

УДК 65.012.8

## МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПІДПРИЄМСТВ ВІД ЕКОНОМІЧНОГО ШПИГУНСТВА

*Чердніченко А.О., аспірант (ХНАМГ)*

*В статті класифіковано методи економічного шпигунства та запропоновані способи захисту підприємств від економічного шпигунства.*

*Ключові слова: безпека підприємства, методи захисту, економічне шпигунство.*

## МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРЕДПРИЯТИЙ ОТ ЭКОНОМИЧЕСКОГО ШПИОНАЖА

*Чердніченко А.А., аспірант (ХНАГХ)*

*В статье классифицированы методы экономического шпионажа и предложены способы защиты строительных предприятий от экономического шпионажа.*

*Ключевые слова: безопасность предприятия, методы защиты, экономический шпионаж.*

## METHODS OF DEFENSE FROM ECONOMIC ESPIONAGE THE COMPANIES

*Cherednychenko A.A.*

*Methods of economic espionage and ways of security from economic espionage in construction industry have been classified in the article.*

*Keywords: enterprise defense, defense methods, economic espionage.*

**Постановка проблеми.** Сучасні умови ведення господарської діяльності в Україні характеризуються чисельними ризиками, які знижують ефективність роботи підприємства.

Забезпечення економічної безпеки підприємства - це важкий процес формування умов та механізмів стабільної роботи конкретного підприємства, на який має вплив велика кількість зовнішніх та внутрішніх факторів.

**Аналіз останніх досліджень.** Важливу роль у дослідженні проблематики економічної безпеки відіграють праці таких вчених, як Барановський О.І., Долженков О.Ф., Камлик М.І., Мунтіян В.І. та ін. [1-4]. Але, в той же час, комплексно не досліджувались проблеми забезпечення економічної безпеки підприємств будівельної галузі. Тому в роботі буде приділена значна увага саме методам комплексного забезпечення захисту підприємств будівельної галузі.

**Метою** статті є дослідження методів економічного шпигунства та визначення основних способів захисту підприємств від нього.

**Виклад основного матеріалу.** Багато держав спрямовують зусилля своїх спецслужб на постійну розвідку досягнень іноземних підприємств, особливо їх патентів, комерційних, технологічних і виробничих таємниць. Саме тому темі економічного шпигунства, захисту інсайдерської інформації стало приділятися велика увага і ця проблематика набула великого значення [5].

Способи захисту від промислового шпигунства такі ж різноманітні, як і саме шпигунство. Для подальшого розвитку питання забезпечення захисту підприємств необхідно визначити, що саме є безпекою підприємства.

Так, безпека підприємства (підприємництва) означає його захищеність від зовнішніх та внутрішніх дестабілізуючих чинників, що дозволить надійно зберігати і вискоєфективно використовувати його фінансовий, матеріальний і кадровий потенціал [9].

Для визначення методів забезпечення захисту інсайдерської інформації підприємств треба, насамперед, розглянути визначення понять інсайдерська інформація, економічне шпигунство (розвідка) або розвідувальна діяльність, визначити методи шпигунства.

У науковій літературі термін «економічне шпигунство» майже не зустрічається, натомість науковці користуються висловом «економічна розвідка». Термін економічна розвідка (економічне шпигунство) означає активні дії спрямовані на збір, викрадення, накопичення та обробку цінної інформації закритої для доступу сторонніх осіб.

На теперішній час найважливішими стають відомості про технологічні та виробничо-економічні «ноу-хау», інсайдерську інформацію [5].

Найбільш точно визначення терміна інсайдерська інформація надано у Законі України «Про внесення змін до деяких законодавчих актів

України щодо інсайдерської інформації». Це неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених законом [6].

Розвідувальна діяльність, згідно до Закону України «Про розвідувальні органи України», це діяльність, яка здійснюється спеціальними засобами і методами з метою забезпечення визначених законом органів державної влади розвідувальною інформацією, сприяння реалізації та захисту національних інтересів, протидії за межами України зовнішнім загрозам національній безпеці України [7]. Виходячи з даного визначення, розвідувальна діяльність на підприємстві - це діяльність, яка здійснюється спеціальними засобами і методами з метою заволодіння інсайдерською інформацією та сприяння реалізації та захисту інтересів підприємства, протидії за межами підприємства зовнішнім загрозам безпеці підприємства.

Розвідувальна діяльність або шпигунство є дуже давнім явищем. Аналіз викритих фактів розвідувальної діяльності свідчить, що у 39% випадків шпигунства проти підприємств замовниками були конкуренти, в 19% - клієнти, у 9% - постачальники і в 7% - розвідслужби [7]. Шпигунством займаються працівники підприємств, приватні шпигунські бюро, детективні агентства, служби безпеки, хакери і безпосередньо професійні розвідники.

Мотивами отримання інсайдерської інформації можуть виступати: фінансово-матеріальна зацікавленість, кар'єрні мотиви, помста, ідеологічні мотиви.

Методи отримання інформації охоплюють весь спектр і персонал розвідслужб, включаючи використання агентурного апарату, кадрових розвідників, можливостей резидентур, використання економічних журналістів, практикантів, отримання інформації технічним шляхом і т.д. Але економічне шпигунство має особливості, до яких відносять:

- аналіз відкритих джерел;
- отримання інформації у ході бесід, перемов, спілкування;
- використання сучасної електронної, інформаційної техніки і спеціальних пристроїв (комп'ютерне шпигунство). Зараз сфера електронної обробки даних з її глобальними мережами являє собою найповніше джерело інформації для економічних шпигунів, серед яких 80% є "внутрішніми злочинцями" (тобто працівниками тих же підприємств, за якими і шпигують);
- агенти на підприємстві - являють собою найбільшу небезпеку для інтересів безпеки підприємства [7].

Економічним шпигунством займаються ті підприємства, метою яких є виготовлення власних більш дешевих копій проектів будівництва і виходу з ними на ринок. Для таких підприємств головним є отримання технічної документації та інформації про проекти та макетів майбутніх споруд підприємств-конкурентів [5].

Виток інформації з підприємств відбувається внаслідок наступних дій інсайдерів представлених на рис. 1

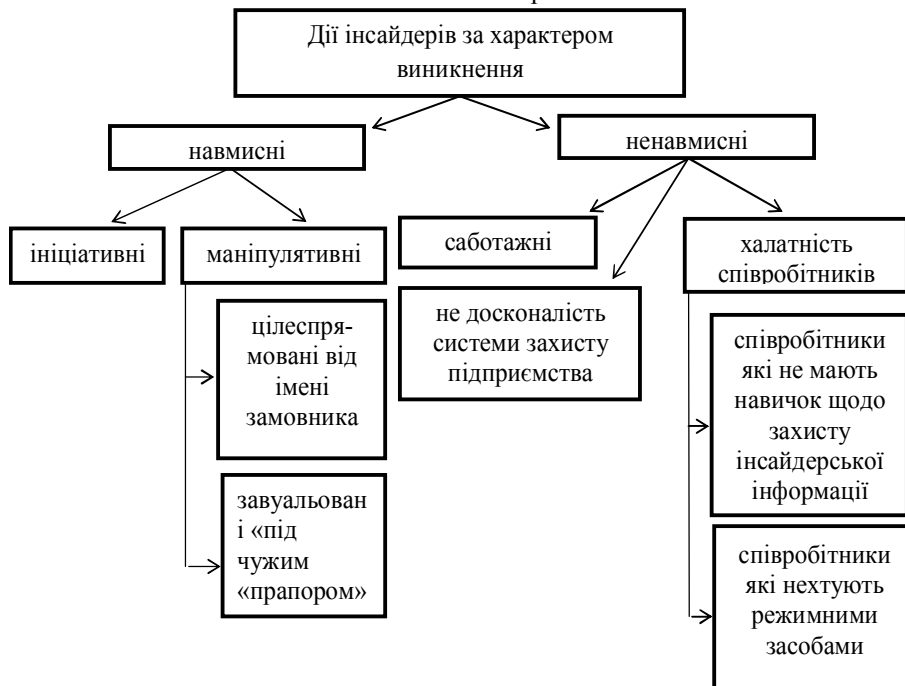


Рис. 1. Дії інсайдерів за характером виникнення

Основна проблема захисту інформації підприємства зводиться до необхідності і вміння керівників та робітників зберігати і захищати свою інформаційну власність (інсайдерську інформацію). Заходи щодо захисту інтересів підприємства вимагають певних витрат. Існує світова статистика усереднених оцінок. Так, в Швейцарії кошти, витрачені на захист комерційних виробничих таємниць становлять 1,5-2% загальних виробничих витрат. За даними "The Boston Globe", компанії, що входять в число "500 самих щасливих", витрачають сотні тисяч доларів, щоб протистояти електронному шпигунству. [8].

Захист кожного об'єкта має бути індивідуальним та комплексним. Для створення ефективного комплексного захисту інформації на підприємстві повинні бути вирішені наступні основні питання:

1. Виявлення інформаційних ресурсів, що підлягають захисту і виділення їх з решти інформації.

2. Оцінка можливого збитку від витоку будь-яких конфіденційних даних і класифікація інформації за ступенем важливості.

3. Визначення усіх видів носіїв інформації, які підлягають захисту.

4. Виявлення можливих факторів вразливості інформації, що підлягають захисту [8].

В більшості підприємств середовищами зосередження інсайдерської інформації корпорації являються:

- керівництво корпорації;
- фінансово-економічні підрозділи;
- юридичні підрозділи;
- канцелярія (реєстраційні підрозділи);
- технологічні бюро.

Способи захисту підприємства від економічного шпигунства залежать від методів економічного шпигунства. Пропонуємо способи захисту від економічного шпигунства згідно класифікації методів шпигунства.

*Таблиця 1*

*Способи захисту підприємства від економічного шпигунства*

Групи методів шпигунства	Способи захисту
<p>перша група:</p> <ul style="list-style-type: none"> <li>— вивчення і аналіз відомостей, що публікуються;</li> <li>— вивчення і аналіз продукції, що випускається;</li> <li>— спостереження за перевезеннями підприємством сировини, товарів, побічних продуктів виробництва</li> </ul>	<ul style="list-style-type: none"> <li>• застосування обмежень при публікації інформації, яка може бути використана конкурентом;</li> <li>• посилення особистого контролю з боку керівника або його заступників за процесом обробки інформації, що підготовлена до публікації, її публічного використання;</li> <li>• запровадження практики укладення на підприємстві інсайдерських договорів (між провідними фахівцями та керівництвом підприємства, носіями секретів та керівництвом підприємства);</li> <li>• підписання договору з клієнтом де передбачити умови, що він не застосовуватиме сам і не передаватиме кому-небудь іншому отриману від підприємства інформацію;</li> <li>• організація фіктивних маршрутів перевезень макетів та проектної документації (з метою приховування справжніх)</li> </ul>
<p>друга група:</p> <ul style="list-style-type: none"> <li>- вивідування даних у керівництва, фахівців і працівників підприємства - конкурента;</li> <li>— проникнення у структуру (підприємство) конкурента з метою отримання інформації;</li> <li>— викрадення документів, зразків продукції, креслень</li> </ul>	<ul style="list-style-type: none"> <li>• обов'язкове проведення інструктажу зі співробітниками, щодо захисту інсайдерської інформації;</li> <li>• впровадження практики матеріальних заохочень працівників за нерозголошення інсайдерської інформації;</li> <li>• необхідність укладення інсайдерського договору між працівниками та керівництвом підприємства;</li> <li>• професійно організована і налагоджена режимно-пропускна система на територію підприємства</li> </ul>
<p>третья група:</p> <ul style="list-style-type: none"> <li>— підкуп співробітників підприємства;</li> <li>— переманювання фахівців</li> </ul>	<ul style="list-style-type: none"> <li>• організувати сприятливу атмосферу в колективі;</li> <li>• укладення інсайдерського договору;</li> <li>• впровадження практики матеріальних заохочень працівників за нерозголошення інсайдерської інформації</li> </ul>
<p>четверта група:</p> <ul style="list-style-type: none"> <li>- технічне шпигунство</li> </ul>	<ul style="list-style-type: none"> <li>• проведення важливих нарад в спеціально обладнаних технічними засобами приміщеннях, що унеможливають витік інформації;</li> <li>• залучення до облаштування приміщень фахівців області технічного захисту інформації з відповідними ліцензіями та досвіду роботи</li> </ul>

В результаті, виконання вищенаведених пунктів значно знизиться можливість (ризик) викрадення і заволодіння інсайдерської інформації.

Питаннями захисту та охорони підприємства має займатися спеціалізована служба – служба безпеки.

Заходи, здійснювані службою безпеки підприємства включають в себе:

- режимні заходи;
- фізичну охорону;
- технічні засоби захисту;
- попереджувально-профілактичну роботу

[10].

Суть захисту зводиться до виявлення, нейтралізації і запобігання загрозам. У якості об'єктів захисту можна виділити:

- інтереси організації;
- інформація;
- технології [10].

Для ефективності захисту необхідно визначити потреби і розміри служби безпеки. Служба безпеки організує свою роботу в тісній взаємодії зі службами внутрішнього контролю, юридичним відділом, відділами забезпечення (програмісти, економісти, фінансисти, господарські служби тощо). Кількість співробітників залежить від розміру підприємства та складності захисту.

Функціональні обов'язки розподіляються за об'єктами захисту: будівлі, територія, майно, виробництво, транспортні засоби, інформація, зв'язок, персонал тощо. Робота організується шляхом взаємного доповнення економічних, правових і технологічних методів захисту.

Незважаючи на розміри підприємства, всі працівники служби безпеки мають визначити максимально можливі методи шпигунства конкретно до їх підприємства та відповідно ним підібрати засоби захисту підприємства від економічних загроз.

**Висновок.** Таким чином, запропоновані способи захисту підприємства від економічного шпигунства дозволить знизити ризик викрадення та заволодіння інсайдерською інформацією та створити ефективну систему забезпечення безпеки підприємства, яка повинна базуватися на сукупності державно-правових, адміністративних, режимних заходів, організації попереджувально-профілактичної

роботи з персоналом, фізичній охороні об'єктів і працівників підприємства, впровадженні технічних засобів захисту від промислового і комерційного шпигунства.

### СПИСОК ЛІТЕРАТУРИ

1. Барановський О.І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення): монографія / О.І. Барановський – К.: КНЕУ, 2004. – 759 с.

2. Долженков О.Ф. Особливості гарантування економічної безпеки підприємницької діяльності в ринкових умовах / О.Ф. Долженков, Ж.О. Жуковська, О.М. Головченко. – Одеса: ОІОІ ХНУВС, 2007. – 207 с.

3. Камлик М.І. економічна безпека підприємницької діяльності: економіко-правовий аспект : навч. посіб. / М.І. Камлик.-К.: Атіка, 2005.-431с.

4. Мунтіян В. І. Економічна безпека України. — К.: КВІЦ, 1999. — 462 с.

5. Кай Хиршманн. Секретные службы <http://www.agentura.ru/library/hirschmann/>

6. Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації 22 квітня 2011 року N 3306-VI : Закон України // [Електронний ресурс] – Режим доступу <http://zakon2.rada.gov.ua/>

7. Про розвідувальні органи України від 22 березня 2001 року N 2331-III : Закон України // [Електронний ресурс] – Режим доступу <http://zakon.nau.ua>

8. Вовченко В.В. Проблемы защиты информации от экономического шпионажа. / В.В. Вовченко, И.О. Степанов // [Електронний ресурс]- Режим доступу <http://www.analitika.info>

9. Способы защиты от экономического шпионажа // [Електронний ресурс] - Режим доступу <http://dehack.ru>

10. Іванюта Т.М., Економічна безпека підприємства / Т.М. Іванюта, А.О. Заїчковський // [Електронний ресурс] - Режим доступу <http://www.bookbrains.com>

*Рецензент д.е.н., професор УкрДАЗТ Компанієць В.В.  
Експерт редакційної колегії к.е.н., доцент УкрДАЗТ Зубенко В.О.*

УДК 657.471

## ОРГАНІЗАЦІЯ ОБЛІКУ ВИТРАТ ПІДПРИЄМСТВА В КОНКУРЕНТНОМУ СЕРЕДОВИЩЕ

*Черноіванова Г.С., к.е.н., доцент (ХНЕУ)*

*У статті обґрунтовано порядок розробки та реалізації стратегії досягнення конкурентних переваг щодо витрат, запропоновано схема формування стратегії досягнення конкурентних переваг щодо витрат.*

*Ключевые слова: конкурентна перевага, облік витрат, управління витратами, організація обліку витрат.*