УПРАВЛІННЯ КОМЕРЦІЙНОЮ ТАЄМНИЦЕЮ НА ПІДПРИЄМСТВІ: ДІЇ ОРГАНІЗАЦІЙНОГО, ТЕХНІЧНОГО ТА ПСИХОЛОГІЧНОГО ХАРАКТЕРУ

Сергій Чікін,
доцент НТУУ «Київський політехнічний інститут», кандидат технічних наук
Валентина Черненко,
адвокат, спеціаліст з інтелектуальної власності

У попередній публікації [1] автори розглянули дії правового характеру як елементи управління об'єктом інтелектуальної власності комерційною таємницею та зокрема, прийняття й упровадження таких внутрішніх документів:

1) Положення про комерційну таємницю підприємства.
2) Перелік відомостей, що становлять комерційну таємницю підприємства.

Як один комплекс організаційних дій, що завершують дії правого характеру необхідно розглянути процес розробки та впровадження Положення «Про комерційну таємницю підприємства» та віднесення інформації до комерційної таємниці (див. Рис. 1).

Дія 1. Керівник підприємства видає наказ про призначення відповідальної особи за режим секретності щодо конфіденційної інформації та комерційної таємниці та комісії з питань комерційної таємниці. В цьому наказі можуть бути визначені основні функції комісії. Серед її першочергових завдань: розробка проекту положення про комерційну таємницю, переліку відомостей, що становлять комерційну таємницю, розробка типових документів, що стосуються охорони комерційної таємниці тощо.

Дія 2. На виконання цього наказу комісія готує проект Положення про комерційну таємницю підприємства та направляє його керівництву для затвердження.

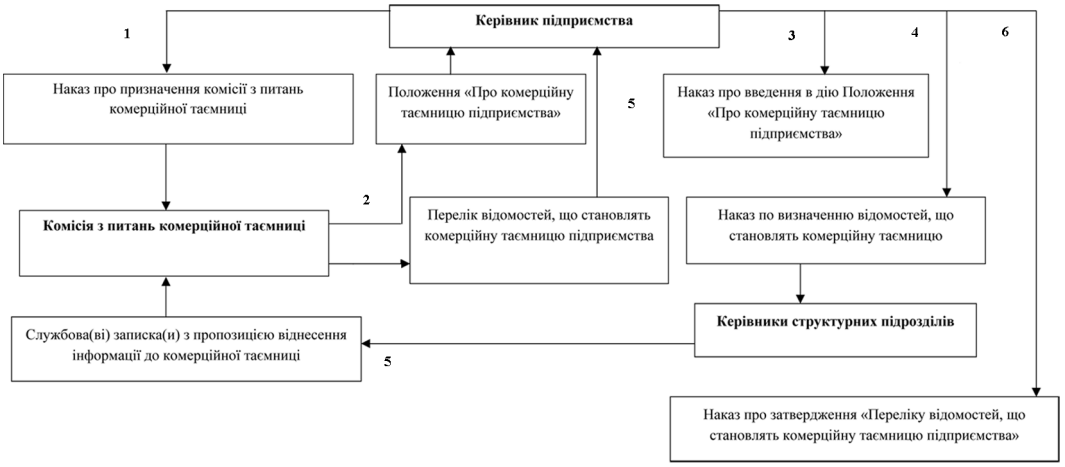

Рисунок 1. Процес віднесення інформації до комерційної таємниці

[*] Закінчення, початок статті у № 4'2011.

У вітчизняному законодавстві відсутні вимоги та регламентації, що стосуються структури та змісту такого Положення. Але, незважаючи на відмінності в сферах діяльності, структурах, кількості працівників і керівного складу підприємств, можна сформулювати 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 послатися на Перелік відомостей, що становлять комерційну таємницю підприємства.

Це може бути: технологічна інформація; відомості про управління підприємством; відомості про фінанси підприємства; відомості про плани підприємства; відомості про виробництво підприємства; відомості про партнерів підприємства; відомості про контракти підприємства; відомості про ціни на підприємстві; відомості про оплату праці на підприємстві; відомості про забезпечення режиму безпеки підприємства; інші відомості, зокрема й і особистого характеру щодо працівників.

Відсутність конкретизації пов'язана з уникненням необхідності переробляти Положення тому, що з часом, у зв'язку, наприклад, з диверсифікацією, може виникнути необхідність віднесення до комерційної таємниці інших видів інформації.

У разі необхідності, в Положенні може бути визначено право підприємства встановлювати особливі режими доступу до певної інформації на підставі певних положень.

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.

Якщо вищезазначені типові документи не будуть обумовлені в положенні, їх необхідно впроваджувати окремим наказом керівника підприємства.

Дія 3 і 4. Керівник підприємства видає накази:

- про затвердження та впровадження на підприємстві Положення про комерційну таємницю підприємства та порядку ознайомлення з ним;
- про визначення відомостей, що становлять комерційну таємницю.

Безпосередніми виконавцями останнього наказу зазвичай є комісія з питань комерційної таємниці та керівники структурних підрозділів.

Дія 5. На виконання цього наказу керівники структурних підрозділів надають комісії з питань комерційної таємниці службові записки з обґрунтованим переліком інформації, щодо якої доцільно обмежити доступ та/або віднести до комерційної таємниці. У службовій записці має бути пропозиція щодо переліку осіб, яким не-

обхідно надати дозвіл на доступ до цієї інформації.

Комісія повинна проаналізувати можливі збитки від розголошення визначених відомостей. Залежно від можливих збитків визначається режим секретності інформації. Крім цього, комісії слід взяти до уваги можливе зниження ефективності діяльності підприємства у зв'язку з обмеженням доступу до інформації. з огляду на все вищезгадане, комісія формує Перелік.

Підготовлений комісією перелік відомостей, що становлять комерційну таємницю підприємства, надається на затвердження керівництву підприємства.

Дія 6. Керівник підприємства видає наказ про затвердження Переліку відомостей, що становлять комерційну таємницю підприємства та введення його в дію. З цим наказом мають бути ознайомлені під підпис всі співробітники, допущені до роботи з інформацією, що визначена як комерційна таємниця.

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.

Потрібно пам'ятати, що вищезазначені дії є необхідними для віднесення інформації до комерційної таємниці, але далеко не достатніми. Так, наприклад, у Постанові Вищого господарського суду України № 12/197(05-5-12/10264-А) від 12.02.2008 року у справі, котра стосується порушення прав на комерційну таємницю, зокрема, зазначається, що, крім віднесення інформації «ААА» до інформації для службового користування, не були надані докази щодо «вжиття передбачених законом заходів щодо визначення відомостей "ААА" такими, які становлять комерційну таємницю.., і встановлення порядку захисту цих відомостей», а також «не підтверджено статусу відомостей "ААА" як комерційної таємниці». З наведеного можна дійти висновку про необхідність вжиття додаткових заходів щодо віднесення інформації до комерційної таємниці.

За даними експертів ЄС, що наведені, наприклад, у роботі [2], основні причини витоку конфіденційної інформації можуть зумовлюватися зов-

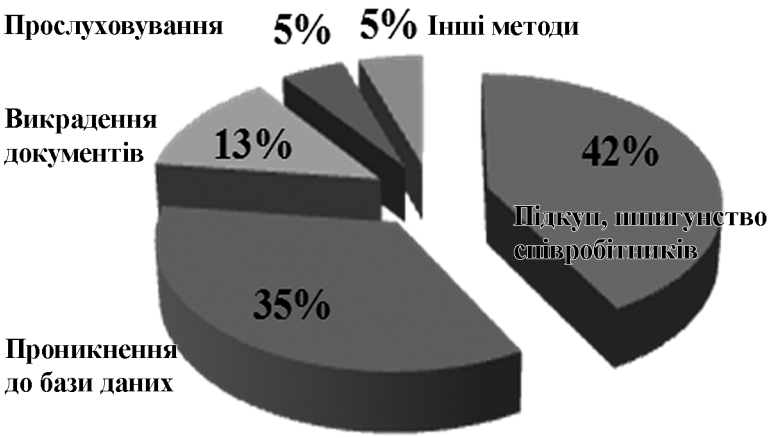

Рисунок 2. Зовнішні чинники, що сприяють витоку інформації

нішніми (див. Рис. 2) та внутрішніми (див. Рис. 3) чинниками.

Як бачимо, комплекс дій із забезпечення нерозголошення інформації, передусім, має бути спрямований на персонал підприємства, на забезпечення захисту баз даних, документації та контроль за їх використанням. Усе це зумовлює вжиття певних дій організаційного, технічного і психологічного характеру.

До **інших дій організаційного характеру** належать такі:

1. Створення режимно-секретного підрозділу з функціями підтримки і контролю за дотриманням встановленого режиму секретності (за доцільності, з огляду на кількісний склад працівників підприємства), діяльність якого визначається відповідними інструкціями, положеннями чи наказами.

Наявність охоронця на вході в підприємство не вирішує повною мірою питань інформаційної безпеки підприємства. Безумовно, що це сприятиме обмеженню доступу в службові приміщення сторонніх осіб і зменшить ризик випадкового розкриття конфіденційної інформації чи комерційної таємниці. Залучення до здійснення функцій режимно-секретного підрозділу спеціалізованих сторонніх організацій пов'язане з необхідністю розкривати перед нею певну частку своїх секретів (не знаючи, що охороняти, неможливо побудувати ефективну систему охорони) та слабкою мотивацією співробітників цієї організації на досягнення цілей саме вашого підприємства. Варто пам'ятати, що залучення до забезпечення інформаційної безпеки підприємства сторонніх осіб-консультантів може бути ефективним тільки на початкових етапах: розробка, впровадження. Подальша підтримка та контроль за функціонуванням має здійснюватися штатним співробітником підприємства.

Не кожне підприємство, що володіє комерційною таємницею, може собі дозволити мати додатковий штат співробітників режимно-секретного підрозділу. В цих випадках, як мінімум, доцільно призначити особу, відповідальну за здійснення необхідних дій. Цілком зрозумілим є те, що здійснення таких функцій вимагає необхідних теоретичних і практичних знань, на формування та підтримку яких також мають бути спрямовані дії підприємства.

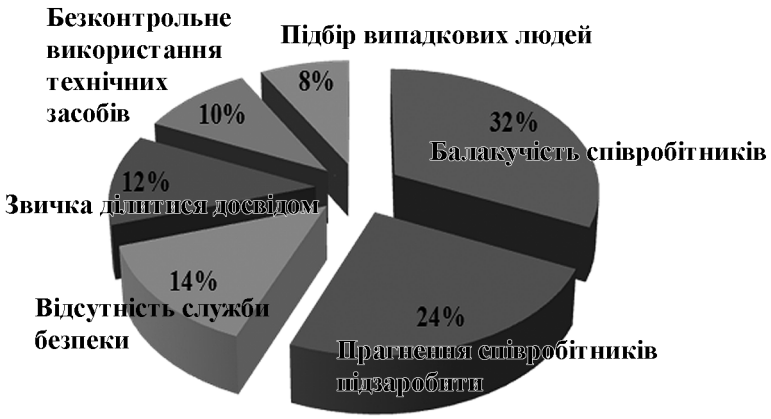

Рисунок 3. Внутрішні чинники, що сприяють витоку конфіденційної інформації

Як основні функції режимно-секретного підрозділу доцільно визначити такі [3]:

- 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.

2. Розробка дозвільної системи доступу до інформації.

За оцінками вітчизняних і зарубіжних фахівців [2; 3; 4] головним джерелом витоку конфіденційної інформації є персонал підприємства. При цьому його дії, здебільшого, мають **свідомий** характер. Вони можуть бути зумовлені, наприклад, бажанням помститися за несправедливість з боку керівництва, корисливими мотивами тощо.

Тож для підприємства вкрай важливим є зафіксувати персональну відповідальність співробітників за доручену їм комерційну таємницю. Здійснюється це через оформлення допуску до комерційної таємниці при прийнятті на роботу чи переведенні на відповідну посаду.

Усвідомлення співробітником можливості покарання за розголошення комерційної таємниці відіграє важливу роль у профілактиці її витоку.

В основу створення системи допуску можуть бути покладені відповідні положення Закону України «Про державну таємницю», які мають бути адаптовані до захисту комерційної таємниці.

Відповідно до ст. 1 Закону України «Про державну таємницю» [5]:

- допуск до державної таємниці — оформлення права громадянина на доступ до секретної інформації;
- доступ до державної таємниці — надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, чи ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Отож, під допуском до комерційної таємниці потрібно розуміти письмове розпорядження керівника підприємства, що дає конкретному співробітникові право на ознайомлення чи роботу з інформацією, що становить комерційну таємницю.

Процедуру надання допуску можна рекомендувати здійснювати так [3]:

- визначення потреби співробітника в конфіденційній інформації при виконанні ним службових обов'язків;
- перевірку співробітника у зв'язку з допуском до комерційної таємниці;
- ознайомлення співробітника з мірою відповідальності за порушення законодавства про незаконне збирання, поширення та використання комерційної таємниці;
- оформлення письмового 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.

У разі звільнення співробітника, який був допущений до комерційної таємниці, від нього відбирається 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 співробітника, що звільняється, комерційної таємниці і 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:

- для конфіденційної інформації — гриф «Для службового користування» (або «ДСК»);
- для різних режимів секретності (за необхідності) комерційної таємниці:
  - гриф «Для службового користування. Комерційна таємниця — секретно» (або «ДСК: КТ-С»);
  - гриф «Для службового користування. Комерційна таємниця — суворо секретно» (або «ДСК: КТ-СС»);
  - гриф «Для службового користування. Комерційна таємниця — особливо секретно» (або «ДСК: КТ-ОС») тощо.

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

4. Організація секретного діловодства.

Залежно від видів інформації, що визначеної як комерційна таємниця, та її обігу в цілях ефективної діяльності підприємства здійснюються різні дії щодо організації секретного діловодства. Та серед мінімально необхідних слід передбачити такі [3]:

- облік документів або носіїв інформації, що має гриф «КТ»;
- забезпечення збереження носіїв інформації, що має гриф «КТ»;
- встановлення порядку роботи з документами чи носіями інформації, що має гриф «КТ»;

(На прохання одного з авторів цієї публікації до співробітників організації, яка працює виключно з конфіденційною документацією інших осіб, описати свої дії впродовж останніх 15 хвилин робочого дня, жоден не згадав про повернення документів на зберігання. Чи дотримується в цій організації порядок роботи з конфіденційними документами? Питання риторичне).

- встановлення порядку розсилки документів або носіїв інформації, що має гриф «КТ» тощо.

Дії **технічного характеру** щонайменше можна поділити на ті, що спрямовані на захист:

- приміщень підприємства та
- інформаційних мереж.

Це щонайменше:

- виявлення можливих джерел витоку конфіденційної інформації, у зокрема й і комерційної таємниці;

- встановлення спеціального обладнання та/або програмних засобів для захисту інформації;
- встановлення спеціального обладнання для спостереження за приміщеннями організації;
- проведення регулярних оперативних заходів з технічного захисту та пошуку каналів витоку інформації.

Зважаючи специфіку дій технічного характеру, вони в цій публікації детально обговорюватися не будуть.

Серед **дій психологічного характеру** варто виокремити наведені нижче:

1. Проведення роз'яснювальної роботи з персоналом, партнерами та клієнтами.

Як заходи, що підвищують мотивацію персоналу на охорону та не розголошення комерційної таємниці підприємства, потрібно розглядати роз'яснювальну роботу, спрямовану на усвідомлення важливості для підприємства віднесення певної інформації до комерційної таємниці та наслідків від її розголошення. Потужним стимулювальним фактором є усвідомлений працівником зв'язок між наявною на підприємстві комерційною таємницею та розміром щомісячної винагороди за свою працю. Усе це має сприяти надійності захисту комерційної таємниці.

Та не менш потужним стимулом є усвідомлення відповідальності за порушення прав на комерційну таємницю.

Законодавством України передбачена дисциплінарна, цивільно-правова, адміністративна чи кримінальна відповідальність за порушення прав на комерційну таємницю.

Дисциплінарна відповідальність. За порушення встановленого на підприємстві порядку захисту комерційної таємниці до працівника можуть застосовуватися дисциплінарні стягнення.

Підставою для їх застосування є ст. 147 КЗпП України [6], колективний договір, правила внутрішнього трудового розпорядку, Положення про комерційну таємницю інші внутрішні документи.

Відповідно до статті 147 КЗпП України [6] за порушення трудової дисципліни до працівника може бути застосовано один з таких заходів стягнення:

- догана;
- звільнення.

Водночас внутрішніми документами можуть бути передбачені й інші заходи впливу за порушення трудової дисципліни, наприклад: переведення на іншу роботу, не пов'язану з допуском до комерційної таємниці; позбавлення премій за результатами роботи; зміна часу надання чергової відпустки.

Цивільно-правова відповідальність. Згідно з ч. 3 ст. 162 ГК України [7] особа, яка протиправно використовує комерційну інформацію, що належить суб'єкту господарювання, зобов'язана відшкодувати завдані йому такими діями збитки відповідно до закону.

Якщо право суб'єкта господарювання на комерційну таємницю порушено у межах укладеного договору, а саме, особою, що одержала доступ до комерційної таємниці на підставі договору, то застосовуються цивільно-правові норми про відповідальність за порушення зобов'язань (глава 51 ЦК України [8]). У разі порушення цього права в позадоговірних зобов'язаннях особою, що одержала незаконним шляхом доступ до комерційної таємниці, слід застосовувати норми про зобов'язання щодо відшкодування шкоди (глава 82 ЦК України [8]).

Згідно зі ст. 22 ЦК України [8], особа, якій завдано збитків у результаті порушення її цивільного права, має право на їх відшкодування.

При визначенні збитків від порушення прав на комерційну таємницю враховуються не тільки прямі збитки, але й упущена вигода.

Адміністративна відповідальність. Відповідно до ч. 3 ст. 164-3 КУпАП [9] отримання, використання, розголошення комерційної таємниці, а

також конфіденційної інформації з метою заподіяння шкоди діловій репутації чи майну іншого підприємця — тягне за собою накладення штрафу від 9 до 18 неоподатковуваних мінімумів доходів громадян.

Крім цього, адміністративна відповідальність за ті ж злочини передбачена Законом України «Про захист від недобросовісної конкуренції» [10], а саме:

- за неправомірне збирання комерційної таємниці (ст. 16);
- за розголошення комерційної таємниці (ст. 17);
- за схилення до розголошення комерційної таємниці (ст. 18);
- за неправомірне використання комерційної таємниці (ст. 19).

Усі перераховані правопорушення є недобросовісною конкуренцією, за яку законом передбачена відповідальність.

Згідно зі ст. 22 Закону України «Про захист від недобросовісної конкуренції» [10], вчинення суб'єктами господарювання дій, визначених цим Законом як недобросовісна конкуренція, тягне за собою накладення штрафу в розмірі до 5 % від доходу (виручки) від реалізації продукції (товарів, робіт, послуг) суб'єкта господарювання за останній звітний рік, що передував року, в якому накладається штраф.

Якщо доходу (виручки) немає чи відповідач на вимогу органів Антимонопольного комітету України, голови його територіального відділення не надав відомостей про розмір доходу (виручки), штраф, передбачений ч. 1 ст. 22 цього Закону, накладається у розмірі до 10 000 неоподатковуваних мінімумів доходів громадян.

Кримінальна відповідальність. За порушення прав на комерційну таємницю передбачена кримінальна відповідальність.

Відповідно до ст. 231 КК України [11] умисні дії, спрямовані на отримання відомостей, що становлять комерційну чи банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це завдало істотної шкоди суб'єкту господарської діяльності, караються штрафом від 200 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до 5 років, або позбавленням волі на строк до 3 років.

Згідно зі ст. 232 КК України [11], умисне розголошення комерційної чи банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною чи службовою діяльністю, якщо воно вчинене з корисливих або інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, карається штрафом від 200 до 500 неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років, або виправними роботами на строк до 2 років, або позбавленням волі на той самий строк.

2. Створення сприятливої атмосфери в колективі. Бізнес-розвідники давно зробили для себе висновки про особисті якості співробітників, здатних до розкриття своїх і чужих секретів. Легше за всіх на це йдуть особи емоційно нестійкі, з низькою чи завищеною самооцінкою, розчаровані у своїх здібностях, невдоволені своїм службовим або матеріальним положенням, хвалькуваті, брехливі, егоїстичні тощо.

Часткові ці фактори можуть бути нейтралізовані на стадії надання дозволу на допуск до комерційної таємниці. Але і створення в колективі атмосфери товариства, взаємопідтримки і, водночас, нетерпимості до порушень, здатне сприяти нерозголошенню конфіденційних відомостей.

Осуд з боку співробітників однакового рівня може бути більш дієвим, ніж з боку керівництва.

3. Проведення регулярних перевірок (гласних або негласних) з ви-

явлення неблагонадійних осіб. Безумовним психологічно стимулювальним фактором є усвідомлення підконтрольності дій. Співробітник має усвідомлювати необхідність контролю як обов'язкового елементу будь-якої системи управління. Несприйняття співробітником контрольних дій може породжувати питання щодо доцільності надання йому доступу.

4. Доведення до всіх працівників, які мають доступ до комерційної таємниці, результатів перевірок і прийнятих заходів упливу щодо виявлених порушників. У такому сенсі «гласність» не суперечить секретності, що завжди пов'язана з комерційною таємницею. Демонстрація ефективності системи захисту комерційної таємниці є важливим психологічним стимулом, що сприяє її не розголошенню.

Розглянуті в цій публікації дії не є вичерпними, тому що залежать від багатьох внутрішніх факторів конкретного підприємства.

Автори цієї публікації сподіваються на те, що сприйняття комерційної таємниці як об'єкта управління, надасть підприємству можливість здійснити необхідний комплекс дій, пов'язаних з нею, і таким чином надійно її захистити. ◆

Список використаних джерел

1. *Чікін С. Управління комерційною таємницею на підприємстві: дії правового характеру / С. Чікін, В. Черненко // Теорія і практика інтелектуальної власності. — 2011. — № 4. — С. 56–61.*
2. *Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны [Текст] : монография / Г. А. Андрощук, П. П. Крайнев. — К. : Ин Юре, 2000. — 400 с.*
3. *Зеркалов Д. В. Защита : хрестоматия / Д. В. Зеркалов. — К. : Наук. світ, 2008. — 159 с. — (Безопасность бизнеса : в 4 кн. ; кн. 4).*
4. *Комерційна таємниця [Електронний ресурс]. — Режим доступу до ресурсу : http://jus.org.ua/glava-13-kommercheskaya-tajna.*
5. *Закон України «Про державну таємницю» № 3856-XII від 21.01.1994 року (зі змінами) // ВВР. — 1994. — № 16. — Ст. 94.*
6. *Кодекс законів про працю України № 322-VIII від 10.12.1971 року (зі змінами і доповненнями) // ВВР. — 1971. — додаток до № 50. — Ст. 375.*
7. *Господарський кодекс України № 436-IV від 16.01.2003 року (зі змінами) // ВВР. — 2003. — № 18, № 19–20, № 21–22.*
8. *Цивільний кодекс України № 435-IV від 16.01.2003 року (зі змінами) // ВВР. — 2003. — № 40.*
9. *Кодекс України про адміністративні правопорушення [Електронний ресурс]. — Режим доступу до ресурсу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80731-10.*
10. *Закон України «Про захист від недобросовісної конкуренції» № 237/96-ВР від 07.06.1996 року (зі змінами) // ВВР. — 1996. — № 36. — Ст. 164.*
11. *Кримінальний кодекс України № 2341-III від 05.04.2001 року (зі змінами) // ВВР. — 2001. — № 25–26. — Ст. 131.*