ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ЛОКАЛЬНОМУ РІВНІ ПІДПРИЄМСТВА

ШЕБАНІЦ Діана Миколаївна - кандидат історичних наук, доцент, доцент кафедри права Маріупольського державного університету

ORCID.ID: 0000-0002-8897-9721

ШЕБАНІЦ Віталій Федорович - здобувач 3 курсу спеціальності 081 «Право» Маріупольського державного університету

ORCID.ID: 0009-0001-3699-9974

УДК 342.951:316.77

DOI: https://doi.org/10.71404/EP.2025.1.24

У статті досліджено особливості правового регулювання забезпечення інформаційної безпеки на локальному рівні підприємства. Проаналізовано національне законодавство України щодо визначення понять «інформація», «інформація з обмеженим доступом» та «комерційна таємниця».

Під інформацію з обмеженим доступом підпадають конфіденційні, таємні та службові відомості. Зазначено, що інформація про фізичну особу (персональні дані), а також будь-які дані, доступ до яких обмежений приватною чи юридичною особою, мають спеціальний статус захисту, крім випадків, коли це стосується суб'єктів владних повноважень. Доведено, що конфіденційними вважаються відомості про дату та місце народження, освіту, стан здоров'я, майновий стан, релігійні переконання та інші персональні характеристики.

Розглянуто основні проблеми у сфері захисту комерційної інформації, зокрема недоліки в чинній нормативно-правовій базі, які впливають на ефективність її охорони. Запропонована низка змін до законодавства, спрямованих на вдосконалення правового захисту комерційної таємниці, зокрема уточнення її визначення, розмежування понять «конфіденційна інформація» та «комерційна таємниця», а також підвищення відповідальності за неправомірне розголошення. Рекомендовано для забезпечення комплексного захисту комерційної таємниці та конфіденційної інформації бізнесу використовувати наступні види заходів: юридичні, організаційні та технічні.

У дослідженні також розглянуто вдалий досвід Польщі у сфері правового регулювання забезпечення інформаційної безпеки на рівні підприємств, зокрема використання інноваційних технологій (штучний інтелект, кібернетичні системи, технологія блокчейн, використання біометричних даних), впровадження стандартів безпеки та підвищення культури захисту даних. Запропоновано рекомендації для адаптації найкращих польських практик в Україні.

Ключові слова: інформаційна безпека, комерційна таємниця, інформація з обмеженим доступом, правове регулювання, підприємство.

Постановка проблеми

У сучасних умовах розвитку цифрових технологій питання інформаційної безпеки набувають особливого значення для суб'єктів господарювання. Витік комерційно важливої інформації або комерційної таємниці може завдати значних економічних збитків, негативно вплинути на репутацію підприємства та його конкурентоспроможність. На локальному рівні забезпечення інформаційної безпеки залежить як від впровадження технічних і організаційних заходів, так і від ефективності правового регулювання цієї сфери.

В Україні проблема правового забезпечення інформаційної безпеки залишається актуальною, адже законодавство досі має

низку недоліків. Зокрема, відсутність чіткого розмежування понять «конфіденційна інформація» та «комерційна таємниця» створює труднощі у визначенні правового статусу інформації, що ускладнює її охорону. Недостатньо врегульовані питання обліку комерційної інформації як нематеріального активу, порядок її передачі органам влади та відповідальність за неправомірне розголошення.

Водночас міжнародний досвід демонструє успішні приклади вдосконалення системи правового захисту інформації на рівні підприємств. Провідні європейські країни активно впроваджують сучасні стандарти інформаційної безпеки, використовуючи інноваційні технології, а також стимулює бізнес до розвитку культури захисту даних.

Метою цієї статті є аналіз чинного законодавства України у сфері інформаційної безпеки підприємств, визначення його недоліків та шляхів вдосконалення, а також вивчення міжнародного досвіду з метою адаптації найкращих практик до українських реалій.

Стан опрацювання проблематики

З огляду на актуальність порушеного нами питання, вважаємо доречним пригадати українських дослідників, роботи яких є вагомим внеском у розвиток наукової думки у сфері інформаційної безпеки. Так, не можна не згадати К. Бєлякова, В. Колпакова, М. Каратай, Т. Коломоєць, А. Марущака, І. Яромій, О. Кравченко та інш.

Виклад основного матеріалу

Перш ніж перейти до питання правового регулювання забезпечення інформаційної безпеки на локальному рівні підприємства, вважаємо доречним детальніше зупинитися на законодавчому підґрунті зазначеного питання. Отож, згідно із Законом України «Про інформацію» від 2 жовтня 1992 року №2657-XII (зі змінами), визначення інформації є наступним: це будь-які дані та/або відомості, що можуть бути представлені на матеріальних носіях або в електронному форматі. За умовами доступу інформація поділяється на відкриту та таку, що має обмежений доступ. Згідно з цим, інформація є відкритою, якщо інше не встановлено законом [1].

Під інформацію з обмеженим доступом підпадають конфіденційні, таємні та службові відомості. Визначення цих категорій, а також умови доступу до такої інформації регулюються законами. Також зазначаємо, що інформація про фізичну особу (персональні дані), а також будь-які дані, доступ до яких обмежений приватною чи юридичною особою, мають спеціальний статус захисту, крім випадків, коли це стосується суб'єктів владних повноважень.

Крім того, стаття 11 Закону України «Про інформацію» та стаття 14 Закону «Про захист персональних даних» № 2297-VI визначають, що збір, зберігання та поширення конфіденційної інформації щодо особи без її згоди забороняється, за винятком випадків, що регулюються законом і служать національній безпеці, економічному добробуту чи захисту прав людини. Передача персональних даних можлива лише за згодою суб'єкта таких даних [1].

Конфіденційними вважаються відомості про дату та місце народження, освіту, стан здоров'я, майновий стан, релігійні переконання та інші персональні характеристики. Згідно зі ст. 182 Кримінального кодексу України, незаконні дії щодо збору, зберігання, використання, поширення чи зміни конфіденційної інформації без згоди особи караються штрафом або іншими видами покарань, включаючи виправні роботи або обмеження волі на певний термін [2].

Наразі гостро стоїть питання про вдосконалення законодавчих норм і підвищення технологічного рівня захисту інформації, адже стрімкий розвиток інформаційної сфери висуває нові вимоги до забезпечення конфіденційності та захисту прав на інтелектуальну власність. Ми розділяємо думку деяких науковців, що для ефективного захисту прав фізичних осіб та організацій потрібна взаємодія правоохоронних органів, бізнесу та громадянського суспільства [3, с. 240].

Самозахист прав на комерційну таємницю (КТ) та конфіденційну інформацію бізнесу в Україні першочергово полягає у створенні ефективної системи адміністративно-правової охорони. Надійний захист інформації має забезпечувати від неправомірного посягання та сучасних загроз.

Нагадаємо, що, відповідно до статті 21 Закону України «Про інформацію», інформація з обмеженим доступом охоплює конфіденційну, таємну та службову інформацію. Згідно з цим законом, конфіденційною визнається інформація, доступ до якої обмежений фізичною або юридичною особою, крім органів державної влади [1]. Слід зауважити, що подібне визначення наводиться у статті 7 Закону України «Про доступ до публічної інформації», де додатково зазначено, що поширення такої інформації можливе лише за бажанням власника відповідно до визначених ним умов [4]. Щодо комерційної таємниці, її правове визначення наведене в Цивільному кодексі України та Господарському кодексі України. Однак сучасна нормативно-правова база потребує вдосконалення, зокрема в частині відповідальності за неправомірні дії стосовно комерційної інформації підприємства. На сьогодні за такі порушення передбачено матеріальну відповідальність. Відтак, чинне цивільне законодавство України наголошує на тому, що комерційна таємниця в будь-якій формі чи комбінації її складових, залишається невідомою та недоступною для осіб, які зазвичай мають справу з відповідним видом інформації. Така інформація має економічну цінність через свою закритість і є предметом заходів для збереження її секретності, які вживає особа, що законно контролює цю інформацію. У статті 162 Господарського кодексу України (ГКУ) йдеться про право суб'єкта господарювання на захист технічної, організаційної чи іншої комерційної інформації від неправомірного використання третіми особами. Це можливо за умови, що така інформація має комерційну цінність, невідома іншим особам, до неї немає законного доступу, а власник вживає заходів для її охорони. Стаття 505 Цивільного кодексу України використовує термін «особа», але не уточнює, чи це фізична чи юридична особа. Для усунення неоднозначності пропонується чітко вказати, що йдеться саме про юридичну особу, і сформулювати положення таким чином: комерційна таємниця — це інформація, яка є секретною в тому сенсі, що вона загалом чи у визначеній формі є невідомою та недоступною для осіб, які зазвичай працюють із цим видом інформації. Вона має комерційну цінність і є об'єктом належних заходів захисту, вжитих юридичною особою, яка її контролює [5, 6]. У статті 162 Господарського кодексу України також слід внести уточнення, замінивши термін «володілець комерційної таємниці» на «власник комерційної таємниці» і виключивши посилання на конфіденційність, яка більше стосується персональних даних. Зокрема: «Суб'єкт господарювання, що є власником технічної, організаційної чи іншої комерційної інформації, має право на захист від неправомірного використання цієї інформації третіми особами за умови, що вона має комерційну цінність, невідома іншим і до неї немає вільного доступу, а власник вживає заходів для її охорони» [7, с. 23-24].

Для ефективного захисту комерційної таємниці підприємствам рекомендовано використовувати комплекс заходів, які включають правові, організаційні та технічні механізми. У свою чергу, держава має підтримувати бізнес у створенні надійної системи охорони інформації, оскільки це безпосередньо сприяє економічному зростанню країни [8, с. 670].

Аналіз чинного національного законодавства та актуальної юридичної наукової літератури дозволив розробити низку наступних пропозицій для вдосконалення системи захисту комерційної таємниці в Україні, а саме:

– розмежування понять конфіденційної інформації фізичних осіб (КІ) та конфіденційної інформації бізнесу (КІБ). Кожне з цих понять потребує окремих методів охорони для запобігання витокам та незаконним діям;

– вдосконалення термінології законодавства. Оскільки в законодавстві згадується можливість обмеження доступу до

інформації юридичними особами, бізнес може класифікувати комерційно цінну інформацію як КІ або КТ. Це вимагає чіткого визначення меж КІ фізичних осіб та КІБ;

– уточнення поняття комерційних секретів (КС) як інформації, що має цінність у сфері бізнесу та стосується технічних, виробничих чи організаційних секретів підприємства. Сукупність КС складає комерційну таємницю;

– перегляд визначення комерційної таємниці (КТ) як інформації, що має цінність для суб'єкта господарювання та захищається від незаконного використання. Її власник зобов'язаний вживати заходів для збереження конфіденційності;

– уточнення поняття КІ фізичних осіб як персональних даних, які можуть охоплювати сімейні секрети, місце роботи, склад сім'ї тощо;

– запровадження чіткого визначення КІБ як інформації, яка є критично важливою для бізнесу і у випадку її витоку може негативно вплинути на його фінансові показники;

– віднесення КІ та КІБ, що обробляються державними органами, до категорії службової інформації для посилення їхнього захисту [8, с. 671].

Зазначимо, що, на нашу думку, такі заходи неодмінно сприятимуть підвищенню рівня правового захисту комерційної та конфіденційної інформації, що є особливо актуальним в умовах сучасних загроз.

Окрім цього, для забезпечення комплексного захисту КТ і конфіденційної інформації бізнесу (КІБ) необхідно використовувати такі заходи:

– юридичні заходи. Включають розробку внутрішніх документів підприємства, таких як статут, засновницький договір, колективний договір, положення про КТ, правила її збереження та доступу до інформації;

– організаційні заходи. Передбачають обмеження доступу до інформації шляхом створення підрозділів безпеки або призначення відповідальних осіб у малих підприємствах;

– технічні заходи. Використання обладнання, програмного забезпечення та інших засобів захисту для запобігання витоку інформації чи технічним витівкам (ТБШ) [7, с. 24].

Також вважаємо доречним зазначити, що, на думку юридичної національної наукової спільноти, доцільно створювати підрозділи конкурентної розвідки або служби безпеки підприємств для ефективної протидії загрозам.

До того ж, на нашу думку, варто акцентувати увагу на тому, що в Україні вже давно назріла потреба в ухваленні спеціального міжгалузевого нормативно-правового акта, що комплексно регулював би питання, пов'язані зі створенням, використанням, збереженням та розголошенням конфіденційної інформації (КІ) або комерційної таємниці (КТ). На думку національної юридичної наукової спільноти у такому акті мають бути чітко визначені:

– поняття КІ та КТ, їх ознаки й умови правової охорони;

– перелік відомостей, які можуть становити або не становити КТ;

– порядок виникнення прав на КТ у суб'єктів господарювання;

– можливість обліку КІ або КТ як нематеріального активу;

– процедура надання доступу до КІ або КТ для правоохоронних та контролюючих органів;

– відповідальність державних органів за розголошення комерційної інформації;

– методи захисту КІ або КТ, адаптовані до сучасних викликів [9, с. 478-479].

Зазначимо, що сьогодні підприємства самостійно реалізують заходи захисту, використовуючи локальні нормативні акти, такі як положення про КТ, правила доступу до інформації та інші внутрішні документи. Однак ефективний захист КІ або КТ, як ми вже зазначали раніше, можливий лише за умови інтеграції правових, організаційних, технічних та адміністративних механізмів. Тож, на нашу думку, задля вирішення проблем у сфері охорони комерційної інформації необхідно розробити та ухвалити Закон України «Про комерційну таємницю», який встановить чіткі правила її захисту. Щодо конфіденційної інформації, важливо уточнити, що цей термін має

стосуватися лише фізичних осіб. Погоджуємося з рекомендаціями деяких науковців щодо виключення згадки про юридичних осіб із визначення КІ, уточнивши його, наприклад наступним чином: конфіденційна інформація — це дані, доступ до яких обмежено фізичною особою і які можуть поширюватися лише за її бажанням відповідно до встановлених умов [9, с. 479].

Вважаємо доцільним проаналізувати та дослідити вдалий досвід європейських країн у сфері правового регулювання забезпечення інформаційної безпеки на локальному рівні підприємства. Відтак, Польща активно адаптується до зростаючих кіберзагроз, впроваджуючи новітні технології та інноваційні методи для посилення інформаційної безпеки. У рамках цих зусиль у країні реалізуються конкретні заходи, спрямовані на підвищення ефективності захисту даних. З-поміж таких варто пригадати наступні інноваційні заходи:

– Розробляються системи штучного інтелекту (ШІ), які аналізують дані з різних джерел і виявляють потенційні кіберзагрози. Завдяки швидкому аналізу та розпізнаванню аномальної активності ШІ сприяє оперативному реагуванню на атаки.

– Впроваджуються кібернетичні системи, здатні ідентифікувати вразливості програмного забезпечення, аномальну поведінку та інші слабкі місця, що дозволяє вчасно нейтралізувати потенційні загрози.

– Технологія блокчейн застосовується для створення надійних, незмінних баз даних, що гарантують цілісність і захищеність інформації, а також можливість виявлення будь-яких спроб несанкціонованих змін.

– Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя чи голосу, значно підвищує рівень захисту доступу до інформаційних систем.

– Методи машинного навчання допомагають аналізувати великі обсяги даних, виявляти патерни й прогнозувати можливі кібератаки, що дозволяє випереджати загрози [10, с. 49-50].

Відтак, Польща демонструє ефективний підхід до вирішення проблем у сфері кібербезпеки, роблячи акцент на інноваціях і співпраці. Такі заходи є важливими не тільки для збереження цифрових інфраструктур, але й для захисту особистих даних громадян і розвитку економіки. Спільні зусилля держави, бізнесу та громадянського суспільства забезпечать стійкість цифрового середовища та захист інформації. Виходячи з цього, пропонуємо розглянути деякі пропозиції з покращення рівня кібербезпеки на підприємствах в Україні:

– впровадження стратегій, що поєднують технічні, організаційні та правові аспекти, створення стандартів безпеки та посилення міжнародної співпраці;

– проведення навчальних програм, тренінгів і інформаційних кампаній для підвищення обізнаності громадян та працівників;

– активне впровадження ШІ, блокчейну, біометрії й інших технологій для захисту даних і виявлення загроз;

– залучення спеціалістів до сфери кібербезпеки через освітні програми й підтримку професійного розвитку;

– регулярне тестування систем, усунення вразливостей та впровадження сучасного програмного забезпечення;

– обмін досвідом із закордонними партнерами, спільна розробка стратегій і спільна протидія кіберзагрозам;

– формування культури безпеки серед працівників через навчання та тренінги [10, с. 51-53].

Висновки

Підсумовуючи вищевикладене, можна зробити низку наступних висновків. По-перше, інформаційна безпека є ключовим елементом функціонування сучасних підприємств, адже витік чи несанкціоноване використання інформації, зокрема комерційної таємниці, може призвести до економічних втрат і погіршення конкурентних позицій.

По-друге, аналіз чинного законодавства України виявив низку прогалин, зокрема відсутність чіткого розмежування понять «конфіденційна інформація» та «комерційна таємниця», недостатню деталізацію умов правової охорони КТ, а також

відсутність механізмів обліку КТ як нематеріального активу.

По-третє, для підвищення ефективності захисту комерційної інформації слід уточнити поняття «комерційна таємниця» та розмежувати його з «конфіденційною інформацією, запровадити чіткі механізми відповідальності за порушення прав на КТ та прийняти профільний Закон «Про інформацію».

Окрім цього, Україна може значно підвищити ефективність захисту інформації, адаптувавши найкращі польські практики. Зокрема, інтегрувавши інноваційні технології (штучний інтелект, блокчейн, біометричні системи), запровадивши національні стандарти захисту інформації та сформувавши культуру безпеки через навчання працівників та підтримку підприємств у впровадженні заходів інформаційної безпеки.

Таким чином, впроваджений комплексний підхід разом із вдосконаленням законодавства та впровадженням передових практик сприятимуть посиленню захисту інформації на підприємствах України, підвищенню їх конкурентоспроможності та розвитку економіки загалом.

Література

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 13.11.2024).

2. *Кримінальний кодекс України*: Кодекс України від 05.04 2001р. № 2341-III (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text240 (дата звернення: 13.11.2024).

3. Яромій І. В., Гудима В. В. Особливості відповідальності за незаконне використання та поширення інформації з обмеженим доступом в Україні. *The 7th International scientific and practical conference "European congress of scientific achievements"* (July 15-17, 2024) Barca Academy Publishing, Barcelona, Spain. 2024. 241 p. С. 237-241. URL: https://sci-conf.com.ua/wp-content/uploads/2024/07/EUROPEAN-CONGRESS-OF-SCIENTIFIC-ACHIEVEMENTS-15-17.07.24.pdf

4. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. URL: http://zakon.rada.gov.ua/laws/ show/2939-17#Text (дата звернення: 05.03.2024).

5. Цивільний кодекс України від 16.01.2003 р. № 435-IV. URL: https://zakon3.rada.gov.ua/laws/show/435-15/paran2312#n2312 (дата звернення: 18.11.2024).

6. Господарський кодекс України від 16.01.2003 р. № 436-IV. URL: https://zakon2.rada.gov.ua/laws/show/436-15/page (дата звернення: 18.11.2024).

7. Кравченко О. М. Удосконалення організаційно-правового забезпечення охорони конфіденційної інформації та комерційної таємниці бізнесу в Україні. *Науково-практичний журнал «Екологічне право»*. Вип. 1-2. 2024. С. 21-27. URL: http://www.ecolaw.idpnan.kyiv.ua/archive/2024/1-2/1-2_2024.pdf

8. Кравченко О. М. Комерційна таємниця та конфіденційна інформація бізнесу в Україні. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів : матеріали Міжнар.наук.-практ. конф.* (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса: Фенікс, 2024. С. 670-673. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/f5a79fa8-d427-4d23-baea-0533d2445fe3/content

9. Кравченко О. М. Охорона конфіденційної інформації та комерційної таємниці в умовах воєнного стану. *Науковий вісник ДДУВС*. Спец. вип. №2. 2022. С. 476-480. URL: https://er.dduvs.edu.ua/bitstream/123456789/11577/1/70.pdf

10. Каратай М. І. Шляхи вдосконалення системи захисту інформації з обмеженим доступом в Польщі. *Наука, технології, інновації: нові підходи та актуальні дослідження. Матеріали II науково-практичної конференції.* (м. Полтава, 27-28 вересня 2024 р.). Одеса: Вид-во «Молодий вчений», 2024. С. 49-53. URL: https://molodyivchenyi.ua/omp/index.php/conference/catalog/view/114/1600/3337-1

Shebanits D.M.
Candidate of Historical Sciences,
Associate Professor of the Department of Law,
Mariupol State University
Shebanits V.F.
third-year law student
Mariupol State University

PECULIARITIES OF LEGAL REGULATION OF INFORMATION SECURITY AT THE LOCAL LEVEL OF THE ENTERPRISE

The article examines the peculiarities of legal regulation of information security at the local level of an enterprise. The article analyses the national legislation of Ukraine on the definition of the concepts of «information», «information with limited access» and «trade secret».

Restricted information includes confidential, secret and proprietary information. It is noted that information about an individual (personal data), as well as any data to which access is restricted by a private or legal entity, has a special protection status, except when it concerns public authorities. The author proves that information on the date and place of birth, education, health status, property status, religious beliefs and other personal characteristics are considered confidential.

The author considers the main problems in the field of protection of commercial information, in particular, shortcomings in the current regulatory framework that affect the effectiveness of its protection. The author proposes a number of amendments to the legislation aimed at improving the legal protection of trade secrets, in particular, clarifying its definition, distinguishing between the concepts of «confidential information» and «trade secret», and increasing liability for unlawful disclosure. The author recommends that the following types of measures should be used to ensure comprehensive protection of trade secrets and confidential business information: legal, organisational and technical.

The study also examines Poland's successful experience in the field of legal regulation of information security at the enterprise level, including the use of innovative technologies (artificial intelligence, cyber systems, blockchain technology, and the use of biometric data), the implementation of security standards, and the enhancement of data protection culture. Recommendations for the adaptation of the best Polish practices in Ukraine are proposed.

Keywords: information security, commercial secret, restricted information, legal regulation, enterprise.