

Інна Зайцева-Калаур,
кандидат юридичних наук, доцент
кафедри економічної безпеки та фінансових
розслідувань юридичного факультету
Тернопільського національного
економічного університету

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПРОЦЕДУРИ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ТА ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

Досліджено правові та організаційні аспекти охорони та захисту комерційної таємниці; виділено основні етапи процесу віднесення інформації до комерційної таємниці; проаналізовано сучасну, дієву систему охорони та захисту інформації, що є комерційно-цінним для суб'єкта господарювання.

Ключові слова: інформація, комерційна таємниця, охорона комерційної таємниці, захист комерційної таємниці, суб'єкт господарювання.

Зайцева-Калаур І.

Организационно-правовые процедуры обеспечения охраны и защиты коммерческой тайны субъекта хозяйствования

Исследованы правовые и организационные аспекты охраны и защиты коммерческой тайны; выделены основные этапы процесса отнесения информации к коммерческой тайне; проанализирована современная, действенная система охраны и защиты информации, которая является коммерчески ценной для предприятия.

Ключевые слова: информация, коммерческая тайна, охрана коммерческой тайны, защита коммерческой тайны, субъект хозяйствования.

Zaitseva-Kalaur I.

Organizational and legal procedures for protection of a commercial secret of business subsidiary

The scientific article is devoted to the study of legal and organizational aspects of the protection of commercial secrets; the main stages of the process of assigning information to commercial secrets are highlighted; modern, effective system of information protection that is commercially valuable for a business entity is analysed.

Keywords: information, commercial secret, protection of commercial secrets, business subsidiary.

Постановка проблеми. Встановлення та застосування режиму «комерційна таємниця» до інформації, що є комерційно-цінною для суб'єкта господарювання, є одним з першочергових питань забезпечення його економічної безпеки.

Аналіз останніх досліджень і публікацій. Проблемам охорони та захисту комерційної таємниці присвячені праці таких науковців: Г. Андрощук, Ю. Носік, О. Сліпачук, А. Сляднева, С. Чікін, В. Черненко та ін. Автори аналізують сучасний стан нормативно-правового регулювання даного інституту, досліджують охорону комерційної таємниці в країнах Європейського Союзу, розглядають заходи правового та організаційного характеру щодо її збереження тощо. Незважаючи на багатий науковий доробок у цій сфері, питання охорони та захисту комерційної таємниці залишаються актуальними і сьогодні. Відсутність спеціального закону про комерційну таємницю покладає на суб'єкта господарювання завдання самостійно встановлювати та застосовувати режим «комерційна таємниця» до інформації, яка є важливою та цінною для підприємства. Це надає як широкі можливості для останнього, так і вимагає великих зусиль та відповідальності при прийнятті ним рішень.

Постановка завдання. Охарактеризувати поетапно процес віднесення інформації до комерційної таємниці, дослідивши дієву систему охорони та захисту даного правового інституту.

Для того, щоб інформація зберігалася у режимі «комерційна таємниця», суб'єкт господарювання має спланувати й організувати дії правового характеру. Насамперед це – внесення відповідних положень до установчих документів.

В установчих документах з посиланням на статті 505, 506 ЦК України [1] та статті 36, 135, 155, 162 ГК України [2] передбачити право підприємства відносити інформацію, що йому належить, до комерційної

таємниці та право приймати внутрішні документи, якими визначається її склад, обсяг та порядок захисту інформації, що є конфіденційною або комерційною таємницею.

На базі вищезазначених документів підприємство планує та організовує розробку, прийняття й упровадження основних документів підприємства. Це документи, які безпосередньо забезпечують захист комерційної таємниці підприємства, та документи, які забезпечують захист комерційної таємниці підприємства при прийомі персоналу.

До документів, які безпосередньо забезпечують захист комерційної таємниці підприємства, належать:

1. Положення про організацію роботи з комерційною таємницею підприємства та іншою конфіденційною інформацією (Положення про комерційну таємницю). У положенні врегульовують заходи з організації охорони та захисту комерційної таємниці, порядок роботи з інформацією, що є комерційною таємницею, зобов'язання працівників щодо збереження комерційної таємниці, порядок розкриття інформації, що містить комерційну таємницю, відповідальність за порушення пов'язані з комерційною таємницею та ін.

2. Перелік відомостей які відносяться до інформації з обмеженим доступом.

3. Положення щодо спеціального діловодства для документів, які містять інформацію з обмеженим доступом.

4. Положення про інформаційну безпеку при роботі з матеріальними носіями, що містять комерційну таємницю.

5. Інструкція про порядок виконання запитів, що надходять від правоохоронних органів, судів та інших державних установ.

6. Інструкція про проведення перевірок щодо дотримання норм інформаційної безпеки при роботі з матеріальними носіями, що містять комерційну таємницю.

Документи, які забезпечують захист комерційної таємниці підприємства при прийомі персоналу складають:

1. Трудовий договір (контракт), посадові інструкції, де прописуються питання, що стосуються роботи з комерційною таємницею та відповідальності за порушення права на використання комерційної таємниці у тому числі після звільнення працівника з посади;

2. Зобов'язання працівників підприємства щодо збереження інформації з обмеженим доступом.

3. Положення про нерозголошення комерційної таємниці підприємства та інші положення, правила, зобов'язання, підпис працівника на яких є підставою для захисту підприємством своїх інтересів.

4. Опис вимог щодо угод з третіми сторонами стосовно доступу, оброблення, передавання або управління інформацією підприємства.

Процедура віднесення інформації до комерційної таємниці – це складне багатоаспектне явище, що передбачає застосування заходів правового та організаційного характеру щодо охорони та захисту комерційної таємниці суб'єкта господарювання.

Процедура віднесення інформації до комерційної таємниці передбачає декілька чітко визначених етапів.

На першому етапі відбувається актуалізація певної інформації, яка потребує захисту у статусі «комерційна таємниця». Далі необхідне ретельне вивчення обраної інформації як секретної і складання робочого варіанту Положення про комерційну таємницю та Переліку відомостей, що становлять комерційну таємницю підприємства. Відповідний перелік конфіденційної інформації може бути сформований за такими напрямками: кадрова політика підприємства, фінансова діяльність підприємства, цінова політика підприємства, збутова діяльність підприємства, забезпечення безпеки підприємства.

Для виконання такого завдання керівник підприємства призначає відповідальну особу за режим секретності щодо конфіденційної інформації, та комерційної таємниці та комісію з питань комерційної таємниці. Формувати перелік відомостей, що становлять комерційну таємницю підприємства потрібно із залученням фахівців профільних підрозділів за кожним із напрямків. Тоді існуватиме можливість у разі виникнення спірних питань щодо належності тієї чи іншої інформації до категорії «комерційна таємниця» залучати в якості експертів фахівців таких підрозділів. Саме такі особи навіть за наявності в інформації основних ознак комерційної таємниці, можуть визначати у кожному конкретному випадку наскільки небезпечним є її розголошення.

У вітчизняному законодавстві відсутні вимоги та регламентації, що стосуються структури та змісту Положення про комерційну таємницю. Але, незважаючи на відмінності в сферах діяльності, структурах,

кількості працівників і керівного складу підприємств, дослідники формують деякі загальні рекомендації щодо його змісту:

1. Загальні положення.
2. Визначення переліку відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства.
3. Порядок захисту комерційної таємниці та конфіденційної інформації підприємства.
4. Порядок видачі працівниками документів, відомостей, передання інформації, що становить комерційну таємницю та конфіденційну інформацію підприємства контрагентам, клієнтам і державним органам.
5. Процедура наймання (звільнення) працівника/співробітника підприємства.
6. Відповідальність за розголошення відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства.
7. Прикінцеві положення.
8. Додатки.

У розділі 2 цього положення перелік відомостей доцільно охарактеризувати загальними поняттями, а для їх докладного визначення посилатися на Перелік відомостей, що становлять комерційну таємницю підприємства [3, с. 57].

У Додатках можуть бути наведені типові документи, що стосуються питань комерційної таємниці, наприклад: «Службова записка з пропозицією віднесення інформації до комерційної таємниці», «Зобов'язання працівника щодо нерозголошення комерційної таємниці та конфіденційної інформації», «Угоди про конфіденційність з відвідувачами підприємства» тощо.

Другий етап – керівник підприємства видає наказ про затвердження та впровадження на підприємстві Положення про комерційну таємницю підприємства та порядку ознайомлення з ним.

Наступний етап – комісія формує Перелік відомостей, що становлять комерційну таємницю підприємства. На цьому етапі передбачено встановлення терміну засекречування інформації. За періодом існування комерційну таємницю можна поділити на короткострокову таємну інформацію та довгострокову таємну інформацію. Як правило, часовий відлік засекречення короткострокової інформації – до 6 місяців, довгострокової – від 6 місяців і довше.

Четвертий етап передбачає затвердження Переліку відомостей, що становлять комерційну таємницю підприємства і складається з двох стадій:

1) присвоєння за кожним видом інформації відповідного грифу секретності. «Особливо секретно» – відомості, оволодіння якими негативно позначиться на усій діяльності підприємства, та «секретно» – відомості, оволодіння якими може спричинити шкоду за окремим напрямком діяльності підприємства;

2) затвердження та підписання керівником підприємства Переліку відомостей, що становлять комерційну таємницю. Усім відомостям, що перелічені у вказаному документі, офіційно наданий статус комерційної таємниці підприємства [3, с. 82].

Перелік відомостей, що становлять комерційну таємницю, має періодично корегуватися. Відомості, які втратили своє значення, стали загальнодоступними чи втратили комерційну цінність тощо, мають вилучатися, а вноситись нові, що потребують захисту.

П'ятий етап – це встановлення матеріальних носіїв інформації, що становлять комерційну таємницю підприємства. Носіями конфіденційної інформації можуть виступати людина, документи, продукція, офіційні засоби інформації, технічні засоби. При цьому людина є сполучною ланкою між усіма іншими носіями комерційної таємниці, оскільки розробляє і затверджує документацію; є виробником продукції; готує матеріали для видання, оголошення та показу в засобах масової інформації; працює за комп'ютерами, друкарською машинкою, з телефонними апаратами, факсами та іншими технічними засобами. За кожним видом конфіденційної інформації вирішується, в якій якості вона буде існувати. Комерційна таємниця може мати декілька носіїв, що треба враховувати при визначенні способів її захисту, а також тих осіб, які нею володіють.

На *шостому етапі* визначаються конкретні особи, що володіють конфіденційною інформацією, або можуть мати доступ до неї.

Розголошення комерційної таємниці здебільшого пов'язано з тим, що керівник підприємства недостатню увагу приділяє вивченню особистості особи, допущеної до роботи з комерційною таємницею.

Надаючи право доступу до інформації з грифом «комерційна таємниця» керівник повинен:

– визначити потребу співробітника в конфіденційній інформації при виконанні ним службових обов'язків;

- здійснити перевірку співробітника у зв'язку з допуском до комерційної таємниці;
- ознайомити співробітника з мірою відповідальності за порушення законодавства про незаконне збирання, поширення та використання комерційної таємниці;
- оформити письмове зобов'язання працівника про нерозголошення комерційної таємниці, що буде йому довірена.

При перевірці співробітника на допуск необхідно брати до уваги таке:

- досягнення ним дієздатного віку 18 років;
- наявність судимості за злочини, пов'язані з розголошенням державної чи комерційної таємниці, а також у фінансово-господарській сфері;
- наявність психічних захворювань, схильність до вживання алкоголю та наркотиків;
- факти надання в процесі підготовки матеріалів для оформлення допуску недостовірних відомостей про себе;

– наявність підозрілих зв'язків із співробітниками підприємств-конкурентів [4, с. 61].

Сьомий етап – вибір способів захисту комерційної таємниці на підприємстві.

Щоб розробити дійову систему захисту комерційної таємниці, необхідно вивчити всі можливі шляхи незаконного оволодіння нею.

Найбільш частими протиправними діями, що дозволяють оволодіти конфіденційною інформацією підприємства, є:

- підкуп співробітників підприємства, що володіють або мають доступ до конфіденційної інформації;
- підслуховування телефонних переговорів;
- дистанційне звукове прослуховування;
- копіювання носіїв інформації;
- розшифровка радіовипромінювання комп'ютерів, факсів, телетайпів;
- візуальний та слуховий контроль приміщення;
- розміщення мікропередавачів в приміщеннях і автомобілях;
- використання шпигунів-професіоналів;
- переманювання працівників конкурента;
- засилання агентів до службовців або фахівців конкурента.

Незаконному оволодінню комерційною таємницею сприяють низький рівень контролю за досягненням заходів безпеки, незадовільні умови праці, неефективна система заохочування працівників, економія на технічних засобах захисту, плінність кадрів, недосконала система праці тощо.

Дієвими способами захисту є:

1. Створення режимно-секретного підрозділу з функціями підтримки і контролю за дотриманням встановленого режиму секретності, діяльність якого визначається відповідними інструкціями, положеннями чи наказами.

Як основні функції режимно-секретного підрозділу доцільно визначити такі :

- розробка, впровадження та забезпечення функціонування дозвільної системи доступу до інформації;
- розробка й упровадження маркування документації та носіїв інформації, віднесеної до комерційної таємниці та дій щодо їх збереження;
- розробка та впровадження секретного діловодства;
- планування й організація дій технічного характеру щодо охорони носіїв інформації та інформаційних мереж;
- дії, що спрямовані на виявлення витоку інформації, джерел такого витоку та локалізації негативних наслідків тощо;
- планування, організація та здійснення дій психологічного характеру: інструктаж персоналу, роз'яснювальна робота, перевірки та ін.;
- контроль, аналіз і надання рекомендацій з поліпшення.

У разі доцільності на режимно-секретний підрозділ можуть бути покладені функції забезпечення захисту майна та персоналу підприємства [4, с. 60].

2. На підприємстві потрібно забезпечити жорсткий режим доступу до інформації конфіденційного характеру. Це передбачає:

- пропускний режим до приміщень, де зберігаються відомості, що становлять комерційну таємницю;

– ретельний підбір кадрів, що працюють з конфіденційною інформацією. Відомо, що чим менше людей мають доступ до таких відомостей, тим більше ймовірність зберегти їх в таємниці. Отже, необхідне обмежене коло осіб, що можуть мати доступ до тієї чи іншої секретної інформації.

У разі звільнення співробітника, який був допущений до комерційної таємниці, ним підписується попередження-зобов'язання про нерозголошення відомостей, які стали йому доступні в процесі роботи на підприємстві. Мета відбору такого попередження-зобов'язання про нерозголошення – профілактика розголошення співробітником, що звільняється, комерційної таємниці та створення юридичних підстав для відшкодування збитків у разі розголошення таких відомостей.

3. Введення відповідного маркування носіїв з конфіденційною інформацією.

Відомості, що становлять комерційну таємницю, можуть бути диференційовані підприємством за ступенем важливості з присвоєнням відповідного грифу.

Наприклад:

1. Для конфіденційної інформації – гриф «Для службового користування» або «ДСК».

2. На підприємстві, як правило, встановлюється триступенева система важливості комерційної таємниці, яка позначається такими обмежувальними грифами:

«Комерційна таємниця – особливо важливо» («КТ-ОВ») «Комерційна таємниця – суворо конфіденційно» («КТ-СК») «Комерційна таємниця – конфіденційно» («КТ-К»).

Вищезазначене маркування наноситься на носії з інформацією, а в разі зберігання інформації в електронному вигляді, гриф має передувати відкриттю безпосередньо інформації.

4. Забезпечення збереженості документів, що містять комерційну таємницю.

Документи, що містять комерційну таємницю, потребують особливого режиму зберігання. Їх треба зберігати у службових приміщеннях у шафах (сейфах), сховищах, що надійно замикаються й опечатуються.

Документи, видані для роботи працівникам-виконавцям, повертають до служби діловодства (секретарю) або в архів того самого дня. У деяких випадках з дозволу керівника служби діловодства чи особи, відповідальної за архів підприємства, документи можуть зберігатися у працівника протягом терміну, потрібного йому для виконання завдання, за умови цілковитого забезпечення їх збереженості. При цьому документи не дозволяється залишати на столі, закінчивши роботу, їх треба покласти до шафи, що замикається, або сейфа [5, с. 44].

Документи, що містять комерційну таємницю, не дозволяється виносити за межі підприємства. Лише за умови потреби їх погодження з фахівцями з інших підприємств, що територіально розташовані в одному населеному пункті, керівник підприємства може видати працівникам письмовий дозвіл на вивезення цих документів за межі підприємства.

Працівникам, відрядженим з виробничою метою до інших населених пунктів, забороняється мати при собі документи, що містять комерційну таємницю підприємства. Такі документи заздалегідь пересилають за призначенням.

Наявність документів, що містять комерційну таємницю, щорічно переглядає комісія, спеціально призначена наказом керівника підприємства. До складу комісії входять особи, яким доручено облік і зберігання цих документів, а також працівники режимно-секретного підрозділу підприємства.

В архівах і бібліотеках, де зберігається значна кількість документів із грифом обмеженого доступу, перевірка їх наявності може проводитися *один раз на n'ять років* [5, с. 45].

Результати перевірок завжди оформляють протоколом. Виявивши у ході перевірки втрату документів з грифом «КТ» або розголошення відомостей, що містять комерційну таємницю, про це терміново доповідають керівництву підприємства, керівникам режимно-секретного відділу і служби діловодства, а також службі безпеки підприємства, якщо така на підприємстві є.

Для розслідування факту втрати документів або розголошення інформації, що міститься в них, наказом керівника підприємства призначається комісія, висновок якої, незалежно від результатів, затверджує керівник підприємства.

5. *Застосування технічних засобів захисту комерційної таємниці.* Технічні заходи захисту базуються на використанні різних електронних пристроїв і спеціальних програм, що входять до складу системи обробки інформації та виконують функції захисту. Наприклад, пошукові прилади, прилади охорони провідних комунікацій, програмне забезпечення, апаратура для виявлення диктофонів, системи акустичного і віброакустичного шумлення, скануючі засоби, засоби виявлення каналів витоку інформації, встановлені спеціального обладнання для спостереження за приміщеннями організації тощо.

6. Підвищення лояльності працівників включають правильно організовану роботу з працівниками підприємства (кадрову політику) і застосування матеріальних та моральних стимулів. Одним із важливих завдань керівника потрібно вважати вірно організований добір співробітників, створення сприятливого соціально-психологічного клімату всередині організації, формування «професійного патріотизму». Завдяки вирішенню питань соціального захисту працівників, організації відпочинку та дозвілля, медичного обслуговування керівник створює в колективі таке сприятливе середовище, що зводить до мінімуму ймовірність усвідомленого заподіяння шкоди підприємству його ж працівниками. Не варто нехтувати і впровадженням системи матеріальних винагород, створенням можливостей для професійного зростання та для участі персоналу в прийнятті рішень. Від умов роботи, що створює керівництво для своїх підлеглих, залежить стан психологічної атмосфери в колективі, тому отримуючи максимальне задоволення від своєї роботи, працівник здатен виконувати свої обов'язки найбільш плідно. Розвиток у них зацікавленості в успіхах підприємства має бути спрямований на те, щоб звести до мінімуму плінність кадрів і разом з тим – втрату інтелектуального потенціалу підприємства і можливість розголошення конфіденційної інформації.

Таким чином, суб'єкт господарювання, який має намір скористатися своїм правом на комерційну таємницю, повинен самостійно спланувати і організувати усі дії правового та організаційного характеру, щоб забезпечити можливість використовувати та охороняти інформацію в режимі «комерційна таємниця». Ефективність її захисту залежатиме від докладених зусиль з боку власника-розпорядника такої інформації. Втім, враховуючи реалії сьогодення, особливу увагу слід приділити питанням, які за даними наукових досліджень більшою мірою впливають на захист комерційно-цінної інформації. По-перше, – це невідпинний розвиток інформаційних технологій, що дають можливість швидкого копіювання та поширення цінної інформації. Часто такі дії відбуваються без дозволу на те власника. Тому важливо особливу увагу приділити застосуванню технічних засобів захисту комерційної таємниці, використовуючи надійні інформаційні системи, ліцензійне програмне забезпечення тощо. По-друге, варто більше уваги приділити питанням підвищення лояльності працівників. Вжиття відповідних заходів дасть змогу покращити продуктивність, закріпити кадри, зменшити їх плінність і завдяки цьому мінімізувати ризик розголошення комерційної таємниці.

Список використаних джерел

1. Цивільний кодекс України від 16 січ. 2003 р. №435 // *Офіц. вісник України*, 2003. – № 11. – Ст. 461.
2. Господарський кодекс України : за станом на 16 січня 2003 р. // *Відомості Верховної Ради України (ВВР)*. – Офіц. вид. – К. : Парлам. вид-во, 2003. – 192 с.
3. Локотецька О. Система захисту комерційної таємниці підприємства / О. Локотецька // *Бізнес Інформ*. – 2011. – №12. С. – 81–83.
4. Чікін С. Управління комерційною таємницею на підприємстві: дії організаційного, технічного та психологічного характеру / С. Чікін, В. Черненко // *Теорія і практика інтелектуальної власності*. – 2011. – № 5. – С. 56–64.
5. Загорецька О. Особливості роботи з документами, що містять комерційну таємницю підприємства / О. Загорецька // *Довідник кадровика*, 2011. – № 09 (111). – С. 40–46.

References

1. *Tsyvilnyi kodeks Ukrainy [The Civil Code of Ukraine].* (2003, January 16). *Offic. Bulletin of Ukraine [in Ukrainian]*.
2. *Hospodarskyi kodeks Ukrainy [Commercial Code Ukraine].* (2003, January 16). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine*. Kyiv: *Parlam. vyd-vo [in Ukrainian]*.
3. *Lokotetska, O. (2011). Systema zakhystu komertsyynoyi tayemnytsi pidpryyemstva [The system of protection of commercial secret of the enterprise]. Biznes Inform – Business Inform, 12, 81-83 [in Ukrainian].*
4. *Chikin, S. & Chernenko V. (2011). Upravlinnya komertsyynoyu tayemnytseyu na pidpryyemstvi: diyi orhanizatsiynoho, tekhnichnoho ta psykholohichnoho kharakteru [Management of commercial secrets in the enterprise: actions of organizational, technical and psychological character]. Teoriya i praktyka intelektualnoyi vlasnosti – The theory and practice of intellectual property, 5, 56-64 [in Ukrainian].*
5. *Zahoretska, O. (2011). Osoblyvosti roboty z dokumentamy, shcho mistyat komertsyynu tayemnytsyu pidpryyemstva [Features of work with documents containing the commercial secret of the enterprise]. Dovidnyk kadrovyka – Handbook of HR, 9, 40-46 [in Ukrainian].*

Стаття надійшла до редакції 2.10.2018.