УДК 65.012.8

А.А. Атабаєва, магістр,
С.П. Голубенко, бакалавр,
Одес. нац. політехн. ун-т

ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ АСПЕКТИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПІДПРИЄМСТВА В УМОВАХ ФУНКЦІОНУВАННЯ СИСТЕМИ ВНУТРІШНЬОГО ЕКОНОМІЧНОГО КОНТРОЛЮ

А.А. Атабаєва, С.П. Голубенко. **Організаційно-методичні аспекти захисту комерційної таємниці підприємства в умовах функціонування системи внутрішнього економічного контролю.** Сформовано перелік інформації, що входить до складу комерційної таємниці. Розроблено класифікацію комерційної таємниці за функціонально-цільовою ознакою та класифікацію способів несанкціонованого доступу до неї, що дозволило запропонувати заходи запобігання розповсюдженню даної інформації.

А.А. Атабаева, С.П. Голубенко. **Организационно-методические аспекты защиты коммерческой тайны предприятия в условиях функционирования системы внутреннего экономического контроля.** Сформирован перечень информации, входящей в состав коммерческой тайны. Разработаны классификация коммерческой тайны по функционально-целевому признаку и классификация способов несанкционированного доступа к ней, что позволило предложить меры предотвращения распространения данной информации.

A.A. Atabayeva, S.P. Golubenko. **Organizational and methodical aspects of an enterprise trade secret protection in conditions of internal economical control system functioning.** The list of information involved in the trade secret content is formed. The classification of trade secret by the functional-target indication, and the classification of methods of unauthorized access to it, are developed, which allowed to propose measures to prevent this information spreading.

Економічні і політичні зміни в Україні, які відбуваються протягом розвитку ринкових відносин, зумовлюють загострення конкурентної боротьби. До інструментів, що спроможні забезпечити високий рівень конкурентоспроможності суб'єкта господарювання, прийнято відноси-

ти сертифіковані системи менеджменту, системи внутрішнього економічного контролю (СВЕК) тощо. Але одним з основних завдань забезпечення дієвості СВЕК є встановлення меж розповсюдження комерційної інформації.

Дане питання розглядалось багатьма авторами, які приділяли увагу програмам та способам захисту комерційної таємниці (КТ), економічної безпеки та безпеки підприємництва [1, 2]. Однак основна увага авторів зосереджена на проблемах правового захисту. Сучасні умови конкуренції та ведення підприємницької діяльності в країні потребують комплексного підходу до зберігання КТ, основою якого є організаційні заходи. Для їх реалізації першочергово необхідно визначити, за якими критеріями інформація набуває статусу КТ. Аналіз Цивільного кодексу України, Господарського кодексу, закону України "Про інформацію" дозволив виділити такі ознаки відомостей, що підпадають під термін "комерційна таємниця":

— вони пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства;

— є секретними, невідомими та не є легкодоступними суспільству;

— мають істотну або комерційну цінність;

— щодо їх захисту та збереження секретності підприємство вживає певних заходів;

— не є державною таємницею;

— не повинні підпадати під дію постанови Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці".

Конкретний склад та обсяг відомостей, що становлять КТ, порядок їх захисту визначаються самостійно власником або керівником підприємства. Отже, наступним за етапом визначення дефініції "комерційна таємниця", доречним буде складання повного переліку інформації, що містить КТ, та встановлення організаційних засад її захисту.

Організацію захисту КТ доцільно покладати на СВЕК [3, 4]. В цьому випадку визначиться центр відповідальності за вихід та розповсюдження інформації — відділ, відповідальний за функціонування СВЕК на підприємстві. До функцій та завдань СВЕК доцільно ввести такі положення: ідентифікацію суб'єктів та об'єктів інформації, що становить КТ; опрацювання внутрішньогосподарської розпорядчої документації (Статут, Установчий договір, Колективний договір, Правила внутрішнього трудового розпорядку, положення ″Про комерційну таємницю та правила її збереження″, положення ″Про дозвільну систему доступу виконавців до документів і відомостей, які є комерційною таємницею підприємства″, положення про структурний підрозділ, посадові інструкції) на предмет встановлення правового статусу інформації та визначення порядку її збереження в носіях.

Процес збереження інформації в документах, що містять КТ, повинен здійснюватися у відповідності з основними стадіями ″життєвого циклу″ документа. Цими стадіями є:

— отримання (відправлення) документа. Документ, що надходить у фірму і містить гриф конфіденційної інформації, повинен бути переданий тільки секретарю-референту або інспектору закритого діловодства та зареєстрований. Далі він передається керівнику, а останній визначає безпосереднього виконавця за цим документом, що має допуск до цієї категорії документів, і адресує документ йому. Подібні заходи безпеки й при відправленні документа — підготовка документа, підпис керівника, реєстрація в спеціальному журналі секретарем-референтом і відправлення;

— зберігання документа. Всі документи, які містять конфіденційну інформацію, повинні зберігатися у спеціально відведених закритих приміщеннях у замкнених шафах, столах або шухлядах. Документи ж, що становлять КТ, — тільки в металевих сейфах, обладнаних сигналізацією. Усі приміщення повинні опечатуватися;

— використання документа. Система доступу співробітників, які не мають відповідних прав за посадою, до конфіденційних документів повинна мати дозвільний характер. Кожна видача таких документів реєструється (розписуються обидва співробітники — і той, хто бере документ, і той хто, його видає) і перевіряється порядок роботи з ними.

— знищення документа. Конфіденційні документи, що втратили практичне значення і не мають якої-небудь правової, історичної чи наукової цінності, термін зберігання яких минув, підлягають знищенню. Для цього створюється комісія (не менше трьох осіб), у присутності якої здійснюється знищення. Потім члени комісії підписують акт про знищення [5].

Однак, окрім документів, важливим об'єктом захисту є інформація в комп'ютерних базах даних. У цій сфері одним із простих та ефективних методів є застосування системи управління доступом до пристроїв входу/виходу інформації на серверах і робочих станціях. Основними завданнями цієї системи є розроблення моделі системи захисту інформації; блокування доступу персоналу до пристроїв входу/виходу інформації на основі затвердженої матриці доступу; реєстрація випадків копіювання інформації персоналом, який має відповідні повноваження; авторизація носіїв інформації для запобігання підключення невідомих пристроїв; кодування даних на зовнішніх носіях.

Невід'ємною частиною організації ефективного захисту економічної безпеки фірми є робота з персоналом при прийомі на роботу. На цьому етапі здійснюється укладення (підписання) двох документів:

трудового договору (контракту). Контракт обов'язково повинен містити пункт про обов'язок працівника не розголошувати КТ і дотримуватися заходів безпеки;

договору (зобов'язання) про нерозголошення КТ, що являє собою правовий документ, в якому кандидат на вакантну посаду дає обіцянку не розголошувати ті відомості, які йому будуть відомі в період його роботи у фірмі, а також про відповідальність за їх розголошення або недотримання правил безпеки [6].

Всі працівники, що мають справу з конфіденційною інформацією, мають право знайомитися з останньою тільки в тому обсязі, який передбачено їх посадовими обов'язками, потрібен для професійного і добросовісного виконання своїх функцій (обсяг встановлюється керівником фірми або спеціальною комісією). З огляду на це можна скласти орієнтовну таблицю відповідності суб'єктів — одержувачів КТ, які мають ту чи іншу можливість доступу до інформації, об'єкта КТ, поділених за функціонально-цільовою ознакою (табл. 1).

Таким чином, до першочергових організаційних заходів захисту інформації, що становить КТ суб'єкта господарювання, потрібно віднести:

— визначення вичерпного переліку користувачів інформації, класифікованого за групами (див. таблицю 1);

— встановлення умов (передумов) допуску до інформаційного масиву як внутрішніх, так і зовнішніх суб'єктів КТ. При цьому необхідно враховувати, що підписання суб'єктами державного фінансового контролю (ДФК) документа про нерозголошення інформації [5] в Україні є необгрунтованим та протиправним, і може розцінюватися як дії, що перешкоджають процесу перевірки (згідно із ст. 12 закону України "Про державну контрольно-ревізійну службу" та ст. 14 закону України "Про Рахункову палату");

— встановлення центру відповідальності за розповсюдження інформації, в тому числі тієї, що становить КТ. Прикладом організації діяльності подібних центрів може стати досвід суб'єктів господарювання США та Франції [7];

— встановлення міри відповідальності за розголошення інформації, що становить КТ.

Серед основних завдань центру відповідальності за розповсюдження інформації слід виділити оперативне та обгрунтоване визначення джерел витоку КТ. Основним інструментом пропонується використовувати наведену класифікацію способів несанкціонованого доступу до КТ з відповідними джерелами витоку та способами запобігання (табл. 2). Під джерелом витоку КТ мається на увазі об'єкт, що має певні відомості, які охороняються та представляють інтерес для зловмисників.

В контексті запропонованої класифікації (див. таблицю 2) доцільно встановити міру відповідальності за витік інформації, що становить КТ. За незаконні дії щодо розголошення комерційної інформації передбачені дисциплінарна і цивільно-правова, адміністративна, кримінальна відповідальності.

Згідно з Кримінальним кодексом України (ККУ) за розголошення КТ особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, — Джерело "Люди" за таблицею 2 — накладається штраф від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправні роботи на строк до двох років, або позбавлення волі на той самий строк (ст. 232 ККУ).

Таблиця 1

Класифікація КТ за функціонально-цільовою ознакою та відповідні суб'єкти КТ

Об'єкт КТ	Суб'єкт КТ**	Зовнішні суб'єкти КТ	
		Мають право	Не мають права
Ділова інформація (відомості про контрагентів; відомості про споживачів; відомості про ділові переговори; відомості про укладені та заплановані контракти та ін.*)	Директор, заст. директора, підрозділ збуту, маркетингова служба, служба закупівлі	— Служба безпеки України (ст. 25 закону України "Про Службу безпеки України"). — Органи, які здійснюють оперативно-розшукову діяльність (ст. 8 закону України "Про оперативно-розшукову діяльність"). — Органи, які ведуть боротьбу з організованою злочинністю (ст. 12 закону України "Про організаційно-правові основи боротьби з організованою злочинністю"). — Міністерство внутрішніх справ (ст. 11 закону України "Про міліцію"). — Державна податкова служба (ст. 11 закону України "Про державну податкову службу в Україні"). — Органи Державної контрольно-ревізійної служби (ст. 10 закону України "Про державну контрольно-ревізійну службу в Україні"). — Антимонопольний комітет України (ст. 16 закону України "Про Антимонопольний комітет України"). — Органи дізнання та органи попереднього слідства (ст. 66 Кримінально-процесуального кодексу України). — Органи прокуратури України (ст. 8 закону України "Про прокуратуру"). — Державна комісія з цінних паперів та фондового ринку України (ст. 8 закону України "Про державне регулювання ринку цінних паперів в Україні"). — Аудитори (ст. 19 закону України "Про аудиторську діяльність").	— Суб'єкти промислового шпигунства — Кримінальні структури — Фірми-розвідники — Конкуренти — Інші зовнішні зацікавлені особи
Науково-технічна інформація (зміст і плани науково-дослідних робіт; зміст "ноу-хау"; плани впровадження нових технологій і видів продукції та ін.*)	Директор, заст. директора, виробничий підрозділ, науково-дослідний відділ		
Виробнича інформація (технологія; плани випуску продукції; плани інвестиційної діяльності та ін.*)	Директор, заст. директора, підрозділ збуту, виробничий підрозділ, служба закупівлі, науково-дослідний відділ		
Організаційно-управлінська інформація (відомості про структуру управління фірмою, що не містяться в статуті; оригінальні методи організації управління та ін.*)	Директор, заст. директора, кадрова служба		
Маркетингова інформація (ринкова стратегія; плани рекламної діяльності; методи роботи на ринках; плани збуту продукції та ін.*)	Директор, заст. директора, маркетингова служба, підрозділ збуту		
Фінансова інформація (планування прибутку, собівартості; ціноутворення; можливі джерела фінансування та ін.*)	Директор, заст. директора, фінансово-економічна служба		
Інформація про персонал фірми (особисті справи співробітників; плани збільшення (скорочення) персоналу та ін.*)	Директор, заст. директора, кадрова служба		
Програмне забезпечення (програми; паролі, коди доступу до конфіденційної інформації, розташованої на електронних носіях та ін.*)	Директор, заст. директора, інформаційно-аналітична служба		

* склад і обсяг КТ визначається самостійно власником;

** можливий інший розподіл функціональних відділів і передача інформації різним співробітникам при необхідності

Таблиця 2

Класифікація способів несанкціонованого доступу до комерційної таємниці

Способи несанкціонованого доступу до КТ	Джерело витоку КТ	Мотив*	Спосіб запобігання несанкціонованому доступу
Ініціативне співробітництво	Люди	Фінансові труднощі, невдоволення просуванням по службі, образи від начальства і влади та ін.	Підписання договору (зобов'язання) про нерозголошення комерційної таємниці; обмеження допуску до конфіденційної інформації; проведення превентивних та поточних заходів, спрямованих на роботу з кадрами (їх виховання, заохочення), партнерами, клієнтами та ін.
Схилення до співпраці	Люди	Підкуп, заляку-вання, шантаж	
Випитування, вивідування (інтерв'ювання)	Люди, публікації	Бажання показати себе значущим суб'єктом, випадкове виказування	
Прослуховування переговорів різними шляхами	Люди, технічні засоби	—	Обмеження допуску до конфіденційної інформації; перевірка апаратури на наявність сторонніх пристроїв; процедури аутентифікації абонентів і повідомлень; шифрування і спеціальні протоколи зв'язку та ін.
Спостереження	Люди, технічні носії, технічні засоби	—	Обмеження допуску до конфіденційної інформації; розробка правил користування інформацією; перевірка апаратури на наявність сторонніх пристроїв та ін.
Розкрадання	Люди, документи, технічні носії, технічні засоби, продукція, промислові та виробничі відходи	—	Обмеження допуску до конфіденційної інформації; розробка правил користування інформацією; охорона, пропускний режим, спеціальні картки для сторонніх, використання закритих приміщень, сейфів; застосування імуностійких і захисних програмних засобів; парольний захист комп'ютерних систем; контроль за утилізацією відходів тощо
Копіювання	Документи, технічні носії, продукція	—	Розробка правил користування інформацією; охорона, пропускний режим, спеціальні картки для сторонніх, використання закритих приміщень, сейфів; застосування імуностійких і захисних програмних засобів та ін.
Підробка (модифікація, фальсифікація)	Документи, технічні засоби, продукція	—	Розробка правил користування інформацією; охорона, пропускний режим, спеціальні картки для сторонніх, використання закритих приміщень, сейфів; застосування імуностійких і захисних програмних засобів; парольний захист комп'ютерних систем; контроль за фірмовим знаком і стилем та ін.
Знищення (псування)	Люди, документи, технічні носії, технічні засоби, продукція	—	Обмеження допуску до конфіденційної інформації; розробка правил користування інформацією; охорона, пропускний режим, спеціальні картки для сторонніх, використання закритих приміщень, сейфів; застосування імуностійких і захисних програмних засобів; парольний захист комп'ютерних систем та ін.

* для джерела "Люди"

Щодо незаконного збирання з метою використання (комерційне шпигунство) або використання відомостей, що становлять КТ, на протидію чому й направлена запропонована класифікація способів несанкціонованого доступу до КТ, передбачено штраф від двохсот до тисячі неоподатковуваних мінімумів доходів громадян, або обмеження волі на строк до п'яти років, або позбавлення волі на строк до трьох років (ст. 231 ККУ).

Підводячи підсумки, необхідно ще раз підкреслити, що в умовах загострення конкурентної боротьби особливого значення набуває створення комплексної системи збереження комерційної таємниці на підприємстві, яка зможе об'єднати існуючі шляхи захисту в єдиний механізм та надасть підприємству впевненість в захищеності його інтересів. Основою такої системи є організаційні методи захисту суб'єктів господарювання. З огляду на це, визначено зміст комерційної таємниці, що стало підґрунтям формування переліку інформації, що входить до її складу, та подальшої класифікації КТ за функціонально-цільовою ознакою. Запропоновано класифікацію способів несанкціонованого доступу до КТ та методи його запобігання. Наведені класифікації можуть бути використані під час розробки внутрішньогосподарських методичних положень захисту інформації, що становить комерційну таємницю.

Література

1. Нікіфоров, Г.К. Підприємництво та правовий захист комерційної таємниці: навч.-практ. посіб. для ВНЗ / Г.К. Нікіфоров, С.С. Нікіфоров. — К.: Олан, 2001. — С. 57 — 66.
2. Андрощук, Г.А. Экономическая безопасность предприятия: защита коммерческой тайны: моногр. / Г.А. Андрощук, П. П. Крайнев. — К.: Ин Юре, 2000. — С. 254 — 272.
3. Атабаєва, А.А. Класифікаційна модель внутрішнього економічного контролю підприємства як основа формування його змісту / А.А. Атабаєва // Тр. Одес. политехн. ун-та. — Одесса, 2009. — Вып. 1(31). — С. 208 — 211.
4. Атабаєва, А.А. Система внутрішнього контролю як об'єкт оцінки рівня аудиторського ризику системно-орієнтованого аудиту / А.А. Атабаєва // Матеріали Міжнар. наук.-практ. конф., м. Кривий Ріг, 4 груд. 2009 р.: тези доп. — Кривий Ріг: Видавн. дім, 2009. — С. 127 — 128.
5. Шлыков, В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. — СПб: Алетейя, 1999. — С. 78 — 82.
6. Іванюта, Т.М. Економічна безпека підприємства: навч. посіб. для студ. ВНЗ / Т.М. Іванюта, А.О. Заїчковський. — К.: Центр учб. л-ри, 2009. — С. 138 — 165.
7. Іващенко, В. Основи методики розслідування незаконного збирання та розголошення комерційної таємниці / В. Іващенко // Юрид. журн. — 2006. — № 8. — С. 32 — 35.

Рецензент канд. техн. наук, доц. Одес. нац. політехн. ун-ту Шаповал С.С.

Надійшла до редакції 26 березня 2010 р.