



УДК 336

*О. В. Черевко,
д. е. н., доцент, Голова спостережної ради ПАТ «Банк «Київська Русь»*

ЗАБЕЗПЕЧЕННЯ РЕЖИМУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ВСЕРЕДИНИ ПІДПРИЄМСТВА

*A. Cherevko,
Ph.D., Associate Professor,
Chairman of the Supervisory Board of PJSC "Bank" Kievan Rus "*

PROVIDING THE TRADE SECRETS WITHIN THE COMPANY

Стаття присвячена питанням встановлення правового режиму комерційної таємниці на підприємстві. Визначено основні нормативні документи, котрі даються визначення поняттю «комерційна таємниця» Розглянуто процедуру введення правового режиму комерційної таємниці на підприємстві. А також вказані заходи по забезпеченню збереження конфіденційної інформації на підприємстві.

Article is devoted to establishing the legal regime of trade secrets in the enterprise. The basic regulations that given the definition of "trade secret" The procedure entry legal regime of trade secrets in the enterprise. Also listed measures to ensure the preservation of confidential information in the enterprise.

Ключові слова: безпека бізнесу, інформаційна безпека, комерційна таємниця, рівень секретності, документообіг.

Keywords: business security, information security, trade secret, privacy level, document management.

Постановка проблеми. Проблеми збереження своїх технологічних секретів життєво важливі для підприємств різних галузей і форм власності. Збереження комерційної таємниці в недоторканності - одна з головних передумов збереження та успішного розвитку бізнесу в майбутньому. Однак це - лише загальний посыл, ринкова аксіома, без конкретного наповнення організаційно-управлінськими заходами, без заданих алгоритмів і планів дії. Залишається нез'ясованою проблема - як забезпечити режим комерційної таємниці, і яка ціна даного питання.

Аналіз останніх досліджень та публікацій. Проблеми правового режиму комерційної таємниці на підприємстві досліджували Е.Я.Соловйова, В.А.Рубанова, В.М.Чаплигіна, А.А.Чернявський, О.А.Городов, Н.С.Гуляєва, С.Е.Жилінський, С.А.Кузьміна, В.Н.Лопатін, С.А.Парашук, О.А.Підпригора, О.О.Підпригора та ін. Однак недостатньо вивченою та дискусійною залишається проблема комерційної таємниці та забезпечення її нерозголошення на підприємстві.

Мета статті. Висвітлення поняття комерційної таємниці на підприємстві та розглянуто забезпечення її нерозголошення, як один із факторів ризику для підприємства, з погляду економічної безпеки підприємства.

Виклад основного матеріалу дослідження. Сучасний бізнес швидко змінюється. В основі цих змін - глобалізація економіки, стирання національних кордонів, постійне впровадження інновацій та підвищення конкуренції. Реалії сьогодишньої підприємницького середовища такі, що саме нетривіальні рішення і нові технології приносять найбільш відчутні прибутки, створюють фундамент для отримання доходу в майбутньому. Як наслідок цієї тенденції, посилюється ріст високотехнологічного сектора в бізнесі, заснованого на останніх досягненнях науки і техніки.

Зростаюча значимість конфіденційної інформації для бізнес-процесів створила передумови для формування законодавства про захист комерційної таємниці в багатьох розвинених країнах.

В Україні формування законодавчої бази про комерційну таємницю почалося з 1992 року у вигляді урядових постанов, окремих статей, законів та Цивільного кодексу. Термін „комерційна таємниця” був введений у правовий оборот Законом України „Про підприємства в Україні” від 27.03.1991 р. Під комерційною таємницею підприємства розуміються відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може заподіювати збиток його інтересам.

Так, в серпні 1993 р. Кабінетом Міністрів України було видано постанову «Про перелік відомостей, що не становлять комерційну таємницю», де визначалися дані, які не могли довільно ставитися підприємцями до числа конфіденційних. У Цивільному кодексі поняття комерційної таємниці трактується як 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 та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію (ст. 505 ЦКУ). Статтею 420 ЦКУ також, визначено, що комерційна таємниця є об'єктом інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором[2].

Положення про комерційну таємницю знайшло своє відображення і в законі «Про банки і банківську діяльність» від 7 грудня 2000 р. Ст. 60 закону «Банківська таємниця» говорить, що інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним, чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, є банківською таємницею[5].

Однак окремі положення законів чи інших правових актів не могли створити цілісної композиції норм, що регулюють різні аспекти діяльності, пов'язаної з комерційною таємницею. Для цієї мети був необхідний спеціальний закон «Про комерційну таємницю», в якому б давалися необхідні дефініції, встановлювалися права та обов'язки сторін, визначалася конкретна відповідальність за порушення тих чи інших положень закону.

Однак, в Україні існує лише проект закону «Про комерційну таємницю», що говорить про те, що система врегулювання питань пов'язаних з комерційною таємницею є не систематизованою, а це дає підстави для вчинення всілякого роду порушень в системі управління підприємством. Ця проблема є чи не найактуальнішою зараз, так як більшість інформації зараз знаходиться на комп'ютерних носіях, а це ще одне слабе та болоче місце – кіберзлочинність, хакерство та

економічна злочинність в комп'ютерних мережах.

Отже, серцевиною багатьох видів і форм бізнесу є комерційна таємниця, тобто ті відомості, які відкривають дорогу до копіювання бізнесу, його відтворенню в різних інтерпретаціях легальними і нелегальними способами. Слід також відзначити, що практично вся сфера сервісу та промисловості, що виготовляє продукцію з високою доданою вартістю, повністю або частково ґрунтується на комерційній таємниці. У розряд закритої інформації потрапляють бази даних, відомості про клієнтів і технологіях, організаційні та управлінські схеми, навчальні методики, склади і рецептури продуктів, способи контролю якості і багато іншого.

Носієм комерційної таємниці про підприємство чи індивідуальному підприємству є держава в особі його фінансових і податкових органів. Як і будь-який інший суб'єкт ринку - як підприємство, так і його працівники, сплачують до бюджетів усіх рівнів податки. За величиною сплачених податків можна судити про суми доходів підприємства і його персоналу. Цей очевидна взаємозв'язок служить сигнальною інформацією для кримінальних елементів всіх видів - здирників, шахраїв, шантажистів, грабіжників.

У цьому зв'язку варто відзначити і значимість збереження банківської таємниці. Практично всі сучасні підприємства та окремі підприємці користуються послугами комерційних банків - мають у них розрахункові та депозитні рахунки, здійснюють безготівкові платежі, розрахунки з партнерами та клієнтами, проводять валютні операції. Іншими словами, співробітники банку знають все або майже все про поточний фінансовий стан того чи іншого підприємства, що є клієнтом банку. Витік конфіденційної інформації про погіршення або поліпшення фінансового стану підприємства може стати джерелом неприємностей для бізнесу. Істотним каналом витоку конфіденційної інформації є власний персонал фірми [9].

Є і ще один аспект, пов'язаний з підтриманням режиму комерційної таємниці в підприємницькому справі. Цей аспект стосується як недобросовісної конкуренції в цілому, так і промислового шпигунства зокрема. Чужі технологічні секрети завжди викликають підвищений інтерес з боку інших учасників ринку і навіть іноземних держав. І це цілком зрозуміло. Розкривши комерційну таємницю конкуруючих фірм, можна заощадити значні фінансові ресурси і час, вжити превентивних заходів і зіграти на випередження.

На першому етапі керівництвом фірми або індивідуальним підприємцем розглядається питання про найбільш вразливих, з точки зору захисту комерційної інформації, секторів бізнесу. Такими секторами є:

У сфері бізнесу високих технологій - способи і рецептури виробленої продукції, добавки та інгредієнти, що покращують якість виробів. Це можуть бути програмні продукти і методи обробки інформації, комп'ютерні моделі та засоби автоматизації виробничих процесів, пристрої та прилади, що працюють на нових принципах або невідомих раніше ефектах;

У сфері сервісу, банківської справи та страхування - бази даних, що містять відомості про клієнтів і партнерів, їх фінансовий стан, активів, поточної та майбутньої платоспроможності. Не підлягають розголошенню дані про способи роботи з клієнтами, про пристрій і принципи функціонування платіжних систем, паролі і коди доступу до рахунків, способах кодування і шифрування комерційної інформації, маршрутах переміщення та зберігання грошових коштів;

У сфері традиційних виробництв - системи охорони підприємств (розташування пунктів контролю, їх технічного оснащення, способів відключення систем сигналізації й блокування), фінансова та маркетингова інформація, дані про переговори і передбачуваних замовленнях, великих покупках або продажах активів, відомості про зарплати співробітників, про величину преміальних виплат.

Разом з секторами можливого витоку конфіденційної інформації визначається і коло осіб, потенційно зацікавлених в отриманні такого роду даних. Зазвичай в нього входять:

- конкуруючі підприємства, що виробляють аналогічні продукти або товари-субститутути;
- особи, що планують відкрити власний бізнес у цій сфері або близької до неї за спрямованістю та складом клієнтів;
- співробітники фірми, незадоволені своїм службовим становищем, рівнем оплати праці, що вступили в конфлікт з начальством. Знання технологічних секретів фірми може зробити цих співробітників вельми небезпечними ворогами підприємства;
- представники спецслужб і приватних детективних агентств, бажаючи заробити на продажі комерційної таємниці фірми її конкурентам або іншим зацікавленим особам;
- кримінальні структури.

Після того, як керівництво підприємства визначило сектори закритої інформації, витік якої може привести до важких і руйнівних наслідків, вступає в дію наступний етап - визначення форм і методів запобігання розголошенню комерційної таємниці. На цій стадії власники бізнесу вирішують непрості завдання організаційно-правового та управлінського характеру, пов'язані із забезпеченням спеціального охоронного режиму[9]. У число цих завдань входить:

Визначення кола осіб, що мають доступ до конфіденційної інформації. З теорії забезпечення секретного режиму відомо, що ніж менше осіб має доступ до закритої інформації, тим менше ймовірність її витоку. На практиці цей принцип реалізується в повному обсязі - до роботи з конфіденційними даними допускаються тільки ті особи, без послуг яких обійтися не можна.

Розробка внутрішньофірмової системи документообігу. Витік конфіденційної інформації вельми часто відбувається з - за несанкціонованого доступу до службових документам. Зміст ділових листів, креслень, схем, робочої документації стає надбанням осіб, які можуть вільно або мимоволі завдати шкоди фірмі. Чітке регламентування системи внутрішньофірмового документообігу в значительній степені знижує ризики розголошення комерційної тайни по цьому каналу.

Для запобігання витоку конфіденційної інформації з даної лінії зазвичай використовується система градації документів за рівнем доступності. Для внутрішньофірмових документів вводяться спеціальні грифи, які позначають рівень секретності: «Для службового користування» (перша градація по обмеженню доступу), «Таємно» (друга градація), «Цілком таємно» (третья градація»). Знайомитися з документами під тим чи іншим грифом можуть тільки спеціально допущені співробітники.

Введення спеціальних форм трудових договорів з працівниками підприємства. При надходженні на підприємство кожен працівник, який по боргу служби буде мати доступ до комерційної таємниці, повинен ознайомитися з умовами спеціальних пунктів трудового договору і підписати його.

Отже задля забезпечення мінімального рівня безпеки, потрібно:

- проведення спеціальних інструктажів та перевірки знань
- створення режимних зон чи об'єктів на підприємстві.
- періодичні перевірки персоналу на поліграфі (детекторі брехні)
- створення на підприємстві власної служби безпеки.

Як правило, завданнями з охорони комерційної таємниці служба безпеки не обмежується. Поряд із заходами щодо підтримання секретності та протидії промислового шпигунству (прослуховування телефонних розмов і розмов персоналу, проникнення в комп'ютерні бази даних і т.д.), службі безпеки ставиться в обов'язки підтримка загального пропускового режиму, припинення розкрадань, виявлення співробітників, що перебувають в стані алкогольного або наркотичного сп'яніння, ізоляція відвідувачів і клієнтів фірми, що ведуть себе неадекватно, супровід і охорона вищих посадових осіб підприємства, взаємодія зі спецслужбами і деякі інші заходи [8].

Перелік інструментів щодо забезпечення комерційної таємниці досить великий і різноманітний. Вартість цих інструментів також різна, але загальна тенденція очевидна - чим вище потрібен рівень захисту інформації, тим дорожче таке забезпечення. В цьому питанні керівники підприємств завжди намагаються знайти якийсь оптимальний - щоб, з одного боку, забезпечити достатньо надійний захист комерційної інформації, з іншого - щоб витрати на безпеку знаходилися в розумних межах і не підірвали основне виробництво.

Висновки. Отже, роблячи висновок, можна сказати, що правові норми у сфері застосування терміна "комерційна таємниця" не отримали достатнього розвитку, законодавець обмежився лише встановленням мінімальної кількості норм, що регулюють даний правове питання. Проблеми в сфері комерційної таємниці були і залишаються актуальними як для науковців, так і для практиків. На сьогодні немає закону України про охорону комерційної таємниці, а відтак виявити і притягти до відповідальності вза неправомірно використання такої інформації майже неможливо. Існуючі на сьогодні в Україні протиріччя в нормативно-правових актах з визначення комерційної таємниці можуть бути усуненні при прийнятті окремого закону, який би врегулював правовий статус та шляхи захисту права на комерційну таємницю, або на основі внесення змін в існуючі законодавчі норми положень. Подальшими векторами в роботі стане система забезпечення безпеки підприємства, маючи витік комерційної інформації, як головну загрозу підприємству. Включення до дослідження визначення можливих джерел та способи усунення ризиків витоків інформації.

Література.

1. Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
2. Цивільний кодекс України від 16 січня 2003 року №435-IV // Відомості Верховної Ради України. – 2003. – №№ 40-44. – Ст. 356.

3. Господарський кодекс України від 16 січня 2003 року №436-IV // Відомості Верховної Ради України. – 2003. – №№ 18-22. – Ст. 144.
4. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету від серпня 1993 р. № 611 / [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=611-93-%EF>.
5. Про банки і банківську діяльність: Закон України №2121-III від 7 грудня 2000 р. //ВВРУ. — 2001. — №5-6 //www.zakon.rada.gov.ua
6. Іваницька Н. Захист комерційної таємниці в трудових правовідносинах / Н. Іваницька // Бизнес и безопасность – 2005. – № 6. – С. 12– 14.
7. Гуз А. Как защитить коммерческую тайну / А. Гуз, А. Марущак // В мире спецслужб, 2006. – № 1. – С. 4–6.
8. Франчук Сергій. Як організувати захист комерційної таємниці та конфіденційної інформації на підприємстві – Електронний ресурс [режим доступу] - <http://www.yur-gazeta.com/article/1326/>
9. Роль и значение коммерческой тайны в предпринимательской деятельности. Каналы утечки конфиденциальной информации [Електронний ресурс]. Режим доступу: <http://vadim-galkin.ru/business-basics/base/trade-secrets/>
10. Комерційна таємниця на підприємстві [Електронний ресурс]. Режим доступу: <http://hrliga.com/index.php?module=profession&op=view&id=343>

References.

1. Verkhovna Rada of Ukraine (1992), “The Law of Ukraine “On Information”, Bulletin of the Verkhovna Rada of Ukraine, vol. 48, p. 650.
2. Verkhovna Rada of Ukraine (2003), “The Civil Code of Ukraine”, Bulletin of the Verkhovna Rada of Ukraine, vol. 40-44, p. 356.
3. Verkhovna Rada of Ukraine (2003), “The Commercial Code of Ukraine”, Bulletin of the Verkhovna Rada of Ukraine, vol. 18-22, p. 144.
4. Cabinet of Ministers of Ukraine (1993), Resolution “On the list of information that does not constitute a trade secret”, available at: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=611-93-%EF> (Accessed 4 January 2013).
5. Verkhovna Rada of Ukraine (2001), “Law “On Banks and Banking”, Bulletin of the Verkhovna Rada of Ukraine, vol. 5-6.
6. Ivanytska, N. (2005), “Protection of trade secrets in labor relations”, *Business and security*, vol. 6, pp. 12–14.
7. Guz, A. (2006), “As the protection of kommercheskuyu mystery”, *In the world of special services*, vol. 1, pp. 4-6.
8. Sergey Franchuk (2013), “How to organize the protection of trade secrets and confidential information in the enterprise”, available at: <http://www.yur-gazeta.com/article/1326/> (Accessed 4 January 2013).
9. Galkin V.V. (2011), “Role and importance kommercheskoy secrets in predprynatelskoy activities. Channels Leaks konfydentsyalnoy of information” available at: <http://vadim-galkin.ru/business-basics/base/trade-secrets/> (Accessed 4 January 2013).
10. Slipachuk O. (2006), “Trade Secret in the enterprise” available at: <http://hrliga.com/index.php?module=profession&op=view&id=343> (Accessed 4 January 2013).

Стаття надійшла до редакції 19.11.2013 р.



ТОВ "ДКС Центр"