of which can cause irreparable harm to the economic sector and the economic security of the state as a whole. The relevance of the study of this issue is due to the influence of the development of information and communication technologies aimed at protecting information in the context of ensuring information security. The concept of "information security" covers the protection of confidentiality, guaranteeing the security of constitutional rights and freedoms of citizens. It provides for the possibility of free access to information and its rational use, while at the same time actualizing the need for its protection. In general, the information protection system is designed to ensure its integrity, reliability and completeness.

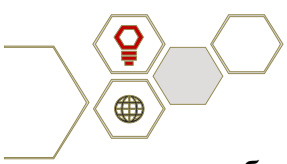
The purpose of the article is to consider the legal, organizational and technical aspects of ensuring the confidentiality of commercial information as one of the key elements of the economic security of Ukraine. The methodological basis of the study was the method of analysis, as well as a comparative legal and systemic approach, which contributed to the identification of patterns in the field of protection of confidential information in the context of the economic security of Ukraine. In the course of the study, an analysis of regulatory and legal regulation in Ukraine was conducted and a number of problems associated with insufficient adaptation of legislation to the conditions of the digital transformation of the economy were identified. Emphasis was placed on the need to strengthen the protection of trade secrets, as well as the protection of personal data. It was determined that the leakage of confidential information can have both short-term and long-term negative consequences - from a decrease in the profitability of enterprises to threats to the economic security of the state. Based on the analysis, vectors for improving information protection policy in the digital economy, taking into account modern challenges, were proposed. Special attention was paid to the formation of an effective information security strategy that would combine legislative regulation, technical solutions, and would also contribute to improving the information culture of business entities.



Keywords: *information, confidential information, economic security, information and communication technologies, commercial information.*

Постановка проблеми. В умовах сучасного розвитку суспільства, війни та росту кіберзагроз, питання забезпечення конфіденційності комерційної інформації набуло важливого значення. Економічна безпека держави залежить від здатності бізнесу захищати стратегічно важливі дані. Наразі правове регулювання захисту комерційної таємниці в Україні залишається фрагментарним та недостатньо-ефективним, ускладнюючи протидію внутрішнім та зовнішнім загрозам. Значна частина підприємств не впроваджує належні інформаційно-технічні засоби безпеки через обмежене фінансування, брак фахівців чи відсутність відповідної економічної політики. Низький рівень інформаційної культури працівників також створює передумови для витоку конфіденційних даних. В рамках цього зростає потреба в системному перегляді механізмів захисту інформації яка має обмежений доступ, враховуючи виклики російсько-української війни, постійні кібератаки та інші загрози. Зважаючи на це, актуальним є наукове осмислення шляхів посилення конфіденційності як одного з фундаментальних елементів економічної безпеки України.

Аналіз останніх досліджень і публікацій. Дослідженням питання конфіденційності комерційної інформації як складової економічної безпеки України займалися вітчизняні та міжнародні науковці. Так, В. М. Топалов [1] власне дослідження спрямував на забезпечення інформаційної безпеки бізнесу України в умовах сучасних загроз. Дослідник І. І. Кульчицький [2] розкриває головні аспекти цифрової економіки та економічної безпеки підприємств, роблячи акцент на стратегії управління інформацією. Дослідник С. П. Жигилій [6] визначає нормативно-правове забезпечення комерційної таємниці та місце у ньому законодавства про працю. Вітчизняні дослідники Г. П. Ситник та М. Г. Орел [13] розкривають зміст національної безпеки в контексті європейської інтеграції України, окремі вектори дослідження спрямовуючи на

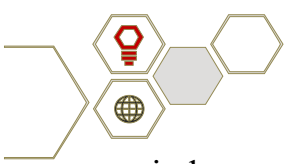


способи та механізми захисту конфіденційної комерційної інформації, як основу захисту національної безпеки.

Однак, незважаючи на напрацювання науковців, питання дослідження конфіденційності комерційної інформації, як складової економічної безпеки держави, залишається невирішеним, потребуючи додаткової розробки.

Виділення невирішених раніше частин загальної проблеми. У вітчизняному науково-правовому полі є чимало досліджень та нормативно-правових актів, зміст яких спрямований на регулювання питання захисту комерційної інформації. Однак не зважаючи на це, проблема залишається не вирішеною, потребуючи всебічного обговорення. Зокрема недостатньо розробленими є підходи, які сприяли б формуванню єдиної національної системи управління конфіденційною інформацією в умовах цифрової трансформації економіки. Не отримали й належного висвітлення питання взаємодії державних органів та бізнесу в контексті запобігання витоку комерційної таємниці, а також механізмів оперативного реагування на загрози у сфері інформаційної безпеки. Поміж з тим, відсутній системний аналіз ефективності законодавства у сфері захисту інформації з обмеженим доступом, як це відбувається в світі. Відкритим залишається також питання формування інформаційної культури суб'єктів господарювання, а також їх вміння дотримуватися режиму конфіденційності, оскільки будь який витік конфіденційної інформації призводить до економічних ризиків, ускладнюючи розробку новітніх технологій, завдаючи шкоди не лише окремим галузям економіки, а й державі в цілому. В умовах війни в Україні питання захисту конфіденційної інформації залишається надважливим, оскільки заволодіння конфіденційною інформацією може завдати шкоди економічній безпеці країни, підірвати її авторитет та спроможність конкурувати на міжнародному ринку.

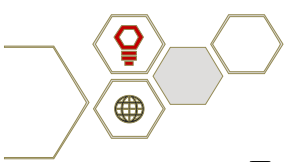
В рамках запропонованого автором дослідження важливо встановити значення конфіденційної комерційної інформації для економічної безпеки України; провести аналіз вітчизняного законодавства у сфері захисту комерційної таємниці; виявити основні загрози та ризики витоку конфіденційної



інформації; запропонувати шляхи вдосконалення механізмів захисту конфіденційної інформації та її впливу на економічну безпеку держави.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд правових, організаційних та технічних аспектів забезпечення конфіденційності комерційної інформації як одного з ключових елементів економічної безпеки України.

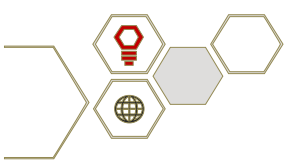
Виклад основного матеріалу дослідження. Стрімкий розвиток сучасного суспільства потребує ефективних механізмів захист конфіденційної інформації, оскільки будь-які оскільки будь-які неправомірні втручання або витoki такої інформації можуть завдати значної шкоди суб'єктам господарювання, підірвати їхню ділову репутацію та фінансову стабільність. У свою чергу це створює загрозу економічній безпеці держави, особливо в умовах тривалої російсько-української війни, кібервійни та інформаційної війни. На думку вітчизняного науковця В. М. Топалова, питання забезпечення інформаційної безпеки бізнесу наразі є досить актуальним в контексті збереження стабільності та забезпечення конкурентоспроможності різних рівнів економіки, особливо в умовах збройної агресії російської федерації проти України. Забезпечення належного рівня захисту інформаційних ресурсів суб'єктів господарювання виступає одним із пріоритетних завдань на сучасному етапі розвитку, враховуючи стрімку цифровізацію, активне впровадження хмарних технологій та інтернет-інфраструктури, посилюючи вразливість до кіберзагроз. Сучасні підприємства змушені реагувати на зростання ризиків, пов'язаних із витокom конфіденційної інформації, фінансових даних, елементів комерційної таємниці, а також загроз, що можуть завдати шкоди їхній репутації. Злочинні дії, зокрема хакерські атаки, фішинг та інші форми кіберзлочинності, здатні спричинити значні фінансові втрати й підірвати довіру клієнтів. У зв'язку з цим особливої ваги набуває питання впровадження сучасних систем кіберзахисту, формування внутрішньої політики інформаційної безпеки та системного підвищення рівня цифрової компетентності персоналу, що є невід'ємними умовами ефективного та безпечного функціонування бізнесу в добу цифровізації [1, с. 159].



Дослідник І. І. Кульчицький зазначає, що цифрова економіка, яка ґрунтується на використанні інформаційно-комунікаційних технологій, інноваційних та нематеріальних активів, здатна впливати не лише на традиційні моделі ведення бізнесу, але й на принципи формування системи економічної безпеки підприємств. Ці впливи мають як позитивні, так і негативні наслідки, підсилюючи необхідність адаптації суб'єктів господарювання реагувати на нові виклики цифрової епохи. З одного боку, цифрова економіка відкриває нові можливості для розвитку бізнесу. Використання сучасних технологій, зокрема штучного інтелекту та автоматизованих систем управління, сприяє підвищенню ефективності виробничих і управлінських процесів, оптимізуючи витрати та покращуючи якість продукції й послуг. Застосування цифрових платформ дозволяє підприємствам вчасно реагувати на зміни ринкової кон'юнктури, аналізувати поведінку споживачів тощо. Такий підхід посилює конкурентоспроможність підприємств, підвищуючи їх стійкість перед загрозами економіці держави.

Серед головних загроз та їх проявів дослідник виокремлює кіберзагрози, ненадійність інформаційних систем, незахищеність даних і порушення конфіденційності, конкурентні загрози в цифровому середовищі, фінансові шахрайства та цифрові злочини, залежність від зовнішніх постачальників цифрових послуг, низький рівень цифрової компетентності персоналу, зміна регуляторного середовища, інноваційна залежність, репутаційні ризики у цифровому середовищі [2]. Окреслені загрози та їх прояви мають вирішуватися як на державному так і на локальному рівнях. Для успішного функціонування бізнесу насамперед необхідно забезпечити збереження конфіденційної інформації. В рамках цього спробуємо розібратися, що таке «конфіденційна інформація» та яка її роль в комерційній діяльності.

Аналіз вітчизняної нормативно-правової бази дає підстави вважати, що забезпечення комерційної таємниці та визначення її ролі, в тому числі й в рамках трудового законодавства, є ключовим фактором, який впливає на регулювання комерційної таємниці як в умовах трудового договору в Україні, так і на основі



положень Конституції України. Так, відповідно до статті 41 Конституції [3], кожна особа має право володіти, користуватися та розпоряджатися своєю власністю, а також результатами інтелектуальної та творчої діяльності. Водночас стаття 13 Конституції передбачає, що держава забезпечує захист прав усіх суб'єктів права власності та господарювання. Норми Конституції України конкретизуються у відповідних положеннях законодавчих актів. Так, ст. 155 Господарського кодексу України [4] встановлює, що комерційна таємниця визнається об'єктом права інтелектуальної власності у сфері господарювання. Окремі положення цього кодексу регламентують правове врегулювання комерційної таємниці, зокрема заборону неправомірного збирання, розголошення та використання інформації, що становить комерційну таємницю. Цивільний кодекс України [5] містить фундаментальні норми правового регулювання інституту комерційної таємниці. Глава 46 Цивільного кодексу України «Право інтелектуальної власності на комерційну таємницю» складається з чотирьох статей, які визначають основні положення які врегульовують правовий статус комерційної таємниці в Україні. У змісті статей комерційна таємниця розглядається як інформація, що є секретною в тому розумінні, що вона в цілому або у певній формі і сукупності своїх складових є невідомою і недоступною для осіб, які зазвичай мають справу з відповідним видом інформації, носить комерційну цінність та охороняється відповідними заходами зі збереження її конфіденційності, вжитими особою, яка законно контролює таку інформацію. Крім того, у Цивільному кодексі визначаються майнові права інтелектуальної власності на комерційну таємницю, а саме: право на використання комерційної таємниці; виключне право дозволяти її використання; виключне право запобігати неправомірному розголошенню, збору або використанню інформації, що становить комерційну таємницю; інші майнові права, встановлені законом. Вказано, що такі майнові права належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не передбачено договором. Окрім того, Цивільний кодекс регламентує строк дії права інтелектуальної власності на комерційну таємницю та передбачає



обов'язок органів державної влади щодо забезпечення охорони комерційної таємниці. Належну увагу варто приділити також і трудовому законодавству. Дослідження та аналіз місця трудового законодавства у системі нормативно-правового забезпечення комерційної таємниці в Україні може свідчити про відсутність у ньому правових норм, які регулюють встановлення режиму комерційної таємниці в межах договірних та трудових відносин, а також порядок запровадження та реалізації матеріальної відповідальності за витік або втрату носіїв комерційної таємниці [6, с. 310].

Згідно зі статтею 21 Закону України «Про інформацію» [7], конфіденційною вважається така інформація, яка стосується фізичної особи або є обмеженою у доступі фізичними чи юридичними особами, за винятком органів державної влади. Така інформація може поширюватися за рішенням тієї особи, яка її обмежує, відповідно до визначених нею умов, якщо інше не передбачено законом. Водночас, стаття 7 Закону України «Про доступ до публічної інформації» [8] зазначає, що конфіденційною є інформація з обмеженим доступом, встановленим фізичною чи юридичною особою, крім органів влади, і вона може бути розголошена лише у випадках, передбачених законом.

Вітчизняна дослідниця Ю. Габрук термін «інформація» визначає як один з основних активів бізнесу, а полювання за інформацією є одним із нових видів діяльності. Разом з цим дослідниця підкреслює, що визначення «комерційна інформація» міститься в Цивільному та Господарському кодексах України і означає секретність, недоступність для широкого загалу, оскільки має комерційну цінність і має певні заходи збереження секретності, які вживаються з метою контролю цієї інформації. Термін «конфіденційна інформація» охоплює ширше коло відомостей в порівнянні із терміном «комерційна таємниця». З цього випливає, що будь-яка комерційна таємниця належить до конфіденційної інформації, проте не вся конфіденційна інформація може бути визнана комерційною таємницею. Так, дані про розмір заробітної плати не підпадають під визначення комерційної таємниці, однак вони можуть бути віднесені до конфіденційної інформації. У цьому контексті постає важливе питання щодо

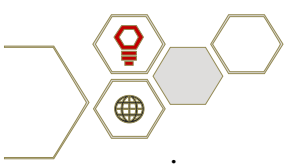


визначення переліку відомостей, доступ до яких може бути обмежений. Комерційною таємницею можуть вважатися відомості організаційного, технічного, виробничого, комерційного чи іншого характеру. При цьому саме керівник або засновник підприємства визначає перелік інформації, що становить комерційну таємницю або вважається конфіденційною. Це можуть бути дані про собівартість продукції, клієнтську базу, плани стратегічного розвитку, маркетингові стратегії, умови укладених договорів тощо.

У розглянутій від 23.11.2020 р. справі №910/1759/19 Верховний суд (КГС) [9] встановив, що інформація щодо повного переліку постачальників та клієнтів (покупців) ТОВ, в якій містяться контактні дані їх представників, розмір націнки, знижка на закупівлю продукції, вироблений обсяг, умови постачання – носить комерційний характер. Тобто, будь яка інформація, що має комерційну цінність для підприємства може вважатися конфіденційною. Винятком є відомості, які, згідно законодавства не можуть обмежуватися в доступі [10].

Безумовно, захист комерційної інформації набуває особливої ваги в умовах повномасштабної війни в Україні, оскільки підприємства стають не лише економічними, а й інформаційними цілями для ворога. Витоки стратегічно важливих відомостей, таких як плани розвитку, логістичні маршрути, контракти з партнерами чи обсяги виробництва, можуть використовуватися для підриву економічної стійкості, дискредитації бізнесу або нанесення прямої шкоди об'єктам інфраструктури. В умовах воєнного стану зростає кількість кіберзагроз, шпигунських атак і спроб отримання інформації ворожими кіберструктурами. Ці аспекти потребують від суб'єктів господарювання впровадження посиленних заходів захисту даних, зокрема технічних, правових та організаційних планів дій. В рамках цього, забезпечення конфіденційності комерційної інформації стає не лише питанням економічної безпеки окремого підприємства, а й елементом загальнонаціональної стратегії захисту від агресора.

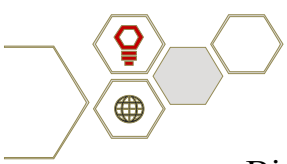
На думку Г. О. Андрощук, інформація та знання, які вона несе в собі, є важливим фактором виробництва, особливо в добу цифровізації. Комерційна таємниця, як різновид інформації та економічна категорія, зберігає корисні



відомості, які втратили б свою цінність під час їх оприлюднення широкій аудиторії. Разом з цим, розголошення конфіденційної інформації є ризиком для підприємця втратити факторний дохід, так звану інформаційну ренту. Інформаційна рента є частиною загального доходу підприємця, який би він отримав в процесі застосування власних чи законно набутих знань про процеси та явища економіки, техніки, суспільства. У сучасному економічному, технічному та соціальному середовищі створення інформації є складним і ресурсомістким процесом, який ґрунтується на інтелектуальному потенціалі працівників і завжди супроводжується елементом невизначеності. У зв'язку з цим наявність інституту комерційної таємниці постає як об'єктивна суспільна потреба. Законодавчий захист комерційно значимої інформації забезпечує досягнення кількох ключових цілей, серед яких:

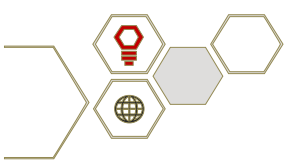
- стимулювання підприємницької діяльності - гарантії збереження конфіденційності заохочують інноваційність і розвиток підприємницьких можливостей;
- формування етичних стандартів у суспільстві - повага до чужої конфіденційної інформації є показником високого рівня моральної свідомості;
- зміцнення довіри між державою та бізнесом - державна підтримка у сфері захисту комерційної таємниці сприяє стабільності та ефективності економічної політики;
- підвищення ефективності підприємницької діяльності - комерційна таємниця є необхідною умовою досягнення позитивного економічного результату, хоч і не гарантує прибуток напряду;
- підтримка конкурентоспроможності - збереження унікальності знань і технологій дозволяє підприємствам ефективніше конкурувати на ринку.

Загалом, інститут комерційної таємниці виконує не лише економічну, а й соціальну функцію, зміцнюючи довіру, моральні принципи та інноваційний розвиток суспільства [11, с. 10].



Вітчизняний дослідник М. О. Шевчук вказує, що нині в Україні захист інформації має забезпечуватися на належному рівні, оскільки будь який витік згубно позначається на економіці країни. По факту інформаційна безпека забезпечує захист національних інтересів України. Інформаційна безпека - це сталий стан інформаційного простору, на основі якого ґрунтується цілісність і захищеність його об'єктів від негативних впливів як внутрішнього, так і зовнішнього характеру, на усвідомленні людиною власних цінностей, життєво важливих потреб та стратегічних цілей розвитку. Інформаційну безпеку України дослідник трактує як такий стан, за якого, незважаючи на існування реальних і потенційних загроз, забезпечується збереження, стабільний і поступальний розвиток інформаційної сфери. Це передбачає належний рівень захищеності інформаційної інфраструктури, інформаційного простору, ресурсів, процесів та їх суб'єктів, а також досягнення національних стратегічних цілей і реалізацію інтересів держави у сфері інформації. Водночас, забезпечення інформаційної безпеки є безперервною діяльністю уповноважених органів, спрямованою на виявлення, запобігання та нейтралізацію загроз, застосування заходів інформаційного впливу, а також створення умов, які дозволяють ефективно реалізовувати і контролювати цю діяльність.

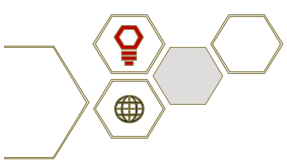
Складна воєнно-політична ситуація, спричинена російсько-українською війною, породила серйозні загрози у сфері інформаційного простору. З огляду на стратегічну важливість інформаційного середовища для стабільного розвитку сучасного суспільства, питання інформаційної безпеки посідає провідне місце в системі національної безпеки України. Як одна з її ключових складових, інформаційна безпека охоплює пріоритетні напрями, серед яких - захист національного інформаційного простору та охорона культурного генофонду людства в умовах розвитку суспільства. При цьому, крім правових, організаційних та технічних інструментів, вагому роль у забезпеченні безпеки інформаційного середовища відіграють соціокультурні чинники [12, с. 134]. В Україні сфери національної безпеки зазвичай розглядаються крізь призму наявних загроз. Подекуди навіть висловлюється думка, що саме загрози



служать основою для формування державної політики у сфері національної безпеки та виступають її ключовим елементом [13, с. 29]. Таким чином, якщо брати до уваги діяльність підприємств, які займаються виготовленням продукції для оборони держави, збереження конфіденційної комерційної інформації має цілком логічне призначення. В умовах російсько-української війни забезпечення нерозголошення відомостей, що стосуються технологічних процесів, обсягів виробництва, логістики, складу замовників та контрагентів, набуває особливої ваги. Така інформація може бути об'єктом цілеспрямованих кібератак, розвідки ворога або внутрішнього витоку, наслідком чого стане підрив обороноздатності держави та її економічної стійкості. Відповідно до цього, формування ефективної системи захисту комерційної таємниці у сфері військово-промислового комплексу є важливою складовою загальної стратегії забезпечення національної безпеки та оборони України. Окреслене питання вимагає комплексного підходу до нормативно-правового регулювання, технічного захисту інформації та підвищення відповідальності суб'єктів господарювання щодо дотримання режиму конфіденційності.

На думку О. М. Кравченко, для того щоб забезпечити на підприємстві збереження конфіденційності комерційної інформації необхідно здійснити правове регулювання не тільки на рівні нормативно-правових актів, якими визначається регулювання комерційної інформації, а й на локальному рівні - прийняти нормативно-правові акти, інструкції, накази, які б також забезпечували можливість збереження і нерозголошення такої інформації третім особам [14, с. 192].

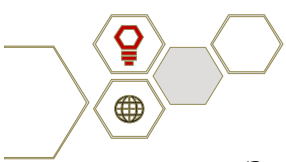
Відповідно до положень статті 162 Господарського кодексу України [4], суб'єкт господарювання, який володіє технічною, організаційною або іншою комерційною інформацією, має право на її правовий захист від неправомірного використання третіми особами. Такий захист надається за умови, що зазначена інформація є комерційно цінною, оскільки вона невідома іншим особам, не має відкритого доступу на законних підставах та за умови, що її володілець здійснює достатні заходи для забезпечення її конфіденційності. Отже, чинне



законодавство встановлює правову охорону комерційної таємниці, як об'єкта інтелектуальної власності та інструменту забезпечення економічної безпеки суб'єктів господарювання. [15, с. 178]

Вітчизняний науковець С. П. Жигилій зазначає, що наявність дієвого нормативно-правового забезпечення, яке реалізується державними інституціями, органами державної влади та місцевого самоврядування, є одним із ключових аспектів правового регулювання комерційної таємниці в Україні. Інститут комерційної таємниці знайшов своє відображення у низці нормативно-правових актів, проте у сфері трудового права аналогічних положень, на жаль, не сформовано. Нині чинне трудове законодавство не містить чітких норм, які регулюють режим використання комерційної таємниці, не встановлює порядок її застосування у трудових відносинах, не регламентує заходи роботодавця щодо запобігання розголошенню конфіденційної інформації, а також обов'язки працівника щодо забезпечення її збереження. Відсутній також визначений алгоритм дій роботодавця у випадках виявлення незаконного розповсюдження комерційної таємниці та, що особливо важливо, механізми відшкодування збитків, завданих протиправною поведінкою працівника. Внаслідок цього відсутність відповідних законодавчих норм створює умови як для порушення прав працівників, так і для завдання шкоди економічним інтересам роботодавців [6, с. 310].

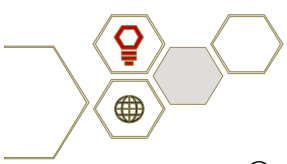
Деякі дослідники, зокрема й О. М. Кравченко, у власних дослідженнях пропонував розробити та прийняти Закон України «Про охорону прав на комерційну таємницю», який би сприяв впровадженню системного підходу до правового регулювання відносин, пов'язаних із захистом комерційної таємниці, а також дозволив би упорядкувати, уточнити та доповнити існуючі законодавчі норми у цій сфері. Альтернативним варіантом стало б і внесення змін до окремих нормативно-правових актів, які регулюють питання охорони комерційної таємниці. Однак такий підхід не забезпечить повноцінної систематизації законодавства, пов'язаного з комерційною таємницею [16].



З огляду на проведенні дослідження науковців необхідно вказати, що пріоритетними є саме правові заходи, оскільки їх основна мета полягає у забезпеченні ефективного функціонування комплексної системи захисту комерційної таємниці. До таких заходів належать розробка положень у сфері гарантування збереження комерційної таємниці, інформування про відповідальність за нерозголошення конфіденційної інформації, а також укладання договорів про матеріальну відповідальність у разі її розкриття [17, с. 112].

Загрози комерційній таємниці традиційно поділяють на внутрішні та зовнішні. Внутрішні загрози виникають безпосередньо всередині організації, тоді як зовнішні - поза її межами. До внутрішніх загроз належать: недоліки у роботі з персоналом; низький рівень організації обігу документів, що містять комерційну таємницю; невирішені соціальні проблеми працівників; висока плинність кадрів та відсутність кваліфікованих фахівців у сфері захисту комерційної таємниці; неефективна діяльність служби економічної безпеки; а також недостатній технічний рівень захисту інформаційних ресурсів підприємства. Зовнішні загрози включають промислове шпигунство, незаконні дії конкурентів, протиправні дії кримінальних груп, а також неправомірні дії працівників правоохоронних органів. Найбільш поширеними способами витоку комерційної таємниці є розголошення інформації працівниками (як навмисне, так і ненавмисне), а також отримання даних через технологічні атаки на системи захисту інформації.

У законодавстві передбачено важливий механізм захисту прав на комерційну таємницю - компенсацію, яка, однак, не є тотожною відшкодуванню збитків. Компенсація застосовується виключно у випадках, коли суд не має сумнівів щодо наявності збитків у потерпілого, але визначення їхнього точного розміру є надзвичайно складним. Враховуючи це, закон не встановлює чітких грошових меж для розміру компенсації, оскільки вважає таке регулювання недоцільним.



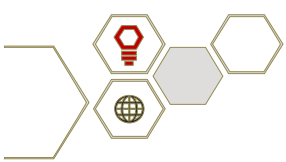
Організаційна форма захисту комерційної таємниці зосереджується на здійсненні самостійних дій, спрямованих на забезпечення її безпеки в межах організаційної структури. Технічна складова цієї форми включає:

- впровадження сучасних і надійних технічних засобів, що забезпечують ефективний режим охорони інформації;
- використання обладнання, здатного швидко або в стислі терміни виявляти потенційні канали витоку конфіденційних відомостей;
- здійснення регуляторного моніторингу функціонування системи захисту інформації;
- застосування таких носіїв інформації, які унеможливають несанкціоноване копіювання або відтворення конфіденційних даних;
- використання надійних систем паролів для обмеження доступу до комерційної таємниці та інших захисних механізмів [18, с. 22].

Отже, на основі проведеного дослідження важливо вказати, що розробка програм стратегічного управління економічною безпекою підприємств передбачає не лише реалізацію комплексних заходів щодо її функціонування, а й оптимізацію економічних та екологічних процесів, управління кадровими ресурсами, а також обов'язкове впровадження надійної системи інформаційної безпеки. Серед головних напрямів її забезпечення необхідно вказати:

- постійне оновлення технічного обладнання та впровадження технологій із високим рівнем захисту;
- створення автономної інфраструктури для зберігання конфіденційної інформації, а також забезпечення резервних джерел електроенергії для безперебійної роботи захисних систем у разі збоїв;
- формування електронної бази даних, що містить інформацію, яка має статус комерційної таємниці підприємства.

Водночас у контексті цифрової трансформації не можна ігнорувати необхідність побудови ефективної кадрової політики, оскільки навіть найсучасніші засоби захисту не забезпечать належного рівня безпеки без усвідомлення значущості конфіденційності працівниками. З огляду на специфіку

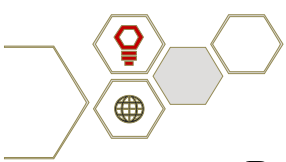


розвитку цифрової економіки, суспільство й надалі зіштовхуватиметься з новими викликами, розв'язання яких потребуватиме невідкладних дій. На підставі викладеного можна зробити висновок, що в найближчій перспективі забезпечення кадрової безпеки має ґрунтуватися на побудові ефективної системи безперервної професійної освіти для працівників, які відіграють ключову роль у розвитку суспільства і держави в цілому. Водночас, важливим є формування лояльного кадрового складу шляхом створення позитивного соціально-психологічного клімату, розвитку корпоративної культури, задоволення потреб персоналу та запровадження результативної системи мотивації.

Загалом, організація захисту комерційної таємниці у межах трудових відносин здійснюється за двома основними напрямками:

- працівники, які мають доступ до інформації, що становить комерційну таємницю, зобов'язані зберігати її конфіденційність і не розголошувати отримані відомості;
- працівники, які не мають доступу до такої інформації, не повинні здійснювати спроби її збору чи використання у неправомірний спосіб [19, с. 86].

Отже, конфіденційність комерційної інформації є ключовим чинником забезпечення економічної безпеки України в умовах цифровізації та глобалізації. Недостатнє правове регулювання захисту комерційної таємниці, особливо в контексті трудових відносин, створює загрози для стабільності підприємств та конкурентоспроможності національної економіки. Ефективна система захисту має охоплювати як правові, так і організаційно-технічні заходи, включаючи кібербезпеку та кадрову політику. Особливу увагу слід приділяти формуванню культури конфіденційності серед працівників і безперервному професійному навчанню. Необхідним є також удосконалення законодавства та розробка спеціального закону про охорону прав на комерційну таємницю. Лише комплексний підхід до захисту конфіденційної інформації дозволить підвищити рівень економічної безпеки держави.



Висновки. Захист конфіденційної комерційної інформації є важливим чинником зміцнення економічної безпеки України. Аналіз вітчизняного законодавства та наукових досліджень науковців, які працювали в цьому напрямку дав змогу виявити низку прогалин у сфері правового захисту комерційної таємниці, тим самим підвищуючи ризики витоку важливих даних. Основними загрозами є кіберзлочинність, низький рівень знань персоналу та недосконалість внутрішньої політики захисту такої інформації. Серед запропонованих шляхів вдосконалення механізмів захисту найперше необхідно виокремити інтеграцію правових, організаційних та технологічних заходів, які впроваджуються в діяльність підприємств, забезпечуючи безперервний захист інформаційно-конфіденційного поля. Подальші дослідження доцільно спрямувати на розробку моделей оцінювання ефективності захисту інформації на підприємствах. Окрім того важливим є вивчення впливу цифрових трансформацій на безпеку комерційної інформації в умовах воєнного та поствоєнного періодів. Перспективою подальших досліджень є підсилений аналіз впливу сучасних цифрових технологій, зокрема штучного інтелекту та блокчейну, на підвищення рівня захисту конфіденційної комерційної інформації. Важливо також розробити комплексні підходи до управління ризиками, пов'язаними з витоком інформації, з урахуванням специфіки вітчизняного бізнесу. Крім того, перспективним є дослідження ефективності впровадження міжнародних стандартів інформаційної безпеки в різних галузях економіки України. Особливу увагу варто приділити створенню механізмів державної підтримки підприємств у сфері кібербезпеки та захисту комерційної інформації. Такий підхід сприятиме посиленню економічної безпеки держави в умовах появи нових зовнішніх і внутрішніх загроз.

Список використаних джерел

1. Топалов В. М. Забезпечення інформаційної безпеки бізнесу України в умовах сучасних загроз. Цифрова економіка та інформаційна безпека. Випуск



6(15). 2024. С. 157 – 161. URL:
<http://www.dees.iei.od.ua/index.php/journal/article/view/509/490>

2. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. Актуальні питання економічних наук. URL: <https://a-economics.com.ua/index.php/home/article/view/123/126>

3. Конституція України: Закон України від 28 червня 1996 р. №254к/96-ВР. Відомості Верховної Ради України. 1996, №30, Ст. 141.

4. Господарський кодекс України від 16.01.2003 р. № 436-IV. URL: [URL://zakon2.rada.gov.ua/laws/show/436-15/page](http://zakon2.rada.gov.ua/laws/show/436-15/page)

5. Цивільний кодекс України від 16.01.2003 р. № 435-IV. URL: [URL://zakon3.rada.gov.ua/laws/show/435-15/paran2312#n2312](http://zakon3.rada.gov.ua/laws/show/435-15/paran2312#n2312)

6. Жигилій С. П. Нормативно-правове забезпечення комерційної таємниці та місце у ньому законодавства про працю. Науковий вісник Ужгородського Національного Університету. 2023. С. 309 – 314. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/08/52-1.pdf>

7. Про інформацію: Закон України. Верховна Рада України. URL: [URL://zakon.rada.gov.ua/laws/show/2657-12#Text](http://zakon.rada.gov.ua/laws/show/2657-12#Text)

8. Про доступ до публічної інформації : Закон України / Верховна Рада України. URL: [URL://zakon.rada.gov.ua/laws/show/2939-17#Text](http://zakon.rada.gov.ua/laws/show/2939-17#Text)

9. Справа №910/1759/19. URL: <https://zakononline.com.ua/court-decisions/show/93149537>

10. Габрук Ю. Охорона конфіденційної інформації та комерційної таємниці: як? що? навіщо? Юридична газета online. 2022. URL: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ohorona-konfidenciynoyi-informaciyi-ta-komerciynoyi-taemnici-yak-shcho-navishcho.html>

11. Андросук Г. О. Комерційна таємниця як фактор забезпечення національної економічної безпеки: практика Китаю. Наука, технології, інновації. Випуск 2. 2022. С. 10-21. URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/61fbc9f7-5aae-4981-91a6-e75dba948d01/content>



12. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського Національного Університету. Випуск 78 (2). 2023. С. 1334-139. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/08/23.pdf>

13. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України. Київ: Міжрегіональна Академія управління персоналом, 2021. 372 с.

14. Кравченко О. М. Інтеграція стандартів охорони конфіденційної інформації та комерційної таємниці України до стандартів європейського союзу. Південноукраїнський правничий часопис. Випуск 2. 2022. С. 189-195. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_2/29.pdf

15. Кравченко О. М. Інтеграція стандартів охорони комерційної таємниці України до європейського бізнес-середовища. Спецвипуск. Том 1. 2022. С. 175 – 181. URL: <https://law.journalsofznu.zp.ua/archive/visnik-spec-1-2022/25.pdf>

16. Про схвалення Концепції проекту Закону України «Про охорону прав на комерційну таємницю»: розпорядж. Каб. Міністрів України від 05.11.2008 № 1404-р. URL: <https://zakon.rada.gov.ua/laws/show/1404-2008-%D1%80#Text>

17. Зайцева-Калаур І. Організаційно-правові процедури забезпечення охорони та захисту комерційної таємниці суб'єкта господарювання. Актуальні проблеми правознавства. 2018. Вип. 4. С. 110-115.

18. Левченко О. М., Левченко А. О., Немченко Т. А. Захист конфіденційної таємниці в контексті стратегічного управління економічною безпекою організації в умовах цифровізації економіки. Центральнотукраїнський науковий вісник. Економічні науки. Випуск 6(39). 2021. С. 20-30. URL: <https://journals.indexcopernicus.com/api/file/viewByFileId/1582418>

19. Тугарова О. К., Шепета О. В. Організаційно-правові питання захисту комерційної таємниці. Науковий вісник Ужгородського національного університету. Серія : Право. 2018. Вип. 52(2). С. 85-88.