УДК 330.322

СИСТЕМА ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПІДПРИЄМСТВА

ЛОКОТЕЦЬКА О. В.

Харків

У сучасних умовах, стабільне існування виробничо-господарської діяльності підприємства, ефективністю комплексної системи економічної безпеки підприємства, функціонування якої потребує відповідного інформаційного забезпечення. Інформаційна безпека являє собою захищеність інформаційних ресурсів, які необхідні для успішної роботи підприємства.

У великому енциклопедійному словнику термін «інформація» кваліфікується, з одного боку, як відомості, які передаються людьми усним, письмовим або іншими способами (за допомогою умовних сигналів, технічних засобів і т. д.), а з іншого – як обмін відомостями між людьми, людиною і автоматом, автоматом і автоматом; обмін сигналами у рослинному світі; передача ознак від клітини до клітини, від організму до організму.

Закон України «Про інформацію» визначає поняття «інформація» таким чином: документовані або публічно оголошені відомості про випадки та явища, які відбуваються у суспільстві, державі та навколишньому природному середовищі [1].

Мета статті – розробка ефективної системи захисту комерційної таємниці з боку самого підприємства.

Методологічною основою дослідження стали фундаментальні дослідження вітчизняних і зарубіжних економістів. Основними методами дослідження, використаними в роботі, є: абстрактно-логічний (теоретичне узагальнення і формування висновків); метод порівнянь та системно-структурний аналіз.

Оскільки на сьогоднішній день правова база із захисту підприємницької діяльності в Україні є не зовсім удосконаленою, тому особливо важливим стає розробка ефективної системи захисту комерційної таємниці з боку самого підприємства. Крім того, далеко не всі підприємства піклуються про зберігання у таємниці інформації, що за статусом може бути віднесена до конфіденційної. Це пояснюється тим, що керівництво підприємств не досить чітко розуміє важливість і необхідність організації системи захисту комерційної таємниці.

Система захисту комерційної таємниці підприємства повинна охоплювати ряд послідовних етапів:

1. Розробка переліку відомостей, що становлять комерційну таємницю.
2. Зазначення часу існування різних видів конфіденційної інформації.
3. Затвердження переліку відомостей, що становлять комерційну таємницю підприємства.
4. Встановлення носіїв відомостей, що становлять комерційну таємницю підприємства.
5. Визначення кола осіб, які володіють конфіденційною інформацією за різними напрямками діяльності підприємства.
6. Вибір способів захисту комерційної таємниці.
7. Контроль за дотриманням заходів безпеки.

На *першому етапі* системи захисту комерційної таємниці, передбачається виділення з усього масиву інформації підприємства, виділення найбільш цінної, яка потребує обмеженого доступу. Далі необхідно ретельне вивчення обраної інформації, як секретної, і складання робочого варіанту зводу відомостей, що становлять комерційну таємницю підприємства. Відповідний перелік конфіденційної інформації може бути сформований за такими напрямками: кадрова політика підприємства, фінансова діяльність підприємства, цінова політика підприємства, збутова діяльність підприємства, забезпечення безпеки підприємства.

Другий етап системи захисту комерційної таємниці, передбачає встановлення терміну засекречування.

За періодом існування комерційну таємницю можна поділити на короткострокову таємну інформацію (від 1 дня до 6 місяців) та середньострокову таємну інформацію (від 6 місяців і більше).

Третій етап, який передбачає затвердження переліку відомостей, що становлять комерційну таємницю підприємства, складається з двох стадій:

1. Присвоєння за кожним видом інформації відповідного грифу секретності. «Особливо секретно» – відомості, оволодіння якими негативно відбиваються на усієї діяльності підприємства, та «секретно» – відомості, оволодіння якими може спричинити шкоду за окремим напрямком діяльності підприємства.

2. Затвердження та підписання керівником підприємства зводу відомостей, що становлять комерційну таємницю.

Отже, усім відомостям, що перелічені у вказаному зводі, офіційно наданий статус комерційної таємниці на підприємстві.

Четвертий етап забезпечення захисту комерційної таємниці – це встановлення носіїв відомостей, що становлять комерційну таємницю підприємства.

Носіями конфіденційної інформації можуть виступати людина, документи, продукція, офіційні засоби інформації, технічні засоби.

При цьому людина є сполучною ланкою між усіма іншими носіями комерційної таємниці. Саме людина розробляє і затверджує документацію; є виробником продукції; готує матеріали для видання, оголошення та показу в засобах масової інформації; працює за комп'ютерами, друкарською машинкою, з телефонними апаратами, факсами та іншими технічними засобами.

За кожним видом конфіденційної інформації вирішується, в якій якості вона буде існувати. Як зазначалось вище, комерційна таємниця може мати декілька носіїв, що треба враховувати при визначені способів її захисту, а також тих осіб, які нею володіють.

На *п'ятому етапі* безпосередньо встановляються конкретні особи, що володіють тією чи іншою конфіденційною інформацією або можуть мати доступ до неї. Керівництву у даному випадку необхідно звернути на посаду членів колективу, особисті якості.

Як свідчать дослідження, розголошення комерційної таємниці у більшості пов'язано з тим, що на підприємстві недостатню увагу приділяють проведенню глибокого аналізу особистості працівника – потенційного носія комерційної таємниці [2].

Шостий етап передбачає вибір способів захисту комерційної таємниці на підприємстві.

Взагалі, оволодіння конфіденційною інформацією можливо через людину, шляхом публікування, на основі вивчення характеристик продукції, при обробці документів, за допомогою використання технічних засобів.

Термін «комерційна таємниця» нерозривно пов'язаний з людським фактором, оскільки, саме людина виступає як носій або власник конфіденційної інформації, як особа, що захищає комерційну таємницю, або як злочинник.

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

Існують такі протиправні дії, що дозволяють оволодіти конфіденційною інформацією підприємства:

- повідомлення, надання та пересилка відомостей, що становлять комерційну таємницю;
- підкуп співробітників підприємства, що володіють або мають доступ до конфіденційної інформації;
- підслуховування та підглядання (спостерігання);
- підключення до технічних засобів;
- крадіжка;
- копіювання та фотографування;
- перехоплювання;
- знищення.

Також, оволодінню комерційною таємницею сприяють низький рівень контролю за досягненням заходів безпеки, незадовільні умови праці, неефективна система заохочування працівників, економія на більш досконалих технічних засобах захисту, текучість кадрів, недосконала система праці, аварійний стан основних фондів, невідповідність співробітника посаді, яку він займає.

Виходячи з того, що основна загроза надходить від людини, пропонуємо складати на підприємстві перелік усіх можливих способів оволодіння комерційною таємницею. Перелік покладається в основу розробки способів захисту конфіденційної інформації на підприємстві.

Залежно від масштабів діяльності підприємства в його організаційній структурі може бути задіяно службу безпеки, до функції якої безпосередньо входить і забезпечення захисту комерційної таємниці підприємства.

Керівництво разом зі службою безпеки розробляють стратегію і тактику зберігання комерційної таємниці.

На підприємстві повинні бути створений жорсткий режим доступу до інформації конфіденційного характеру. Це передбачає:

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

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

3) встановлення відповідальності за розголошення комерційної таємниці підприємства, що не суперечить законодавству України:

- дисциплінарна відповідальність настає у разі розголошення комерційної таємниці в зв'язку з балакучістю, недбайливістю, безвідповідальністю співробітника підприємства. Це знажен-

ня посади, переведення на роботу, не пов'язану з комерційною таємницею, звільнення з роботи (з відповідною позначкою у трудовій книжці). Стягнення накладається не пізніше шести місяців з дня порушення;

- матеріальна відповідальність може наступати і разом з дисциплінарною. Призначенням є відшкодування втрати (фактичної чи можливої) в наслідок порушення. Вважаємо, що саме матеріальна відповідальність – це один з головних стримуючих чинників у скоєнні злочину. Залежно від масштабів збитку (втрати) компенсуванню підлягає частка заподіяної шкоди, повний розмір заподіяної шкоди, не отриманий прибуток протягом 6 місяців.

Але тут слід зазначити, що відшкодування не може перевищувати третю частину заробітної платні порушника, інакше згідно із законодавством – обов'язкове звернення до суду;

- кримінальна відповідальність – це державна форма відшкодування втрати. Підставою кримінальної відповідальності є суспільно небезпечні вчинки, що учинені особою і мають склад злочину;
- використання технічних засобів захисту комерційної таємниці. Такі заходи пов'язані з додатковими витратам и для підприємства. У сучасних умовах існує різноманітний перелік технічних засобів, до яких можна віднести засоби захисту вікон та дверей і території, програмні засоби захисту, засоби захисту засобів зв'язку, тощо;
- організаційні заходи захисту комерційної таємниці підприємства полягають у створенні умов зберігання інформації в секреті. У випадку, коли на підприємстві не має служби безпеки, вважаємо за необхідне наявність співробітника, до функції якого входить забезпечення безпеки функціонування підприємства, у тому числі захист комерційної таємниці. Обов'язковим для підприємств є реєстрування осіб, що працюють з конфіденційною інформацією. Журнал реєстрації заповнюється кожний день. Доступ до конфіденційних відомостей дозволяється у письмовій формі керівником підприємства з повідомленням служби безпеки. При цьому слід конкретно вказувати відомості, якими може користуватися особа. Пильної уваги заслуговують копіювання документації, файлів та ін. з грифами конфіденційності, а також зберігання та знищення чернетки з конфіденційною інформацією. Ці процеси також повинні підлягати реєстрації в окремому журналі і постійно контролюватися торговельним підприємством. У межах цього напрямку забезпечення захисту комерційної таємниці також вирішуються питання фінансування заходів безпеки, переобладнання приміщень, де зберігають, використовують конфіденційні дані, проведення профілактичної роботи з персоналом, розробки загальної стратегії захисту комерційної таємниці, залучення до забезпечення безпеки підприємства інших організацій та установ.

Сьомий етап захисту комерційної таємниці – контроль за дотриманням заходів безпеки. Контроль повинний бути своєчасний, повний, об'єктивний, надійний.

Суб'єктами контролю виступають керівник підприємства, керівники структурних підрозділів, служба безпеки.

Об'єктами контролю є виконання внутрішніх правил, положень про нерозголошення комерційної таємниці, її зберігання і захист; дотримання режиму доступу до конфіденційної інформації; підтримання у робочому стані технічних засобів захисту комерційної таємниці; наявність документів (файлів) з грифом «секретно» у повному обсязі при поверненні на зберігання; проведення рекламних заходів; підготовка до переговорів; порядок використання носіїв конфіденційної інформації; стан приміщень, де зберігається і використовується комерційна таємниця; персонал підприємства, що володіє комерційною таємницею та інше.

Здійснення контролю базується на таких основних принципах, як:

1) *повнота*;

2) *всебічність*, тобто контроль повинен охоплювати усі етапи організації системи захисту комерційної таємниці;

3) *своєчасність*, мається на увазі проведення перевірок в означенні терміни, при здійсненні певних операцій, діяльності, що пов'язані з користуванням або збиранням відомостей, які є комерційною таємницею;

4) *об'єктивність*, тобто проведення перевірки згідно з розпорядженням незалежно від почуттів, знань про особу, що підлягає перевірці, посади та ін.

5) *надійність*, яка полягає в достовірності звітних даних за результатами перевірки у зв'язку з високою відповідальністю.

Від того, наскільки здійснення контролю відповідає вказаним принципам, залежить ефективність системи захисту комерційної таємниці і в цілому конкретні позиції підприємства.

Враховуючи, що процес організації системи захисту комерційної таємниці гнучкий, то для усіх етапів властиве корегування: внесення нових видів конфіденційних відомостей до переліку і відповідного встановлення нових носіїв, кола осіб, що мають доступ до інформації, способів захисту та ін.

Таким чином, формування системи економічної безпеки підприємства повинно здійснюватись в умовах узгодженості державної економічної політики з напрямками і заходами забезпечення економічного захисту суб'єкту господарювання. При цьому особливе місце належить створенню системи захисту комерційної таємниці підприємства.

ЛІТЕРАТУРА

1. Закон України «Про інформацію» // Відомості Верховної Ради України (ВВР).– 1992.– № 48.– Ст. 650.

2. Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны.– Монография.– К.: Издательский Дом «Ин Юре», 2000.– 400 с.