Міністерство освіти і науки України
Національний університет водного господарства та природокористування
Інститут економіки та менеджменту
Кафедра фінансів і економіки природокористування

06-03-158

Управління захистом комерційної таємниці на підприємстві

КОНСПЕКТ ЛЕКЦІЙ

для здобувачів вищої освіти другого (магістерського) рівня
за спеціальністю 073 «Менеджмент»
(в т.ч. зі скороченим терміном навчання)

Рекомендовано методичною комісією зі спеціальності 072 «Фінанси, банківська справа та страхування»
Протокол № 6 від 30 січня 2018 р.

Рівне – 2018

Конспект лекцій з навчальної дисципліни «Управління захистом комерційної таємниці на підприємстві» для здобувачів вищої освіти другого (магістерського) рівня зі спеціальності 073 «Менеджмент» (в т.ч. зі скороченим терміном навчання) / Н. М. Білоус. – Рівне : НУВГП, 2018. – 37 с.

Укладач: Н. М. Білоус**,** доцент кафедри фінансів і економіки природокористування, к.е.н.

Відповідальний за випуск: Н. М. Білоус, к.е.н., доцент кафедри фінансів і економіки природокористування.

ЗМІСТ

Вступ

Навчальними планами спеціальності «Менеджмент» зі спеціалізації «Управління фінансово-економічною безпекою» освітньо-кваліфікаційного рівня магістр передбачено вивчення дисципліни «Управління захистом комерційної таємниці на підприємстві».

Сьогодні, в Україні посилюється практичний інтерес до комерційної таємниці та інших, пов'язаних з нею понять, як одного з ефективних заходів інформаційної безпеки.

Комерційна таємниця виконує важливу функцію в забезпеченні конкурентоздатної діяльності, тому правовласник, безумовно, має право на захист її від неправомірного використання.

Мета вивчення навчальної дисципліни є підготовка фахівців з управління фінансовою безпекою, здатних активно користуватися правовими та управлінськими знаннями для ефективного захисту комерційної таємниці на підприємстві.

Дисципліна «Управління захистом комерційної таємниці на підприємстві» посідає важливе місце серед навчальних предметів, які формують фахівця фінансового профілю.

Завдання дисципліни:

– розвиток у майбутніх фахівців з управління фінансовою безпекою здібностей, які забезпечують захист комерційної таємниці на підприємстві правовими засобами;

– опанувати поняття та ознаки комерційної таємниці;

– засвоїти права та обов'язки суб'єктів права власності на комерційну таємницю;

– засвоїти систему нормативно-правових актів, які містять норми щодо управління захистом комерційної таємниці на підприємстві;

– знати способи і форми захисту комерційної таємниці;

– орієнтуватися в особливостях цивільно-правового захисту комерційної таємниці на підприємстві.

Предметом дисципліни є суспільні відносини, що складаються в сфері захисту комерційної таємниці.

ТЕМА 1
СУТНІСТЬ, ОЗНАКИ ТА ВИДИ ІНФОРМАЦІЇ

План

1.1. Основні види інформації.
1.2. Основні умови віднесення інформації до комерційної таємниці.
1.3. Цінність інформації, що становить комерційну таємницю.

1.1. Основні види інформації

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

Захист інформації – сукупність заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Згідно закону України "Про інформацію" (ст. 20) інформація поділяється на **відкриту та інформацію з обмеженим доступом**.

*Інформацією з обмеженим доступом є **конфіденційна**, **таємна** та **службова** інформація.*

До інформації з обмеженим доступом **не можуть бути віднесені** такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;
2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;
3) про стан здоров'я населення, його життєвий рівень, включаючи харчування,одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;
4) про факти порушення прав і свобод людини і громадянина;
5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;
6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Різновидами конфіденціальної інформації є:

Особиста інформація – інформація про особу (в тому числі дитину), її особисте життя.

Службова інформація – інформація про фінансову діяльність, господарську діяльність (*яка не пов'язана з секретами виробництва*, введенням новацій та ноу-хау, розробкою стратегії розвитку, веденням переговорів, розробкою та впровадженням нових технологій) та внутрівідомчу службову діяльність установи, її посадових, службових осіб та кореспонденцію (*доповідні*

записки, листування між підрозділами тощо), які пов'язані з процесом прийняття рішень та передують їх прийняттю.

Різновидами відкритої інформації є:

Офіційна інформація – інформація про офіційну діяльність установи, її посадових, службових осіб та офіційні документи. Офіційна інформація може бути віднесена до публічної інформації та конфіденційної інформації.

Публічна інформація – інформація яка вільно збирається, отримується, зберігається, використовується та поширюється.

Комерційною таємницею є 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.***

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.*

Усі види інформації, які можуть вважатися комерційною таємницею, умовно можна розділити на дві групи:

- технічна інформація
- комерційна інформація.

До першої групи належать незапатентовані науково-технічні розробки, бази даних та інші комп'ютерні програми, створені підприємством, усі види «ноу-хау», технічні проекти, промислові зразки, незапатентовані товарні знаки.

До другої групи віднесено:

- умови контрактів,
- дані про постачальників і покупців,
- інформація про переговори,
- маркетингові дослідження,
- дані про розрахунок відпускних цін,
- розміри знижок тощо.

Інформація характеризується різноманітними формами існування:

Державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких **може завдати шкоди національній безпеці України** та які визнані державною таємницею і підлягають охороні державою.

Ознакою державної таємниці є гриф секретності – реквізит матеріального носія інформації, що засвідчує ступінь її секретності.

Віднесення інформації до державної таємниці, зміни ступеня її секретності та розсекречування здійснює відповідно до вимог законодавства державний експерт з питань таємниці.

Комерційна таємниця – це право підприємства, компанії, фірми, банку на зберігання в таємниці документів, даних, що відображають їх діяльність

(більш детально у наступних розділах).

Службовими таємницями, зокрема, є:

✓ Зміст плану контрольно-ревізійної роботи та терміну до часу повідомлення об'єкту контролю про початок проведення перевірки;

✓ Факти виявлених під час проведення ревізій і перевірок порушень, зловживань до їх повного документального підтвердження й закріплення в актах, а також заплановані з цією метою зустрічні перевірки, раптові інвентаризації готівки і майна, контрольні обміри та інші ревізійні дії;

✓ Надані правоохоронними органами оперативні та інші відомості щодо діяльності підприємств, установ і організацій (вчинених порушень, зловживань посадових осіб, дані посадовими особами письмові пояснення, протоколи допитів з конкретних питань тощо);

✓ інформація про оперативну й слідчу роботу органів прокуратури, МВС, СБУ, їх органів дізнання в тих випадках, коли її розголошення може зашкодити слідству, порушити право людини на справедливий та об'єктивний розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;

✓ конкретні пояснення посадових осіб щодо виявлених фактів зловживання, крадіжок тощо;

✓ відомості, які містяться у зверненнях громадян щодо їхнього (чи інших громадян) особистого життя, та інша інформація, що зачіпає (порушує) їх права та законні інтереси;

✓ документи, що становлять внутрішньовідомчу службову кореспонденцію (відповідні записки, листування між підрозділами, матеріали колегій тощо), якщо вони безпосередньо пов'язані з розробкою лояльності Державної контрольно-ревізійної служби, процесом прийняття рішень і передують їх прийняттю;

✓ інформація банківських і фінансових установ підготовлена на запити органів Державної контрольно-ревізійної служби;

✓ чернетки матеріалів ревізії та перевірок.

Розголошення посадовою особою державної чи службової таємниці є порушенням трудових обов'язків, за яке передбачене звільнення з роботи як за одноразове грубе їх порушення згідно з кодексом законів про працю України.

1.2. Основні умови віднесення інформації до комерційної таємниці

Основними умовами віднесення інформації до комерційної таємниці є:

- справжня або потенційна комерційна важливість інформації;
- відсутність вільного доступу до інформації на законних підставах;
- вжиття заходів володарем інформації для її охорони та збереження конфіденційності.

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві створюється спеціальна комісія, яка займається групуванням і уточненням інформації для цього переліку.

Чисельність такої комісії не повинна перевищувати чотирьох-п'яти осіб. Створюється вона з найбільш кваліфікованих і компетентних фахівців основних підрозділів і представників служби безпеки підприємства, ознайомлених як з діяльністю підприємства в цілому, так і з роботою окремих підрозділів.

До її складу включають:

- фахівця, який володіє фінансовими питаннями, кон'юнктурою ринку та інформацією щодо діяльності конкуруючих фірм (як правило, це фінансовий менеджер);
- фахівця, який досконало знає систему організації роботи підприємства, її особливості;
- фахівця з питань зв'язків з іншими підприємствами, а також з укладення контрактів і договорів;
- фахівця, який володіє всіма відомостями про продукцію, що випускається, її технологічний цикл і виробництво, про проходження усіх видів інформації (усної, документальної, у вигляді зразків, вузлів, блоків, готової продукції).

Якщо підприємство є досить великим або виготовлена продукція має різнорідний характер, можна створити кілька таких груп: одну – головну, з метою координації та узагальнення результатів роботи, інші – залежно від необхідності по кожній окремій ділянці.

Отже, перед групою експертів необхідно поставити комплекс питань у такій послідовності:

а) виділити всі види діяльності підприємства, що приносять прибуток на даний момент;

б) на основі наявних даних про ринок збуту оцінити, чи перевищує рівень прибутку для даного виду діяльності аналогічні показники на інших підприємствах;

в) визначити ймовірну перспективу рентабельності цієї діяльності.

Якщо з економічної точки зору зазначений вид діяльності відповідає цілям підприємства і на даний момент, і в перспективі, а прибуток є вищим, аніж у конкуруючих фірм, то експерти повинні визначити, що саме в даному виді діяльності дозволяє отримувати прибуток. Відповідь на це питання і буде комерційною таємницею підприємства.

Так, для відомостей наукового характеру – це:

- ідеї, винаходи, відкриття;
- окремі формули;
- нові технічні проекти;
- нові методи організації праці та виробництва;
- програмне забезпечення;
- результати наукових досліджень.

Для відомостей технологічного характеру:

- конструкторська документація, креслення, схеми, записи;
- описи технологічних іспитів;

- «ноу-хау»;
- точні знання конструкційних характеристик виробів та оптимальних параметрів розроблювальних технологічних процесів (розміри, обсяги, конфігурація, процентний зміст компонентів, температура, тиск, час тощо);
- відомості про матеріали, з яких виготовлені окремі деталі, умови експериментів, обладнання та устаткування, на якому вони проводилися і т. д.;
- окремі нові або унікальні вимірювальні комплекси, прилади, верстати й устаткування, що використовуються на підприємстві.

Для відомостей ділового характеру:

- відомості про укладені або заплановані контракти;
- дані про постачальників та клієнтів;
- огляди ринку, маркетингові дослідження;
- інформація про конфіденційні переговори;
- калькуляція витрат виробництва підприємства, структури цін, рівень прибутку;
- плани розвитку підприємства та його інвестицій.

1.3. Цінність інформації, що становить комерційну таємницю

Визнання інформації комерційною таємницею дозволяє:

1) забезпечити охорону об'єктів виключних прав (результатів інтелектуальної діяльності), які потребують передбаченої законодавством реєстрації, до проведення такої реєстрації. Так, отримання патенту є достатньо тривалим процесом, у ході якого існує необхідність зберегти конфіденційну інформацію у таємниці до того моменту як на неї буде поширено патентну охорону, а також ту інформацію, яка не охоплюється патентним захистом;

2) забезпечити правову охорону тих продуктів інтелектуальної діяльності, які мають комерційну цінність, але не можуть у силу об'єктивних причин отримати охорону відповідно до законодавства про промислову власність або авторські і суміжні права. Деякі такі продукти взагалі є не патентоспроможними, оскільки не мають новизни винаходу (наприклад, списки клієнтів), але мають комерційну цінність і тому можуть отримати охорону в рамках режиму комерційної таємниці;

3) обрати простіший та менш витратний (порівняно, наприклад, із захистом об'єктів промислової власності) спосіб охорони комерційно цінних результатів інтелектуальної діяльності шляхом поширення на відповідну інформацію режиму комерційної таємниці;

4) забезпечити безстрокову охорону конфіденційної інформації. Будь-який патентний режим надає обмежений у часі захист, по завершенні якого будь-хто може використовувати запатентовану інформацію за своїм бажанням. Тоді як охорона комерційної таємниці триває настільки довго, наскільки зберігаються умови існування режиму комерційної таємниці, хоча б і вічно.

ТЕМА 2
СУТНІСТЬ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

План

2.1. Поняття комерційної таємниці.

2.2. Основні ознаки комерційної таємниці.

2.3. Комерційна таємниця в умовах розвитку інформаційної економіки.

Комерційна таємниця – це навмисно приховувані з комерційних міркувань інтереси і відомості про різні сторони виробничо-господарської, управлінської, науково-технічної, фінансової діяльності фірми, охорона яких обумовлена інтересами конкуренції і можливими загрозами економічної безпеки фірми. Формою комерційної таємниці є комерційні секрети або відомості, оформлені у вигляді документів, схем, виробів, які належать до комерційної таємниці, і підлягають захисту з боку служби безпеки.

Віднесення тих чи інших відомостей до комерційної таємниці повинна відповідати таким вимогам:

- їх відкрите використання може заподіяти шкоду;
- фірма може забезпечити збереження їх конфіденційності;
- ці відомості потребують захисту, оскільки вони не є державною таємницею і не захищені патентом.
- їх приховування не завдає шкоди суспільству.

Сутність поняття "комерційної таємниці" міститься в декількох наступних положеннях, або ознаках:

1) це будь-яка ділова інформація, що має дійсну або потенційну цінність для підприємства з комерційних причин, розголошення якої може завдати шкоди підприємству;

2) в Законі України " Про підприємництво в Україні" від 27.03.91р. у ст. 30 визначено поняття "комерційної таємниці підприємства;

3) "під комерційною таємницею підприємства розуміються відомості, пов'язані з виробництвом, технологічною інформацією, управлінням фінансами та іншою діяльністю підприємства, які не являються державною таємницею, розголошення (передача), яких може завдати шкоди його інтересам".

Комерційна таємниця – *це виробнича, науково-технічна, управлінська, фінансова та інша документована інформація, яку використовують для досягнення комерційних цілей (одержання прибутку, запобігання втратам, одержання добросовісної переваги над конкурентами), яку підприємець вважає конфіденційною*.

Аналіз законодавчого визначення комерційної таємниці дозволяє сформулювати її ознаки, що є необхідними умовами охороноздатності інформації **як комерційної таємниці:**

1) інформація, що становить комерційну таємницю, є таємною, тобто вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з цим видом інформації;

2) така інформація повинна мати комерційну цінність для її володільця чи для інших осіб;

3) особа, яка законно контролює інформацію, повинна вживати адекватних заходів щодо збереження її секретності.

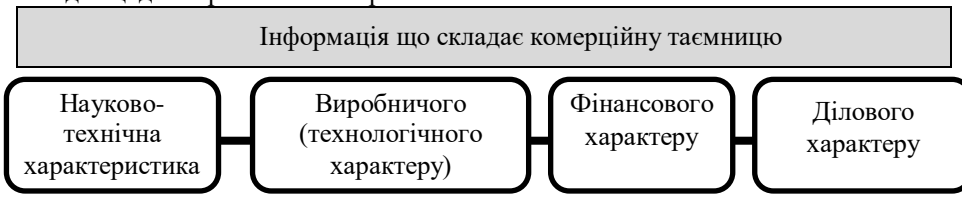

Рисунок 2.1 – Класифікація відомостей, що становлять комерційну таємницю

Отже, ***до комерційної таємниці відноситься така інформація:***

1. ***Ділова інформація***:

- фінансові відомості;
- дані про ціну (собівартість) продукції, послуг, технології;
- ділові плани і плани виробництва нової продукції;
- списки клієнтів і продавців, контакти, преференції та плани;
- інформація про маркетинг;
- договори, пропозиції, квоти;

списки персоналу, організаційні схеми та інформація про співробітників тощо.

2. ***Технічна інформація***:

- науково-дослідні проекти;
- конструкторські розробки з виробництва продукції та її технічні параметри;
- заявки на патенти;
- дизайн, ефективність і можливості виробничих методів, обладнання і систем;
- інформаційний процес;
- програмне забезпечення ЕОМ тощо.

Відомості (їх склад і обсяг), що становлять комерційну таємницю, порядок їх захисту визначає керівник підприємства.

Отже, відомості, які можуть бути віднесені до комерційної таємниці, підприємства, повинні мати такі **ознаки:**

- не містити державної таємниці;
- не наносити шкоди інтересам суспільства;
- відноситись до виробничої діяльності підприємства;
- мати дієву або потенційну комерційну цінність та створювати переваги в конкурентній боротьбі;
- мати обмеження в доступі тощо.

2.2. Основні ознаки комерційної таємниці

Ознаки комерційної таємниці можна поділити на кілька груп:

- ті, що стосуються властивостей самого об'єкту;
- ті, що відносяться до умов його правової охорони та інші.

Розглянемо **першу групу** ознак.

1) *Нематеріальність.*

По-перше, комерційній таємниці властиві всі ознаки нематеріального об'єкту – можливість одночасного використання необмеженим колом осіб, відсутність фізичної амортизації тощо.

По-друге, має значення зміст, сутність нематеріального об'єкту, тобто самі відомості, які становлять комерційну таємницю, а не форма їх зовнішнього представлення (на відміну від авторського права).

2) *Результат інтелектуальної діяльності*: від інформації, що становить комерційну таємницю, не вимагається, щоб вона являла собою обов'язково результат творчої діяльності (остання є різновидом інтелектуальної діяльності та передбачає створення якісно нового об'єкту)..

3) *Конфіденційність інформації, що становить комерційну таємницю*: Інформація, на яку правомірно поширено режим комерційної таємниці, є різновидом конфіденційної інформації.

До **другої групи** ознак відносять ознаки комерційної таємниці, що властиві їй в силу сутності об'єкту, обумовлюють особливі умови надання об'єкту правової охорони.

Цими умовами є: відсутність загальновідомості, відсутність загальнодоступності, оборотоздатність, відсутність потреби реєстрації об'єкту.

1) *Відсутність загальновідомості полягає в тому*, що інформацією володіє обмежене коло осіб, хоча й не обов'язково одна особа.

2) *Розвиває попередню умову ознака відсутності загальнодоступності інформації, яка становить комерційну таємницю*.

3) Оборотоздатність об'єкту передбачає його комерційну цінність, тобто можливість отримання економічної вигоди від введення його в оборот.

4) *Інформація, яка становить комерційну таємницю,* не потребує офіційного визнання її охороноздатності, реєстрації чи дотримання інших формальних процедур для поширення на неї правової охорони.

До **третьої групи** ознак комерційної таємниці можна віднести необмеженість строку її захисту.

Розглянемо юридичні ознаки комерційної таємниці, без наявності яких такі відомості не можуть складати секрет підприємства.

1. Інформація може складати комерційну таємницю в тому випадку, якщо вона в цілому або у визначеній формі і сукупності її складових є невідомою і не є легкодоступною для осіб, що звичайно мають справу із суміжними видами інформації.

2. Інформація, що може складати комерційну таємницю, повинна мати комерційну цінність, тобто визначену або потенційну ринкову вартість.

3. Комерційна таємниця – це склад і обсяг відомостей, що визначений керівником підприємства (іншого суб'єкта підприємництва).

4. Відомостями, що складають комерційну таємницю, не можуть бути відомості, які складають державну таємницю.

5. Відомості, що складають комерційну таємницю, не повинні бути об'єктами авторських і патентних прав (подібні об'єкти охороняються Законами України «Про охорону прав на винаходи і корисні моделі», «Про авторське право і суміжні права», «Про охорону прав на промислові зразки», «Про охорону прав на знаки для товарів і послуг» і т.д.).

6. При визначенні складу й обсягу комерційної таємниці, необхідно виключати відомості, передбачені в постанові Кабінету Міністрів України від 09.08.1993 р. № 611 «Про перелік відомостей, що не складають комерційної таємниці».

7. Власник інформації повинен вживати належних заходів по охороні інформації, визначеної як комерційна таємниця підприємства.

8. Термін правової охорони комерційної таємниці обмежується періодом дії сукупності факторів, коли така інформація: має комерційну цінність, невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а власник інформації вживає належних заходів до охорони її таємності.

2.3. Комерційна таємниця в умовах розвитку інформаційної економіки

Для організації ефективного захисту комерційно цінної економічної інформації необхідно, щоб економічно важливі відомості мали статус комерційної таємниці, тобто потрібно належним чином їх оформити:

• обумовити існування комерційної таємниці в установчих документах;

• виключити з переліку інформацію, яка є державною таємницею, та ту, що не є КТ;

• згрупувати та класифікувати конфіденційну інформацію, яка належить до комерційної таємниці;таємниці, що належать державі, тобто та інформація, яка становить державну таємницю.

• розробити положення про КТ, яке є основним правовим захистом інформації;

• розробити договори-контракти для укладення їх із працівниками щодо нерозголошення КТ, розробити інструкції та порядок ознайомлення працівників із документами щодо захисту інформації;

• розробити правила внутрішнього розпорядку та посадові інструкції осіб, які мають доступ до таємної інформації;

• розробити інструкцію з дотримання режиму таємності та графік роботи з таємними документами тощо. фінансово-кредитну таємницю.

Закріплення права на КТ здійснюється у таких документах підприємства:

• статуті підприємства, (прописати, що на підприємстві вводиться режим комерційної таємниці);

• засновницькому договорі;
• колективному договорі;
• положенні «Про комерційну таємницю і правила її збереження»;
• положенні «Про дозвільну систему доступу виконавців до документів і відомостей, що є комерційною таємницею підприємства», «Режим роботи з комерційною таємницею співробітників»;
• та інших аналогічних документах.

Серед методів захисту можна відзначити:

• розробку положення про КТ на підприємстві;
• розробку інструкцій щодо дотримання співробітниками режиму нерозголошення КТ;
• включення до статуту підприємства розділів, що регламентують захист;
• розробку угоди про нерозголошення комерційної таємниці з особами, що мають доступ до цієї інформації.

ТЕМА 3
ОСНОВНІ ОБ'ЄКТИ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

3.1. Режим комерційної таємниці.
3.2. Ноу-хау" як різновид комерційної таємниці.
3.3. Права власності на комерційну таємницю.

3.1. Режим комерційної таємниці.

Режим комерційної таємниці – правові, організаційні, технічні та інші прийняті власником інформації, що становить комерційну таємницю, заходи з охорони її конфіденційності.

Віднесення інформації до категорії комерційної таємниці диктується, необхідністю захисту економічних інтересів підприємства в умовах ринкової конкуренції, особливо, коли вона носить несумлінний характер.

Тому, приступаючи до етапу визначення відомостей, що становлять комерційну таємницю, слід проаналізувати можливі устремління конкурентів. Найчастіше вони зводяться до одержання інформації про:

- фінансове становище підприємства;
- прогноз його розвитку в майбутньому;
- умовах контрактів та угод;
- технологічної і технічної специфікації випускається перспективної продукції;
- маркетингу та стратегії цін;
- системі безпеки підприємства.

Основними складовими комерційної таємниці виступають:

- комерційна інформація, що допомагає керівництву підприємства планувати свою діяльність. Її предметом можуть бути: ділові зв'язки; закупівля сировини та товарів; дані про постачальників; плановий прибуток тощо.

На рисунку 3.1подано види даних, що складають комерційну таємницю.

Рисунок 3.1 – Види даних, що складають комерційну таємницю

- секрети виробництва («ноу-хау»);
- організаційно-управлінська діяльність підприємства – це складне і неоднорідне явище, орієнтоване на отримання прибутку.

В організаційному плані роботу з визначення відомостей, що становлять комерційну таємницю можна розділити **на три етапи**.

Перший етап передбачає видання наказу про порядок визначення відомостей, що становлять комерційну таємницю.

Де передбачаються:

- створення постійно діючої комісії з комерційної таємниці;
- визначення категорій персоналу, якому надається право попередньої класифікації інформації як комерційноїтаємниці (інженерно-технічний, наукові співробітники, менеджери, маркетологи, економісти, юристи тощо);
- порядок документування роботи з визначення відомостей, що становлять комерційну таємницю;
- строки підготовки переліку відомостей, що становлять комерційну таємницю і його подання для затвердження керівництвом.

З метою забезпечення єдиного підходу до відбору відомостей, що становлять комерційну таємницю, на підприємстві може бути розроблена відповідна методика.

На другому етапі постійно діюча комісія повинна проаналізувати можливі збитки від витоку виділених на першому етапі відомостей.

Третій етап зводиться до формування переліку відомостей, що становлять комерційну таємницю підприємства та введення його в дію.

Структура такого переліку може бути наступна:

Виробництво; Управління; -Плани; Наради; Фінанси; Стан ринку; Партнери; Контракти; Ціни; Науково-технічні досягнення; Система безпеки підприємства.

Підготовлений постійно-діючою комісією перелік відомостей, що становлять комерційну таємницю, подається на затвердження керівництву підприємства і після його затвердження вводиться в дію відповідним наказом.

3.2."Ноу-хау" як різновид комерційної таємниці

З поняттям "комерційна таємниця" тісно пов’язане поняття "ноу-хау". "Ноу-хау" є вужчим поняттям і складає підінститут комерційної таємниці.

З моменту появи терміна "ноу-хау" (від англ. know how – знаю як) і дотепер немає чіткого наукового визначення цього поняття.

Нині "ноу-хау" визначається як сукупність знань і навичок, що стосуються промислової власності або процесу, пов’язана з таємницями виробництва, є конфіденційною (економічним надбанням, придатним для експлуатації), передається в речовій (матеріальній) та нематеріальній формах.

Згідно з визначенням Міжнародної ліги конкурентного права, ноу-хау складаються із технічної, комерційної, адміністративної або іншої інформації, що не охоплюється патентами і використовується при експлуатації певного

підприємства, здійсненні інформаційної діяльності, до якої немає легкого доступу (секрет виробництва) і яка може передаватися за договором

До ноу-хау можуть бути віднесені:

– різного роду технічні знання і досвід, що не мають правової охорони, включаючи методи, способи і навички, необхідні для проведення проектування, розрахунків, будівництва або виготовлення будь-яких об'єктів чи виробів, науково-дослідних, дослідно-конструкторських, пусконалагоджувальних та інших робіт;

– розробки та використання технологічних процесів; склад речовин, сплавів тощо, методи і способи лікування, пошуку і видобутку корисних копалин; знання і досвід адміністративного, економічного, фінансового або іншого порядку.

Водночас, на думку деяких дослідників, "ноу-хау" і "комерційна таємниця" – поняття не стільки ідентичні, скільки такі, що перетинаються.

За своєю юридичною природою і характером правової охорони "ноу-хау" має визначені особливості.

Так, інформація, що складає предмет "ноу-хау", не підлягає реєстрації в будь-якому державному органі і на неї не одержується патент, свідоцтво тощо. Спеціальне законодавство, яке докладно регламентувало б правову охорону "ноу-хау", у розвинутих країнах є відсутнім.

Не є винятком і Україна. Для забезпечення правової охорони "ноу-хау" застосовуються загальні положення цивільних законодавств (положення про службову і комерційну таємниці), норми, спрямовані на захист від недобросовісної конкуренції, положення договірного права. Згідно з деякими міжнародними документами, ратифікованими на території України, визначені положення і права на ноу-хау як на вид інтелектуальної власності.

Таким чином, комерційна таємниця – це виробнича, науково-технічна, управлінська, фінансова та інша документована інформація, яку використовують для досягнення комерційних цілей (одержання прибутку, запобігання втратам, одержання добросовісної переваги над конкурентами), яку підприємець вважає конфіденційною.

3.3. Права власності на комерційну таємницю

Для правового регулювання відносин суб'єктів підприємницької діяльності в умовах, захисту їх інтересів від неправомірних дій конкурентів необхідно було створити відповідну правову базу, та поділити на два основних підмасиви:

- таємниці, що належать підприємствам, які не підпадають під державне управління (маються на увазі відомості, що становлять комерційну та банківську таємницю концернів, асоціацій, господарських товариств, комерційних банків;
- таємниці, що належать державі, тобто та інформація, яка становить державну таємницю.

Закон "Про інформацію" (далі – Закон) вніс деякі корективи до вказаного умовного підходу до класифікації секретів, встановивши поняття "інформація з

обмеженим доступом", яка за своїм правовим режимом поділяється на:

- конфіденційну інформацію; таємну інформацію.

Аналізуючи (ст. 62 ГКУ) цього Закону, слід зробити висновок про те, що до інформації з обмеженим доступом відноситься:

- інформація, яка містить комерційну таємницю;
- інформація, яка складає банківську таємницю;
- конфіденційна інформація.

Зміст комерційної таємниці становлять три види:

- власну комерційну таємницю;
- промислову таємницю;
- фінансово-кредитну таємницю.

До промислової таємниці вони, зокрема, пропонують віднести секрети виробництва, ноу-хау, відкриття, хімічну формулу будь-якої речовини, методи та засоби керівництва виробництвом, маркетинг і т. ін.

До фінансово-кредитної таємниці відносять – інформацію, яка міститься в бухгалтерських та інших фінансових документах. На їх думку, збереження в таємниці цієї інформації від усіх сторонніх суб'єктів господарювання є невід'ємною умовою в боротьбі з конкурентами, та її захист доцільний в зв'язку з небезпекою промислового шпигунства. Тому, слід відзначити наступне:

По-перше, комерційною таємницею підприємства може бути все, що не заборонено законом, корисно у підприємницькій діяльності та дає перевагу над конкурентами, які не володіють нею.

По-друге, інформація, яка складає комерційну таємницю підприємства, повинна мати певні ознаки та відповідно до Господарського кодексу, закону "Про інформацію".

Суб'єктом права власності на комерційну таємницю, відповідно до чинного законодавства України, зокрема Господарського кодексу, Цивільного кодексу, законів "Про інформацію", "Про науково-технічну інформацію" тощо, є: держава, громадяни України, інших держав, підприємства, установи, організації всіх форм власності, які здійснюють свою діяльність відповідно до законодавства України і визначили інформацію, яка складає їх комерційну таємницю.

ТЕМА 4
СИСТЕМА ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

План

4.1. Вплив комерційної інформації на формування системи захисту інформації на підприємстві.

4.2. Поняття та зміст конфіденційної інформації та канали її витоку.

4.3. Недобросовісна конкуренція і методи викрадення таємниць підприємства.

4.1 Вплив комерційної інформації на формування системи

захисту інформації на підприємстві

Для забезпечення захисту комерційної таємниці на підприємстві необхідно дотримуватися наступних рекомендацій:

1. Існування комерційної таємниці та конфіденційної інформації **бажано вказати в установчих документах** підприємця, включивши, наприклад, в установчий договір й (або) статут підприємства розділ, що регламентує захист інформації з обмеженим доступом.

2. При формуванні переліку відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємця, доцільно видати **наказ про створення переліку відомостей, які складають комерційну таємницю**.

3. Розробка положення про комерційну таємницю та конфіденційну інформацію на підприємства розкриває:

- загальні положення у сфері захисту інформації,
- принципи і процедури розмежування доступу до такої інформації,
- порядок прийому, реєстрації, інвентаризації та обліку носіїв інформації, що містить комерційну таємницю та конфіденційну інформацію.
- процедури забезпечення доступу до комерційної таємниці сторонніх осіб (включаючи контролюючі органи).
- порядок поширення комерційної таємниці та конфіденційної інформації, а також процедуру виключення інформації з переліку комерційної таємниці та конфіденційної інформації.

4. Інструкція про порядок підготовки, обліку, зберігання та знищення документів, справ, видань і матеріалів, що містять комерційну таємницю та конфіденційну інформацію підприємства, встановлює конкретні механізми охорони комерційної таємниці та конфіденційної інформації.

5. Рекомендується **включати норму про нерозголошення** комерційної таємниці та конфіденційної інформації **в трудовий договір** (контракт) як керівника підприємства, так й інших співробітників.

6. Працівник під розписку повинен бути попереджений про відповідальність за невиконання взятих на себе зобов'язань.

7. На підприємстві варто розробити **спеціальний договір про збереження комерційної таємниці та конфіденційної інформації**. Навіть перевіряючі повинні будуть дотриматися всіх процедур, які встановлені на підприємстві для одержання доступу до комерційної таємниці. І, підписавши документ про нерозголошення комерційної таємниці та конфіденційної інформації, такі особи не мають права використати отриману інформацію у своїй діяльності без згоди керівництва підприємства.

8. **Правила внутрішнього розпорядку** і **посадові інструкції осіб**, що працюють із комерційною таємницею, а також **інструкції про ведення переговорів**, інструкції про **роботу з документами** також повинні містити застереження про комерційну таємницю та конфіденційну інформацію.

9. Необхідним є **застосування технічних засобів захисту відомостей**.

10. Особливістю **організації інформаційних потоків на підприємстві** з

метою захисту «критичної» інформації, протидії промисловому шпигунству та організації дезінформування є розробка на підприємстві **Порядку поширення інформації з обмеженим доступом**, яка належить підприємству.

4.2. Поняття та зміст конфіденційної інформації та канали її витоку

Початок використання комп'ютерів у бізнесі створив великі можливості, але і не менші загрози. Вкрасти інформацію непомітно набагато легше із комп'ютерної системи ніж, наприклад, із архіву. Тому що копія електронного документу нічим не відрізняється від оригіналу.

- Юридичний захист інформації.
- Організаційний.
- Фізичний.
- Технічний.

Проблема інформаційних систем – доступ до них мають багато користувачів (різні права доступу).

Ускладнення засобів і методів організації машинної обробки інформації призводить до того, що інформація стає все більш уразливою:

– постійно зростаючі обсяги даних,
– накопичування і зберігання даних в обмежених місцях,
– постійне розширення кола користувачів, які мають доступ як до ресурсів інформаційної системи, так до програм і даних, що зберігаються в них,
– зростання складності ПЗ.

Різниця між "розголос інформації" та "витік інформації".

Розголошує інформацію завжди людина - усно, письмово, за допомогою жестів, міміки, умовних сигналів, особисто або через посередника.

Термін "витік інформації" – втрата інформації за рахунок її перехоплення або злому комп'ютерних систем.

Інколи перехід інформації до третьої особи може бути класифікованій, як ненавмисний:

1) втрата або випадкове розповсюдження документу;
2) незнання або нерозуміння співробітником вимог по захисту інформації;
3) надмірна балакучість співробітників;
4) робота з конфіденційними документами при сторонніх особах,
5) несанкціонована передача конфіденційного документа іншому співробітнику;
6) використання конфіденційних відомостей в особистих записах, неслужбових листах;
7) надмірна кількість конфіденційної інформації в фірмі;
8) копіювання співробітником документів в особистих цілях.

4.3. Недобросовісна конкуренція і методи викрадення таємниць підприємства

Відомі три форми недобросовісної конкуренції:

1. Економічне придушення, яке передбачає різні засоби і способи обмеження ділової практики, компрометацію фірм-конкурентів, їх керівників, шантаж персоналу, зрив операцій, паралізацію діяльності фірм шляхом використання ЗМІ і мафіозних зв'язків у державних органах.

2. Промислове або комерційне шпигунство, яке має на меті протиправне заволодіння комерційними засобами конкурента для отримання власних вигод.

Якщо інформація про конкурентів, що надходить легальними каналами, не

3. Пряме фізичне придушення, що є злочинним посяганням на життя і здоров'я персоналу підприємства. Основні методи фізичного придушення конкурента:

– організація пограбувань і розбійних нападів на офіси, виробничі та складські приміщення, розкрадання вантажів тощо;

Методами економічного шпигунства вважається:

– підкуп або шантаж співробітників фірми;

– знімання інформації з ПЕВМ спецтехнікою (проникнення в бази даних, копіювання програм);

– копіювання або розкрадання документів, креслень, експериментальних і товарних зразків;

– прослуховування телефонних розмов, підслуховування розмов в приміщеннях і автомобілях.

Відповідно до міжнародних правових норм розрізняють три види недобросовісної конкуренції:

1) коли комерційну діяльність однієї фірми прагнуть видати споживачеві за діяльність іншої;

2) дискредитація комерційної діяльності за допомогою розповсюдження помилкової інформації;

3) неправомірне використання в комерційній діяльності позначень, що вводять споживача в оману.

Існуючі на Заході законодавчі акти щодо товарних знаків, фірмових найменувань, недобросовісної конкуренції визначають конкретну відповідальність за такі дії:

– підкуп покупців конкурентів;

– з'ясування комерційних таємниць конкурента за допомогою шпигунства або підкупу його службовців;

– установлення дискримінаційних комерційних умов;

– таємна змова на торгах і неофіційне створення таємних картелів;

– бойкот торгівлі іншої фірми для протидії конкуренції або запобігання їй;

– продаж своїх товарів за свідомо заниженою ціною з наміром протидіяти конкуренції або придушити її (демпінг);

– навмисне копіювання товарів, послуг, реклами або інших видів комерційної діяльності конкурента і т.ін.

ТЕМА 5
ОХОРОНА КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

План

5.1. Основні права на комерційну таємницю підприємства.

5.2. Сутність охорони комерційної таємниці на підприємстві.

5.3. Загальні положення договору про нерозголошення комерційної таємниці в Україні.

5.1.Основні права на комерційну таємницю на підприємстві

Правами на комерційну таємницю в суб'єктивному розумінні є сукупність встановлених законом правомочностей особи щодо належної їй комерційної таємниці, а саме:

- право на використання комерційної таємниці,
- виключне право дозволяти її використання іншим особам,
- виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці.

Права на комерційну таємницю в Україні прирівняні до прав промислової власності (а саме – до прав на захист від недобросовісної конкуренції).

Власник інформації, що становить комерційну таємницю, має право:

1) встановлювати, змінювати й скасовувати в письмовій формі режим комерційної таємниці відповідно до цього Закону й цивільно-правового договору;

2) використовувати інформацію, що становить комерційну таємницю, для власних потреб у порядку, що не суперечить законодавству;

3) дозволяти або забороняти доступ до інформації, що становить комерційну таємницю, визначати порядок і умови доступу до цієї інформації;

4) вводити в цивільний оборот інформацію, що становить комерційну таємницю, на підставі договорів, що передбачають включення в них умов про охорону конфіденційності цієї інформації;

5) вимагати від юридичних і фізичних осіб, що одержали доступ до інформації, що становить комерційну таємницю, органів державної влади, інших державних органів, органів місцевого самоврядування, яким надана інформація, що складає комерційну таємницю, дотримання обов'язків по охороні її конфіденційності;

6) вимагати від осіб, що одержали доступ до інформації, що становить комерційну таємницю, у результаті дій, здійснених випадково або помилково, охорони конфіденційності цієї інформації;

7) захищати у встановленому законом порядку свої права у випадку розголошення, незаконного одержання або незаконного використання третіми особами інформації, що становить комерційну таємницю, у тому числі вимагати відшкодування збитків, заподіяних у зв'язку з порушенням його прав.

Використанням комерційної таємниці слід вважати її застосування у виробничих, технічних, економічних, організаційних та інших цілях, зокрема у товарах, що

виробляються, при виробленні товарів, при реалізації економічних та організаційних рішень тощо.

Суб'єктом права на комерційну таємницю є учасник цивільних відносин, який потенційно може набувати права щодо комерційної таємниці. Такими суб'єктами можуть бути будь-які учасники цивільних відносин, названі у ст. 2 ЦК України, а саме:

- фізичні та юридичні особи,
- держава Україна,
- територіальні громади,
- іноземні держави та інші суб'єкти публічного права.

Право на комерційну таємницю може належати лише тій особі, яка своїм волевиявленням засвідчила намір утримувати певні комерційно цінні відомості в режимі конфіденційності та вжила адекватних дій щодо збереження такого стану невідомості інформації.

Суб'єктивні права на комерційну таємницю виникають на підставі юридичного складу, тобто за умови одночасного настання таких обставин:

– правомірне володіння особою інформацією з правом визначати режим доступу до неї;

– наявність в цієї інформації ознак конфіденційності та комерційної цінності;

– вжиття такою особою адекватних існуючим обставинам заходів щодо збереження її конфіденційності.

Правомірне володіння інформацією, конфіденційність та комерційна цінність інформації, яка становить комерційну таємницю, є юридичними фактами-станами, а вжиття заходів захисту – правомірними юридичними діями.

Загальною підставою припинення правовідносин щодо комерційної таємниці є припинення хоча б однієї з її ознак.

5.2. Сутність охорони комерційної таємниці

Під охороною права розуміють систему заходів, спрямованих на забезпечення прав та інтересів правомочної особи.

Чинний Цивільний кодекс України (далі ЦК України) закріпив норму щодо охорони комерційної таємниці органами державної влади, що проявляється в недопущенні недобросовісного комерційного використання такої інформації та її розголошення. Виключення становлять тільки випадки, коли таке розголошення необхідне для забезпечення захисту населення або коли не вжито заходів щодо її охорони від недобросовісного комерційного використання.

Відповідно особа, яка законним чином контролює комерційну таємницю (це ж стосується і ноу-хау) повинна вжити необхідні заходи щодо охорони її конфіденційності. Такі заходи повинні бути направлені на збереження комерційної таємниці (або ноу-хау) в секреті.

Вимога щодо охорони конфіденційності інформації взаємопов'язана і з іншими критеріями охороноздатності, оскільки якщо інформація не зберігається

в секреті, то вона може бути доступна необмеженому колу осіб. Таким чином, зразу порушується умова незагальновідомості і нелегкодоступності, в результаті чого втрачається її комерційна цінність, а як наслідок і режим «конфіденційності».

Відповідно особа, яка законно контролює комерційну таємницю або ноу-хау повинна здійснювати фактичні дії, направлені, з одного боку, на створення «режиму недоступності» до інформації, яку вони вважають конфіденційною а, з іншого боку, направлені на створення «режиму доступності» до неї. Однак аналіз практики свідчить про те, що ні фізичні, ні юридичні особи, їх посадові особи, як правило, не мають достатнього досвіду по відношенню до підстав і порядку описання інформації, яка і є охороноздатною, тобто підпадає під режим обмеженого доступу.

Таким чином, право доступу до комерційної таємниці і ноу-хау засновано на принципі конфіденційності. Отже, комерційна таємниця, ноу-хау існує до того часу, поки відомості про них залишаються конфіденційними (недоступними іншим особам). Тому можна сказати, що охороняється не сама комерційна таємниця чи ноу-хау, а «законний інтерес» особи, яка законно її контролює.

При цьому режим «комерційної таємниці» або «ноу-хау» існує до того часу, поки дотримується її секретність (конфіденційність). Охорона може бути і в тих випадках, коли дані про них передані (надано доступ). Умовно виділяють два види охорони інформації, що використовуються в підприємницькій діяльності та становить комерційну таємницю: пасивну й активну.

Пасивна охорона характеризується тим, що власник інформації надає їй режим відкритості, доступності для всіх зацікавлених осіб, але ці особи не можуть використовувати її в комерційних цілях.

Активна охорона інформації, що більше підходить для охорони комерційної таємниці від несанкціонованого власником використання, пов'язана з тим, що власник встановлює певний режим доступу. Таким чином, комерційна таємниця як об'єкт взагалі не охороняється, оскільки їй не надається абсолютна охорона, незалежно від зовнішніх обставин, тому здійснюється «захист» інтересів суб'єктів в зв'язку з відповідними об'єктами. Але цей «захист» надається уже в зв'язку не стільки з внутрішніми властивостями самих об'єктів, скільки з урахуванням зовнішніх обставин.

5.3. Загальні положення договору про нерозголошення комерційної таємниці в Україні

Договір – це домовленість двох і більше осіб, спрямована на встановлення, зміну або припинення цивільних прав та обов'язків. Поняття договору розкривається через поняття угоди. Договір у цивільному праві являє собою угоду, яка вчиняється на підставі погодження волі сторін з приводу певних прав і обов'язків. 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 визначають що конкретно є конфіденційною інформацією.

Умови 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 ліцензії на інтелектуальну власність з конфіденційної інформації;
- захистити себе від будь-якої потенційної відповідальності за конфіденційну інформацію.

Отже, договір про нерозголошення конфіденційної інформації (комерційної таємниці) – це угода між правовласником, який передає відомості, предметом яких є комерційна таємниця зацікавленій особі, яка зобов'язується належним чином дотримуватись умов договору, а в разі їх порушення нести відповідальність відповідно до умов договору та чинного законодавства.

Тема 6
ОСНОВНІ ЗАСАДИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

План

6.1. Методи захисту комерційної таємниці.

6.2 Цивільно-правовий та адміністративно-правовий захист комерційної таємниці.

6.3. Основні засади кримінального захисту комерційної таємниці в договірних відносинах.

6.1. Методи захисту комерційної таємниці

Враховуючи небезпечні можливості витікання комерційної таємниці, світовою практикою розроблені відповідні **методи захисту**:

1. правові;
2. організаційні;
3. технічні.

Правовий захист полягає в оформленні деяких документів, що забезпечують його, - наказ, статут, трудові контракти та угоди, правила внутрішнього розпорядку.

Організаційний захист передбачає:

• організацію конфіденційного діловодства;

• обмеження доступу до документів з відповідною градацією допуску до них;

• порядок використання технічних засобів і приміщень (при цьому для копіювання та розмноження паперів здійснюється облік паперу, підтверджений

свідками або відповідними документами);

•супровід відвідувачів під час їх перебування в службових приміщеннях;

•встановлення порядку ведення переговорів (виявлення наміру відвідувачів, мети їх приходу);

•навчання співробітників заходам захисту, підвищення вимогливості і відповідальності.

До технічних відносяться заходи, пов'язані з використанням різноманітних технічних засобів, які перешкоджають несанкційованому доступу до інформації. *Технічний захист використовує*:

•засоби охорони територій (контролюючи системи, огорожі з автоматичною системою телевізійного контролю, електронно-оптичні засоби контролю);

•засоби захисту комунікацій (процеси обробки, передачі і збереження інформації за допомогою електроніки – пристроїв з побічними чи паразитними випромінюваннями.

Застосовуючи весь арсенал засобів для попередження витікання комерційної таємниці, слід вжити і відповідних заходів захисту:

•пошук підслуховуючих пристроїв;

•шифрування ділової кореспонденції;

•захист апаратури від випромінювання з допомогою захисних блоків;

•створення комп'ютерних систем і банку технічних даних по охороні;

•створення внутрішніх перепон акустичним імпульсам.

Важливою проблемою є захист інформації від підробок та виправлень. Найпоширенішим способом захисту є використання сейфів та передача важливих документів на збереження в банк.

6.2 Цивільно-правовий та адміністративно-правовий захист комерційної таємниці

Підставами для цивільно-правової відповідальності може бути порушення договірного зобов'язання або позадоговірні порушення. Договірні порушення стосуються переважно ліцензійних договорів – на них поширюються всі загальні правила про відповідальність за порушення зобов'язання (Глава 51 ЦКУ).

Позадоговірний захист прав на комерційну таємницю ґрунтується на загальних положеннях про деліктну відповідальність та особливостях правового режиму комерційної таємниці як об'єкту інтелектуальної власності. Стаття 432 ЦКУ надає кожній особі право звернутися до суду за захистом свого права інтелектуальної власності відповідно до статті 16 Кодексу, якою визначаються можливі способи захисту цивільних прав та інтересів.

З особливостей об'єкту захисту комерційної таємниці та її правового режиму випливають характерні риси відповідальності за порушення прав на комерційну таємницю. Для комерційної таємниці як неформалізованого результату інтелектуальної діяльності (на відміну від об'єктів авторського або патентного права) властивий принцип свободи використання і презумпція

добросовісності користувача прав на комерційну таємницю, якщо не буде доведеним факт порушення встановленого законом режиму охорони. Тоді як для об'єктів авторського та патентного права діє презумпція недобросовісності їх використання третіми особами (якщо інше прямо не передбачено договором з правовласником) – звідси відповідальність незалежно від вини. Натомість вина є обов'язковою умовою відповідальності за порушення прав на комерційну таємницю.

Для комерційної таємниці не можливим є такий спосіб захисту як відновлення становища, яке існувало до порушення. Адже, відомості розголошуються безповоротно, їх не можна вилучити зі свідомості особи, яка незаконно з ними ознайомилася. Відповідно захист може полягати лише у відшкодуванні збитків та забороні продовжувати порушення.

Ці способи можуть застосовуватись лише до обмеженого кола фактичних порушників. останніх можна поділити на дві групи: особи, які безпосередньо неправомірно втрутилися у сферу правовласника (первинні порушники); та особи, які використали результати первинного порушення (вторинні порушники)

Вчинення дій, визначених Законом «Про захист від недобросовісної конкуренції» як недобросовісна конкуренція, «юридичними особами, їх об'єднаннями та об'єднаннями громадян, що не є господарюючими суб'єктами», тягне за собою накладання на них Антимонопольним комітетом України, його територіальними відділеннями штрафів.

6.3. Основні засади кримінального захисту комерційної таємниці в договірних відносинах

Кримінальна відповідальність за діяння, пов'язані з порушенням режиму комерційної таємниці, була введена в українське законодавство в 1994 році, коли Законом №3888-12 від 28.01.2004 Кримінальний кодекс УРСР було доповнено двома статтями 148-6 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю» та 148-7 «Розголошення комерційної таємниці». Ці два склади злочини були закріплені й у Кримінальному кодексі України (відповідно, статті 231 та 232).

У статті 231 безпосередньо розшифровано поняття «незаконне збирання відомостей, що становлять комерційну таємницю», яке раніше тлумачилось відповідно до положення статті 16 Закону «Про захист від недобросовісної конкуренції», що було відтвореним з незначними змінами й у статті 36 Господарського кодексу Україні («добування протиправним способом відомостей, що відповідно до законодавства України становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю)»).

Статтею 231 чинного ККУ, передбачена відповідальність за два окремі склади злочину: 1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю; 2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це спричинило істотну шкоду суб'єкту

господарської діяльності.

З конструкції статті 231 ККУ випливає, що злочин у цій формі вважатиметься закінченим з моменту вчинення будь-яких дій, спрямованих на незаконне збирання зазначених відомостей, незалежно від подальшого їх використання, якщо використання таких відомостей може завдати істотної шкоди суб'єкту господарювання. Отже, для наявності закінченого складу цього злочину, не обов'язковим є фактичне використання незаконно одержаних відомостей, так само як не є обов'язковим і заподіяння реальної шкоди (тому важливим є визначення безпосередньо в тексті кримінального закону терміну «незаконне збирання»).

Суб'єктивна сторона незаконного збирання характеризується прямим умислом та обов'язковою ознакою – наявністю мети: подальше розголошення або інше використання відомостей. Таким використанням може бути: розголошення з метою заподіяння матеріальної чи іншої шкоди; використання для власних потреб. Термін розголошення слід вживати в розумінні статті 17 Закону «Про захист від недобросовісної конкуренції», положення якої були продубльовані в Господарському кодексі України.

Під незаконним використанням відомостей, що становлять комерційну таємницю, у свою чергу, розуміється (але не обмежується) «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 законодавства України комерційну таємницю» (стаття 19 Закону «Про захист від недобросовісної конкуренції»).

Щодо наслідків незаконного використання зазначених відомостей у вигляді спричинення істотної шкоди суб'єкту господарської діяльності умисел може бути як прямим, так і непрямим.

Тема 7
ПРОМИСЛОВЕ ШПИГУНСТВО ТА ЗАСОБИ БОРОТЬБИ З НИМ

7.1. Методи захисту комерційної таємниці.

7.2 Цивільно-правовий та адміністративно-правовий захист комерційної таємниці.

7.3. Основні проблеми комерційної таємниці суб'єктів господарювання у договірних відносинах.

7.1. Промислове шпигунство як засіб неправомірного отримання комерційної таємниці

Виділяють *три пріоритетних напрямки*:

- макроекономічна розвідка – збір стратегічної інформації про глобальні процеси в економіках інших держав;
- мікроекономічна розвідка – збір тактичної й оперативної інформації про діяльність окремих компаній;
- економічна контррозвідка – протидія спробам іноземних державних

спецслужб і комерційних фірм здобути американські торгово-економічні й технологічні секрети.

Промислове шпигунство щодо бізнесу – це різновид економічного шпигунства, якому властиве звуження масштабів завдань з одержання інформації, що цікавить, від державного – до масштабу однієї або декількох фірм-конкурентів. Отже, для бізнесу промислове шпигунство – лише спосіб конкурентної боротьби.

Промислове шпигунство має дві мети:

• отримання інформації конкурентів, насамперед конфіденційної, про стратегічні й тактичні наміри їхнього бізнесу;

• здобуття конкурентної переваги на ринку, через витіснення або знищення конкурента.

Інсайдер – особа, яка володіє конфеденційною діловою інформацією в силу свого службового положення.

Довідники описують **промислове шпигунство** як вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність.

Необхідно одразу розмежувати поняття *розвідка і промислове шпигунство*. Метою як конкурентної розвідки, так і промислового шпигунства є одержання інформації, яка б дала змогу здобути конкурентну перевагу на ринку. Головною відмінністю між конкурентною розвідкою та промисловим шпигунством є методи й способи отримання інформації. Характерні ознаки промислового шпигунства наведено на рис.7.1.

Промисловий шпіонаж, навпаки, передбачає нелегальні методи й технології. Служба конкурентної розвідки користується тільки відкритими джерелами, оскільки робота розвідника — інформаційно-аналітична, тобто збирання й обробка різних даних, що впливають або можуть вплинути на розвиток бізнесу.

Сукупність *методів, притаманних промисловому шпигунству*, можна об'єднати у дві групи.

- **Агентурні методи.**
- **Технічні методи**.

Агентурний метод одержання інформації містить два напрями діяльності: або вербування, або впровадження своєї людини.

Інший напрям промислового шпигунства, що набуває популярності в усьому світі, а також і в Україні, — це отримання *конфіденційної інформації* за допомогою Інтернету.

В Україні понад 30 підприємств мають ліцензію на розробку й виготовлення підслуховувальних закладних пристроїв.

Це основні методи промислового шпигунства, які, у свою чергу, поділяються ще на низку способів добування конфіденційної інформації (дезінформування конкурентів, шантаж і підкуп, використання можливостей правоохоронних та контрольних органів тощо).

Рисунок 7.1 – Основні ознаки промислового шпигунства

7.2. Конкурентна розвідка як противага промисловому шпигунству

Конкурентна розвідка – постійний процес збору, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії й надання вищому менеджменту компанії інформації, що дозволяє йому передбачати зміни в обстановці й приймати своєчасні оптимальні рішення щодо управління ризиками, впровадження змін у компанії й відповідних заходів, спрямованих на задоволення майбутніх запитів споживачів і підтримку прибутковості.

Методи конкурентної розвідки умовно можна поділити на цілком законні (білі) та методи, які за своєю формою не порушують норм законів, проте не завжди відповідають морально-етичним нормам ведення чесної конкурентної боротьби (сірі методи).

До першої групи методів конкурентної розвідки, тобто до законних, належать:

• вивчення й аналіз публікацій конкурента;

• вивчення, аналіз та обробка матеріальне заохочення співробітників конкурента з метою відкритої інформації про конкурента.

До другої групи методів належать такі:

• отримання конфіденційної інформації;

• «переманювання» спеціалістів конкурента і отримання в них відомостей, що мають обмежений доступ;

• вивідування інформації у співробітника конкурента;

• проведення підставних переговорів з метою вивідування конфіденційної інформації;

• отримання необхідної інформації про конкурента через зв'язки в правоохоронних та контролюючих органах.

Залежно від спрямованості виділяють наступні види конкурентної розвідки:

1. Розвідка проти компанії.

а) *систематичний аналіз інформаційного поля.*

б) *Аналіз установчих і статутних документів й організаційної структури компанії.*

в) *Співбесіда при «наймі» на роботу працівників конкурента, установлення помилкових партнерських зв'язків через дружні підприємства*

2. Розвідка проти персони:

а) *Аналіз ділових зв'язків і комунікативних контактів осіб, які приймають рішення/*

б) *Аналіз біографії керівників компанії конкурента/*

в) *Аналіз позаділового життя керівників компанії конкурента/*

3. Фінансовий моніторинг. Фінансовий моніторинг дозволяє визначити економічну потужність загроз, використовуючи наступні методи:

а) *Метод аналогії.*

б) *Метод розрахунку за непрямими ознаками*.
в) *Метод інтерполяцій*.

4. Оцінка інвестиційних проектів конкурентів. Якщо розвідувальні дії виконуються регулярно, то інформації буде досить для проведення швидкої оцінки інвестиційних проектів конкурентів, використовуючи наступні методи:

а) *Метод експертного інтерв'ю*.

б) *Вивчення ділового й адміністративного оточення конкурента*.

Отже, використання методів економічної розвідки потрібне найперше за таких випадків:

- відкриття нового напряму бізнесу;
- зміни поводження на ринку конкурента, партнера;
- появи нового партнера, конкурента на вашому полі;
- появи у вашому бізнесі проблем зовнішнього характеру (зриви поставок, компрометуючі факти в пресі, поява проблем з контролюючими органами влади).

7.3. Основні проблеми комерційної таємниці суб'єктів господарювання у договірних відносинах

Захист комерційної таємниці, яка міститься у господарських договорах, як частина діяльності щодо забезпечення безпеки підприємництва, в цілому припускає, що можливі протиправні посягання на таку інформацію можуть мати різну спрямованість. Володіння комерційною таємницею суб'єктів господарювання особами, які є конкурентами у бізнесі, дозволяє їм своєчасно координувати свою стратегію, виявляти додатковий ринок збуту своїх товарів чи послуг, покупців, знижувати свої комерційні ризики і витрати та підвищувати свої доходи.

У зв'язку з цим ефективний механізм захисту комерційної таємниці суб'єкта господарювання повинен передбачати: правове забезпечення інформаційної безпеки комерційної таємниці; впровадження новітніх світових досягнень технічного захисту комерційної інформації; здійснення інженерно-технічного захисту; мотивацію співробітників, від поведінки яких залежить витік інформації; відповідальність за розголошення конфіденційних відомостей.

Для більш ефективного захисту небажаної від розголошення інформації, яка може міститися й у договорах, слід розуміти поняття «комерційна інформація», «комерційна таємниця» та «конфіденційна інформація».

Підписання відповідних угод виправдане і у випадках, коли партнери вимагають надання всієї конфіденційної інформації для оцінки реального стану контрагента з метою прийняття рішення про укладення угоди. Однак до цього слід ставитися досить обережно. Угода також необхідна на той випадок, коли в діловій розмові один із партнерів повідомив іншому конфіденційні відомості, після чого останній, отримавши необхідну інформацію, відмовляється від укладення угоди, мотивуючи це різними обставинами, в тому числі й тим, що повідомлені конфіденційні відомості йому нібито були вже відомі.

Таким чином, перед підприємствами та іншими суб'єктами господарювання гостро постає завдання збереження інформації від розголошення, її безпеку, у тому числі відомостей, що становлять комерційну таємницю у відповідних договорах.

У системі забезпечення безпеки особливу роль необхідно приділити інформаційній безпеці підприємства. Зростаючий масив інформації, вдосконалення технічних засобів її зберігання, обробки та передачі потребує запровадження нових методів, прийомів та способів її захисту на основі діючого законодавства.

Розробку заходів щодо збереження комерційної таємниці підприємства слід здійснювати, дотримуючись принципів комплексного перекриття можливих каналів витоку інформації та забезпечення надійності захисту всіх її носіїв.

ТЕМА 8
ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В МІЖНАРОДНОМУ ЗАКОНОДАВСТВІ

8.1. Міжнародні договори в галузі охорони та захисту комерційної таємниці.

8.2. Законодавство іноземних країн стосовно захисту комерційної таємниці.

8.1. Міжнародні договори в галузі охорони та захисту комерційної таємниці

На відміну від патентів, торгових марок та авторського права, для комерційної таємниці відсутній єдиний міжнародний договір, що надавав би загальне визначення та встановлював уніфіковані основи правового захисту. Захист комерційної таємниці здійснюється у межах регіональних угод. Основою такого захисту вважається стаття 10 Паризької конвенції про охорону промислової власності 1883 року в редакції 1967 року (набула чинності для України 25 грудня 1991 р.) щодо недобросовісної конкуренції, основними положеннями якої є:

1) Країни Союзу зобов'язані забезпечити громадянам країн, що беруть участь у Союзі, ефективний захист від недобросовісної конкуренції.

2) Актом недобросовісної конкуренції вважається будь-який акт конкуренції, що суперечить чесним звичаям у промислових і торговельних справах.

Іншим важливим для характеристики комерційної таємниці міжнародним актом є Стокгольмська конвенція про заснування Всесвітньої організації інтелектуальної власності 1967 року. Відповідно до її статті 2, "інтелектуальна власність" включає права, що відносяться, зокрема, до "захисту проти недобросовісної конкуренції".

«Охорона закритої інформації» виділяються наступні положення, що мають відношення до комерційної таємниці:

1. У процесі забезпечення ефективного захисту від недобросовісної

конкуренції, як це передбачено статтею 10 Паризької конвенції (1967), країни-учасниці повинні охороняти закриту інформацію відповідно до частини другої цієї статті та дані, надані урядам або урядовим органам відповідно до частини третьої цієї статті.

2. Фізичні та юридичні особи повинні мати можливість перешкоджати тому, щоб інформація, яка правомірно знаходиться під їхнім контролем, була без їхньої згоди розкрита, отримана або використана іншими особами в спосіб, що суперечить чесній комерційній практиці, якщо ця інформація:

3. Країни-учасниці, у випадках, коли умовою погодження торгового обігу фармацевтичних або сільськогосподарських хімічних продуктів, у яких використовуються нові хімічні речовини, є подання попередньо нерозкритих даних про випробування або інших даних, отримання яких було пов'язано зі значними зусиллями, повинні охороняти такі дані від недобросовісного комерційного використання. Також, країни-учасниці повинні охороняти такі дані від розкриття (крім випадків, коли це необхідно для захисту населення або не вживаються заходи для забезпечення охорони цих даних від недобросовісного комерційного використання).

Отже, в Угоді ТРІПС було закріплено три відомі критерії режиму комерційної таємниці: *секретність, комерційна цінність та вжиття адекватних заходів для забезпечення секретності,* які запозичені з американського законодавства.

Правова система ЄС (acquis communautaire) не містить окремого акту для охорони комерційної таємниці. Це пов'язано, зокрема, з відмінною від американської ідеологією ставлення до охорони об'єктів інтелектуальної власності, що виходить з пріоритетності вільної конкуренції та вільного руху товарів (робіт, послуг).

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».

Огляд міждержавних угод, що стосуються охорони комерційної таємниці, свідчать про те, що така охорона більше не є справою виключно національного законодавства.

8.2. Законодавство іноземних країн стосовно захисту комерційної таємниці

У розвинутих країнах Європи охорона конфіденційної комерційної інформації має свою довгу історію, хоча підходи різняться залежно від країни. Найрозвиненішу систему охорону 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 та отримало назву конфіденційного права. Отже, охорона комерційної таємниці ґрунтується на концепції «порушення довіри»: керівним принципом є довіра між законним володільцем таємниці та отримувачем конфіденційної інформації.

Охорона комерційній інформації також надається законодавством Німеччини та Франції. Так, Розділом І Закону ФРН про недобросовісну конкуренцію встановлено відповідальність за завдання шкоди особою, яка при здійсненні підприємницької діяльності в цілях конкуренції вчиняє дії, несумісні з «чесною практикою». Під комерційною таємницею розуміється інформація, що має ознаку секретності (доступна лише відомому обмеженому колу осіб) та відповідає умові наявності у володільця цієї інформації обґрунтованого інтересу в її збереженні. Передбачена кримінальна відповідальність за злочини, пов'язані з порушенням режиму комерційної таємниці. У трудовому законодавстві міститься обов'язок працівника не розголошувати комерційну таємницю після припинення трудових відносин.

Законодавство Франції містить поняття промислових або виробничих секретів та комерційної таємниці. Перша категорія походить з 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 і може відноситися до організаційної структури підприємства, списку постачальників, особистих справ персоналу, контрактів з іншими організаціями, списків клієнтів, планів розвитку бізнесу, схеми дистрибуції тощо. Виробничі та комерційні секрети не вважаються власністю у Франції і отримують захист в якості деліктів з недобросовісної конкуренції та договірних зобов'язань.

Існує також значна кількість кримінальних законів, що стосуються незаконного заволодіння комерційною таємницею, основним з яких є федеральний Закон про Економічний шпіонаж 1996 року. Виділяють такі чотири основні елементи режиму комерційної таємниці в США:

По-перше, це повинна бути «обмежена інформація», тобто інформація, яку можна відрізнити від загально відомих знань та навичок.

По-друге, елемент «секретності» – інформація не є добре відомою або такою, яку можна легко отримати.

По-третє, інформація повинна мати економічну цінність, що полягає у наданні певної конкурентної переваги.

По-четверте, володілець повинен вжити розумних зусиль для того, щоб зберегти інформацію в таємниці.

Комерційною таємницею в американському законодавстві є інформація, у тому числі формула, зразок, компіляція, програма, пристрій, метод, техніка або

процес, яка:

а) має самостійну економічну цінність, дійсну або потенційну, у силу того, що не є загально відомою або легко доступною з використанням необхідних засобів для осіб, які можуть отримати економічну вигоду від її розкриття або використання;

б) є предметом розумових зусиль, за відповідних обставин для збереження її секретності.

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:

1) секретність інформації;

2) те, що її було надано конфіденційно;

3) те, що особі, якій її було надано, була використана зі зловживанням.

Теорія договірного зобов'язання. Обов'язок не розкривати або не використовувати комерційну таємницю виводиться з договірних відносин між правовласником та особою, якій надано доступ до відповідної конфіденційної інформації. Таким чином, захист комерційної таємниці у цьому випадку залежить від договірного застереження про захист конфіденційної інформації.

Теорія довірчих відносин. За цією теорією, окремі види відносин передбачають презюмований обов'язок зберігати секретність. Отже, конфіденційність інформації не залежить від укладення попередньої угоди. Обов'язок не розкривати секретну інформацію випливає не з договору, але з довіри, що покладається володільцем комерційної таємниці на отримувача при передачі конфіденційної інформації.

Теорія неправомірного заволодіння. Цей підхід передбачає, що комерційна таємниця не повинна здобуватись за допомогою недозволених засобів. На відміну від патенту, комерційна таємниця не надає її володільцю абсолютного права використовувати конфіденційну інформацію. Таким чином, вважається, що особа юридично не використовує комерційну таємницю, якщо тільки вона не отримала конфіденційну інформацію неправомірним шляхом.

Теорія недобросовісної конкуренції. Не вирішеним залишається "пропрієтарний" характер комерційної таємниці.

Американські дослідники характеризують комерційну таємницю як об'єкт права власності, виходячи з права володільця комерційної таємниці використовувати та розкривати інформацію третім особам з встановленням обмежень на подальше використання та розкриття. Натомість, англійське право заперечує концепцію права власності стосовно конфіденційної інформації і ґрунтується на праві конфіденційності. У більшості ж правових систем континентальної правової системи це питання розглядається з точки зору практики недобросовісної конкуренції.

Останній підхід виходить зі збереження комерційної етики та основну увагу приділяє поведінці конкурентів.

9. Рекомендована література

1. Білоус Н. М. 06-03-144. Методичні вказівки до проведення практичних заняття виконання самостійної роботи з навчальної дисципліни «Управління захистом комерційної таємниці на підприємстві» для студентів за спеціальністю 073 « Менеджмент ». Рівне : НУВГП. 2018. 23 с.

2. Бондар О. В. Ситуаційний менеджмент. К. : Центр учбової літератури, 2014. 388 с.

3. Іваницька Н. Організаційно-правові засади захисту інформації з обмеженим доступом при укладанні господарських договорів / Бизнес и безопасность. № 4/2010. С. 68–70.

4. Організаційно-правові основи захисту інформації з обмеженим доступом : навчальний посібник / за заг. ред. проф. В. С. Сідака. К. : Вид-во Європейського ун-ту, 2010. 232 с.

5. Марущак А. І. Правові основи захисту інформації з обмеженим доступом : курс лекцій. К. : КНТ, 2011. 208 с.

6. Капіца Ю. Захист комерційної таємниці в Європейських країнах та Україні. 2011. № 11. С. 16 – 20.

7. Сляднева А. О. Определение понятия коммерческой тайны субьекта хозяйствования / Підприємництво, господарство і право. 2014. № 9.

9.1. Інформаційні ресурси

1. Законодавство України. URL : http: // www.rada.kiev.ua.

2. Обласна наукова бібліотека. – м. Рівне, майдан Короленка, 6. URL : / http: // www. library@libr.rv.

3. Наукова бібліотека НУВГП – (м. Рівне, вул. Олекси Новака,75) URL : http: // www.nuwm.edu.ua.