

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Т. М. Іванюта, А. О. Заїчковський

# ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

НАВЧАЛЬНИЙ ПОСІБНИК

*Рекомендовано  
Міністерством освіти і науки України  
як навчальний посібник для студентів  
вищих навчальних закладів*

Київ  
«Центр учбової літератури»  
2009

ББК 65.290-2я73  
УДК 658.15 (075.8)  
I 24

*Гриф надано*  
*Міністерством освіти і науки України*  
*(Лист № 1.4/18-Г-1936 від 24.07.2008)*

**Рецензенти:**

**Пелішенко В. П.** — доктор економічних наук, професор;  
**Гудзинський О. Д.** — доктор економічних наук, професор;  
**Волощук Г. О.** — доктор економічних наук, професор.

Іванюта Т. М., Заїчковський А. О. Економічна безпека підприємства: **навч. посіб. [для студ. вищ. навч. закл.]** / Т. М. Іванюта, А. О. Заїчковський — К.: Центр учбової літератури, 2009. — 256 с. — ISBN 978-966-364-830-9.

В даному навчальному посібнику розглянуті сутність та складові елементи економічної безпеки держави, регіону, підприємства. Викладені основи правового регулювання комерційної таємниці за кордоном та у вітчизняному законодавстві. Обґрунтована необхідність в інформації на підприємстві та наведені методи її збирання. Наведені заходи щодо забезпечення безпеки підприємства та його інформації, а також технічні засоби захисту.

Призначена для студентів економічних юридичних спеціальностей, менеджерів, маркетологів, керівників підприємств, співробітників служб економічної безпеки підприємств.

Розділ 2 написаний разом з Олексієнко Г. В.

ББК 65.290-2я73  
УДК 658.15 (075.8)

ISBN 978-966-364-830-9

© Іванюта Т. М., Заїчковський А. О., 2009  
© Центр учбової літератури, 2009

# ЗМІСТ

<b>Вступ</b> .....	5
--------------------	---

## **Розділ 1. Економічна безпека**

1.1. Поняття економічної безпеки .....	7
1.2. Предмет, об'єкт, суб'єкт економічної безпеки .....	10
1.3. Економічна безпека держави .....	12
1.4. Економічна безпека регіону .....	14
1.5. Поняття економічної безпеки підприємництва .....	16
Питання для самоконтролю .....	28

## **Розділ 2. ПРАВОВИЙ ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ**

2.1. Проблеми правового захисту комерційної таємниці в Україні .....	30
2.2. Правове регулювання захисту комерційної таємниці за кордоном .....	33
2.3. Поняття та ознаки комерційної таємниці. Об'єкти та суб'єкти права власності на комерційну таємницю .....	58
2.4. Система правового захисту комерційної таємниці підприємства, її елементи та складові .....	65
2.5. Юридичне закріплення права підприємства на комерційну таємницю .....	69
2.6. Визначення відомостей, що складають комерційну таємницю підприємства .....	74
2.7. Допуск та доступ до комерційної таємниці .....	79
2.8. Правове регулювання порядку збереження комерційної таємниці при укладанні господарських договорів, веденні ділових переговорів. Перевірка ділових партнерів .....	85
2.9. Відповідальність за порушення законодавства про комерційну таємницю .....	88
Питання для самоконтролю .....	91

### **Розділ 3. Економічна розвідка (економічне шпигунство)**

3.1. Економічна розвідка як фактор у конкурентній боротьбі. ....	92
3.2. Організація та ефективність економічної розвідки. ....	99
3.3. Методи шпигунства (методи збирання інформації). ....	110
3.3.1. Легальні методи збирання інформації. ....	110
3.3.2. Напівлегальні методи збору інформації. ....	113
3.3.3. Нелегальні методи збору інформації. ....	116
3.4. Канали витікання інформації. ....	121
3.5. Дані про ділових партнерів та конкурентів. ....	124
3.6. Технічні засоби збирання інформації. ....	126
3.6.1. Технічні засоби і збирання розвідувальних даних. ....	126
3.6.2. Аудіо- і радіотехніка в розвідувальній роботі. ....	127
3.6.3. Відеотехніка в розвідці. ....	132
3.6.4. Комп'ютерна розвідка. ....	133
Питання для самоконтролю. ....	137

### **Розділ 4. СИСТЕМА ЗАХИСТУ ПІДПРИЄМСТВА**

4.1. Загальні положення і класифікація заходів захисту. ....	138
4.2. Проблеми захисту підприємницької діяльності та організація захисту в розвинутих країнах. ....	141
4.3. Завдання забезпечення захисту підприємництва в Україні. ....	145
4.4. Служба економічної безпеки підприємства. ....	147
4.5. Способи захисту від економічного шпигунства. ....	153
4.6. Комплексна система заходів захисту підприємництва. ....	156
4.6.1. Основні завдання щодо захисту підприємництва. ....	156
4.6.2. Системи заходів забезпечення безпеки. ....	158
4.6.3. Організація захисту об'єктів підприємництва. ....	159
4.6.4 Програма захисту комерційної таємниці підприємства. ....	161
4.7. Технічні засоби захисту бізнесу. ....	161
Питання для самоконтролю. ....	173

<b>ДОДАТКИ</b> .....	175
----------------------	-----

<b>ПЕРЕЛІК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ</b> .....	248
--	-----

## ВСТУП

Наша країна переживає складний період свого розвитку. Об'єктивно необхідні зміни в переважній більшості сфер суспільного життя відбуваються з великими труднощами. Перехід до нових форм державного управління та господарювання в умовах неузгодженості правової бази, відсутності науково обґрунтованої концепції реформ, політична нестабільність та ірраціональність мислення породили цілий ряд проблем, загострення яких висуває насамперед проблему забезпечення національної безпеки держави.

Ситуація, що склалась у суспільстві та в економічній системі, викликала багато непередбачуваних небезпек і загроз для підприємництва, яке ще не має необхідного досвіду. Окрім того, ситуація погіршується за рахунок розкрадання, корупції, шахрайства, криміналізації бізнесу, фальсифікації тощо.

У навчальному посібнику розглянуті питання, пов'язані із забезпеченням збереження промислової та економічної таємниці. Раніше цією проблемою в нашій країні (як і в усіх країнах колишнього СРСР) займались державні служби безпеки, а тепер своєю безпекою повинно опікуватись кожне підприємство окремо.

Досвід показує, що економічне та промислове шпигунство можуть завдати підприємству шкоди не меншої ніж економічна криза, необґрунтоване управлінське рішення тощо. На жаль, цим питанням надається все ще мало уваги, оскільки, по-перше, наслідки шпигунства, як правило, виявляються не відразу; по-друге, недостатність знань у вітчизняних підприємців призводить до того, що вони не можуть організувати ефективну власну службу безпеки. Окрім того, необхідної літератури в даній галузі практично немає, державні органи безпеки своїми напрацюваннями ділитись не хочуть, а шлях через власні помилки може коштувати підприємцю дуже дорого.

Все це вимагає, щоб підприємці, менеджери, фінансисти, економісти різних рівнів знали теорію економічної безпеки, розуміли суть еконо-

мічної безпеки підприємства, її структуру, об'єкти економічної безпеки, основні небезпеки та загрози, кількісні та якісні показники оцінки рівня економічної безпеки, основні напрями забезпечення безпеки, а також вміли застосовувати на практиці теоретичні положення.

Без сумніву, забезпечення економічної безпеки підприємства повинно спиратись на існуючі закони, мати правову основу. Однак законодавча база забезпечення безпеки розроблена недостатньо, а більшість нормативних актів, що впливають на результативність господарської діяльності, змінюються дуже швидко.

Економічне, промислове та комерційне шпигунство знаходиться у тісному взаємозв'язку з багатьма галузями знань. А оскільки основним носієм знань є людина, то для успішного ведення бізнесу керівнику (власнику) підприємства необхідно встановити відповідні відносини зі своїми працівниками.

В умовах ринкової економіки підприємство не може ефективно працювати, не маючи найновішої інформації про стан ринку, діяльність конкурентів тощо. Для продуктивного ведення господарської діяльності керівництву підприємства необхідно приймати рішення різного рівня, інформаційну підтримку яких забезпечує система економічної розвідки.

Окрім того, кожного інвестора, зарубіжного бізнесмена нерідко хвилює незахищеність вітчизняних підприємств від промислового та комерційного шпигунства. Тому необхідно на підприємствах створювати надійну програму захисту технологій, розробок, ноу-хау, стратегічно важливої інформації тощо.

Саме для поглиблення теоретичних знань з вирішення вищенаведених завдань пропонується даний навчальний посібник.

Сподіваємося, що дана робота буде корисна студентам економічних спеціальностей, менеджерам, маркетингологам, керівникам підприємств, співробітникам служб економічної безпеки підприємств.

# Розділ 1. ЕКОНОМІЧНА БЕЗПЕКА

## 1.1. Поняття економічної безпеки

Україна проходить складний історичний період державного становлення. Маємо визнати, що переважна більшість важливих рішень, які закладали основи стратегічного економічного розвитку Української держави після набуття нею незалежності, часто приймалися спонтанно, без належного наукового обґрунтування (під гаслом “ринок все відрегулює”) і врахування національних інтересів. Тому перші роки існування Української держави позначені руйнуванням значного економічного потенціалу, що дістався їй у спадок. Як наслідок, економічний потенціал України, який є матеріальною основою національної безпеки, надто ослаблений.

Також не можна забувати, що Україна як незалежна держава існує у взаємопов’язаному та взаємозалежному світі, де все яскравіше проявляється домінанта міжнародного співробітництва, інтеграції господарської діяльності, економічної та соціальної політики. Водночас не припиняється запекла боротьба за контроль над обмеженими ресурсами і транспортними коридорами. Спостерігається жорстке суперництво національних економік, наднаціональних угруповань і транснаціональних утворень у відстоюванні власних інтересів. Ситуація постійно загострюється через відсутність аналізу нового міжнародного економічного порядку у розв’язанні глобальних господарських проблем.

Тому перед Україною постало питання, що полягає у певному протиріччі між необхідністю інтегруватися у світову економіку, з одного боку, та забезпеченням внутрішньої економічної інтеграції, захистом свого внутрішнього ринку, власного товаровиробника і національних інтересів, з іншого.

Тож лише створення *власної системи економічної безпеки* дасть можливість забезпечити захист національної економіки, її конкурентоспроможність, вітчизняного товаровиробника й ефективно взаємодіяти з міжнародними фінансовими та економічними структурами.

Проблема економічної безпеки України має кардинальне значення не лише в рамках сфери національної безпеки, а й у контексті загального рівня розвитку країни. Це зумовлює виняткову увагу до проблеми економічної безпеки держави, яка поєднує питання розвитку окремих галузей економіки України із пріоритетами та національними інтересами держави.

Добре відоме в практиці діяльності управлінських структур західних країн поняття *економічної безпеки* практично не досліджене вітчизняними науковцями. Так, наприклад, у науковій праці російської академії ім. Г.В. Плеханова “Основи економічної безпеки” вона визначається як “стан, в якому народ (через державу) може суверенно, без втручання і тиску ззовні, визначати шляхи і форми свого економічного розвитку”.

У редакції Національного інституту стратегічних досліджень України під *безпекою* у загальному плані мається на увазі захищеність країни від наявних чи потенційно можливих загроз.

У науковій роботі Інституту систем енергетики ім. Л.О. Мелентьєва, присвяченій визначенню основних засад проблеми економічної безпеки держави, вона визначається як стан захищеності життєво важливих інтересів особи, суспільства й держави від зовнішніх і внутрішніх загроз. При цьому життєво важливими інтересами вважається сукупність потреб, задоволення яких забезпечує існування і можливість прогресивного розвитку особи, суспільства і держави.

➔ Підсумовуючи усі попередні тлумачення, визначимо *економічну безпеку* як загальнонаціональний комплекс заходів, спрямованих на постійний і стабільний розвиток економіки держави, що включає механізм протидії внутрішнім та зовнішнім загрозам.

Забезпечення економічної безпеки держави — один з головних напрямків діяльності державного управління. Тому науку про економічну безпеку мають добре засвоїти державні службовці вищого рівня управління.

До *основних принципів забезпечення економічної безпеки* України відносять:

- дотримання законності на всіх етапах забезпечення економічної безпеки;
- баланс економічних інтересів особи, сім’ї, суспільства, держави;
- взаємну відповідальність особи, сім’ї, суспільства, держави щодо забезпечення економічної безпеки;
- своєчасність і адекватність заходів, пов’язаних із відверненням загроз і захистом національних економічних інтересів;

- надання пріоритету мирним заходам у вирішенні як внутрішніх, так і зовнішніх конфліктів економічного характеру;
- інтеграцію національної економічної безпеки з міжнародною економічною безпекою.

За рівнем теорія розрізняє такі види економічної безпеки: **міжнародну** (глобальна і регіональна), **локальну** (регіональна або галузева всередині країни) і **приватну** (фірм і окремих осіб).

➔ **Міжнародна економічна безпека** — це комплекс міжнародних умов співіснування домовленостей та інституціональних структур, за яких кожній державі — члену світової спільноти забезпечується можливість вільно обирати і здійснювати свою стратегію соціального та економічного розвитку, не зазнаючи зовнішнього тиску і ризиковуючи на невтручання, розуміння та взаємоприйнятну і взаємовигідну співпрацю з боку інших держав.

Міжнародна економічна безпека має сприяти співробітництву держав у вирішенні не лише їхніх національних проблем, й глобальних проблем людства, стати матеріальною основою мирного співіснування в без'ядерному і ненасильницькому світі, гарантією прогресу у справі ліквідації економічного відставання та слаборозвинутості.

➔ **Глобальна безпека** має своєю основною метою гарантію безпеки відразу усієї світової спільноти, а не тільки окремих регіонів і країн.

В основу її побудови було закладено трансформацію взаємозв'язків, що діяли раніше між окремими країнами, в одну загальну глобальну систему.

➔ **Економічна безпека підприємства** — це система створення механізму мобілізації й найбільш оптимального управління корпоративними ресурсами даного підприємства з метою найбільш ефективного їх використання і забезпечення стійкого функціонування того чи іншого підприємства, його активної протидії будь-яким негативним чинникам впливу на свою економічну безпеку.

Економічну безпеку підприємства складають юридичні, виробничі відносини і організаційні зв'язки, матеріальні й інтелектуальні ресурси, що забезпечують стабільність його функціонування, фінансово-комерційний успіх, прогресивний науково-технічний і соціальний розвиток.

## 1.2. Предмет, об'єкт, суб'єкт економічної безпеки

**Об'єктами економічної безпеки** є держава, суспільство, сім'ї, окремі громадяни, підприємства, установи, організації, окремі території, а також основні елементи економічної безпеки.

Водночас держава є не лише об'єктом, й основним суб'єктом національної економічної безпеки і здійснює свої функції в цій сфері через органи законодавчої, виконавчої та судової гілок влади. В Конституції України чітко зазначено, що поряд із захистом суверенітету і територіальної цілісності України забезпечення її економічної безпеки є найважливішою функцією держави і справою всього українського народу.

- ⊙ *Таким чином, економічній безпеці притаманний інтегральний характер, оскільки вона є результатом спільних зусиль усього народу, і це проявляється через дії всіх гілок влади на всіх рівнях (від центрального до місцевого), наявних у державі сил і засобів, об'єднаних громадян і окремих осіб.*

**Суб'єктами економічної безпеки України** є функціональні і галузеві міністерства та інші органи державної влади, податкові й митні служби, банки, біржі, фонди і страхові компанії, а також виробники робіт і послуг, продавці продукції і вітчизняні споживачі.

**Предметом** державної діяльності в галузі економічної безпеки є:

- визначення і моніторинг факторів, що підривають стійкість соціально-економічної системи і держави в короткотерміновій і довготерміновій перспективі;
- формування економічної політики та інституціональних перетворень, що усуватимуть або пом'якшуватимуть шкідливий вплив виявлених факторів у рамках єдиної програми економічної реформи.

**Стратегія** економічної безпеки передбачає:

- визначення характеристики зовнішніх і внутрішніх загроз економічній безпеці як сукупності умов і чинників, що створюють небезпеку життєво важливим економічним інтересам особистості, суспільства і держави;
- визначення критеріїв і параметрів стану економіки, що відповідають вимогам економічної безпеки і забезпечують захист життєво важливих інтересів країни;

- формування механізму забезпечення економічної безпеки країни, захисту її життєво важливих інтересів на основі застосування усіма інститутами державної влади правових, економічних і адміністративних заходів впливу.

Практична реалізація державної стратегії економічної безпеки повинна здійснюватися через систему конкретних заходів, механізмів, що реалізуються на основі якісних індикаторів і кількісних показників соціально-економічного розвитку країни. Така система складає основу і зміст економічної політики держави.

При створенні системи економічної безпеки першочергове значення має визначення **національних економічних інтересів (НЕІ) України**, адже саме від цього залежить вироблення ефективних засобів їх реалізації та захисту.

**Національні інтереси України** відображають фундаментальні цінності та прагнення українського народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення і способи досягнення.

Кожна суверенна країна має власні національні інтереси, які не збігаються з інтересами інших країн, а в ряді випадків і альтернативні їм. Це є об'єктивним наслідком нерівномірності суспільного розвитку і дає підстави стверджувати, що боротьба між країнами ведеться постійно, а її характер (змагання чи антагонізм) обумовлюється наявністю й величиною конфліктного потенціалу.

- ➔ В ролі виразника і гаранта захисту НЕІ повинна виступати держава. Національні цінності, інтереси і цілі — триада першоджерел, основних рушійних сил системи економічної безпеки, що визначає її зміст, характер, конфігурацію, спрямування.

Для **створення цілісної системи НЕІ** та її ефективного функціонування насамперед необхідно:

- створити відповідну нормативну базу;
- проводити моніторинг НЕІ та їх моделювання;
- створити банк даних НЕІ;
- забезпечити баланс НЕІ та їх гармонійне поєднання.

Національні інтереси України та їх пріоритетність обумовлюються конкретною ситуацією, що складається в країні та за її межами.

Але головний інтерес України полягає в тому, щоб посісти таке місце у світовому розподілі праці, міжнародній торгівлі та фінансах, яке б від-

повідало її природним, трудовим та інтелектуальним ресурсам, сприяло реалізації потенціалу великої європейської держави.

- ⊙ *Загрозами економічній безпеці України слід вважати явні чи потенційні дії, що ускладнюють або унеможливають реалізацію національних економічних інтересів і створюють небезпеку для соціально-економічної та політичної систем, національних цінностей, життєзабезпечення нації та окремої особи.*

Загрози економічній безпеці України набули перманентного характеру і за цілим рядом основних критеріїв перейшли критичну межу. Тому завдання полягає не лише у виході з економічної кризи, а й у відродженні національної економіки, створенні надійної економічної системи, забезпеченні її життєздатності й розвитку, спроможності адаптуватися до нових економічних умов.

Критична межа критеріїв — це граничні величини показників економічної безпеки, недотримання значень яких перешкоджає нормальному ходу розвитку різних елементів відтворення, призводячи до формування негативних, руйнівних тенденцій в економічній безпеці.

### **1.3. Економічна безпека держави**

Гарантом економічної та політичної незалежності держави є економіка. Спостерігається пряма залежність між рівнем розвитку економічного потенціалу держави і ступенем її залежності від міжнародних ринків та впливу економіки інших держав.

#### **Елементи економічної безпеки держави:**

Перерахуємо основні складові економічної безпеки держави. [93]

1. Наявність власних управлінських кадрів на всіх рівнях управління.
2. Економічно обґрунтована бюджетно-фінансова політика держави.
3. Наявність розвинутої економічної інфраструктури: господарюючих суб'єктів — вільних підприємців, фермерів, малих, середніх та великих підприємств; банківської мережі; страхових, інвестиційних та інших фондів; товарних бірж й інших організацій і посередників, які функціонують на ринках.
4. Внутрішні інвестиції.

5. Мобілізаційна підготовка економіки, території та комунікацій. Першочергове значення тут мають стратегічні матеріали і товари, необхідні для національної оборони.
6. Державні резерви.
7. Система стандартизації. В розвинутих країнах стандартизація ефективно вписується в загальні механізми господарювання і регулювання економіки. Невідповідність національних стандартів міжнародним вимогам знижує інтеграційні та економічні можливості країни.
8. Правовий захист суб'єктів підприємницької діяльності в даній державі. Цей факт прямо впливає на економічну безпеку регіонів, підприємництва в цілому та підприємців зокрема. В якості прикладу можна розглянути межі економічної безпеки в сфері валюти. В Україні рішенням Національного банку в 1998 р. були встановлені межі валютного коридору гривні в межах 1,7–2,25 до долара США. Це, по суті, є межею економічної безпеки України. Подібним заходом досягається стабільність на валютному ринку, забезпечується захист вітчизняних виробників, заощаджень населення, стимулювання внутрішніх інвестицій.

### **Загрози економічній безпеці держави**

Україна отримала від колишнього Радянського Союзу гіпертрофовану структуру народного господарства, державний монополізм у системі управління в усіх сферах, технологічну відсталість виробництва, значну імпорتنу залежність від постачання енергоресурсів та інших стратегічно важливих товарів і сировини.

Перерахуємо основні фактори, які складають загрозу економічній безпеці держави [93].

1. Звертання наукомістких виробництв.
2. Відсутність розвинутої банківської системи та системи страхування, а також гарантійних організацій.
3. Дефіцит державного бюджету та інфляція.
4. Велика частина вивезеного за межі країни капіталу; занадто великий вивіз стратегічно важливих товарів та ресурсів; зниження вартості підприємств, що приватизуються, в тих випадках, коли вони продаються зарубіжним підприємцям.
5. Непомірно високі податки на виробника, за допомогою яких придушється власний виробник і відкривається шлях для захоплення вітчизняного ринку іноземними виробниками. При цьому за-

гроза економічній безпеці криється ще й в тому, що виробники зацікавлені приховувати дійсні обсяги виробництва, щоб уникнути сплати непомірно високих податків.

6. Низький рівень достовірності статистичних даних в економіці. Офіційна державна статистика України з року в рік фіксує падіння виробництва в державному секторі економіки. Одночасно органи статистики не можуть налагодити облік виробництва продукції та послуг новоствореними підприємствами, фірмами і окремими підприємцями. Так, колективні і приватні торговельні підприємства України впродовж декількох років багаторазово збільшили товарообороти, підвищили якість торговельних послуг, а державна статистика постійно фіксує зниження цих показників в цілому по державі. Недостовірна інформація наносить значної шкоди державі: вона деморалізує населення, викликає недовіру потенційних іноземних і вітчизняних інвесторів, сприяє витіканню капіталів з країни, створює передумови для спекулятивного маніпулювання інформацією в інтересах окремих груп населення, в першу чергу консерваторів та противників економічних реформ.
7. Злидні та бідність більшої частини населення, високий рівень безробіття, страйки.

#### **1.4. Економічна безпека регіону**

Економічна безпека регіону залежить від його ресурсного та виробничого потенціалу, інвестиційного забезпечення, ступеня економічної свободи регіонів в державі, регіональної бюджетно-фінансової політики, рівня розвитку ринкової інфраструктури, наявності підготовлених кадрів для місцевого самоврядування.

- ➔ Економічна безпека регіону характеризується ступенем можливості формування ним власної економічної політики з врахуванням його специфіки та не на шкоду державі. При цьому першочергове значення має розподілення функцій управління між централізованою державною владою та регіональним управлінням. Світовий досвід свідчить, що децентралізація призводить до економічного розвитку регіонів, підвищення конкурентоспроможності господарюючих суб'єктів, зростання життєвого рівня населення регіонів, появи місцевої ініціативної еліти [93].

**Загрози економічній безпеці регіону [93].**

1. Відсутність правової бази, яка регламентує права і обов'язки регіонів. Недосконалість або відсутність правової бази стає причиною конфліктних ситуацій, подібних до тих, що виникли в Росії – Чечня, Італії – П'ємонт або Сицилія, Україні – Кримська Автономія, Англія – Північна Ірландія. Цей перелік може бути продовжений.
2. Бюджетно-фінансова політика. В економічно розвинутих державах (США, ФРН, Японія) на долю місцевих фінансів припадає 50–60% фінансових ресурсів цих держав. Україна поки істотно відстає стосовно цього від розвинутих держав.

Для забезпечення економічної безпеки регіонів необхідне створення мережі регіональних банків; надання регіонам права проведення позик і лотерей, стягнення місцевих податків і зборів; складання вільного регіонального фінансового балансу; формування спеціальних фондів; забезпечення фінансової стабільності підприємств, що знаходяться у власності регіональних органів управління.

3. Відсутність або недостатній розвиток економічної інфраструктури, в першу чергу господарюючих суб'єктів – підприємств та підприємств. Рішення цієї проблеми в більшості залежить від регіонів та їх політики сприяння підприємництву.
4. Незадовільний рівень підготовки управлінських кадрів, засилля консервативних керівників – противників економічних реформ та перетворень, особливо в агропромисловому комплексі.
5. Незадовільно поставлена робота по розтлумаченню широким масам населення суті економічних реформ, а також відпрацюванню у населення свідомості господаря свого регіону і держави в цілому.

Розроблена Міністерством економіки України економічна концепція регіональної політики передбачає надання регіонам більшої економічної самостійності, створення вільних економічних зон, проведення обґрунтованої бюджетної політики, оптимального розміщення продуктивних сил. Крім того, необхідно підготувати кадри управлінців, які розуміють завдання сучасного економічного розвитку і здатні вирішувати їх.

## 1.5. Поняття економічної безпеки підприємництва

Економічна безпека підприємництва залежить передусім від наявності правової системи його захисту та ефективного механізму забезпечення її реалізації. Гарантом економічної безпеки підприємництва є держава.

Важливим фактором безпеки підприємництва є методи економічного регулювання зі сторони держави, і, в першу чергу, — податкова політика та податкова система. Основна умова безпеки підприємництва — стабільність податкової політики.[93]

Безпека підприємництва залежить від ступеня втручання держави в економіку. Якщо держава майже не втручається в економіку, це є модель класичного капіталізму. Якщо ж вона втручається майже в усі економічні процеси, це є модель державного соціалізму, який існував в СРСР протягом багатьох десятиріч.

В Україні в умовах радикальних економічних перетворень все більшого значення набувають питання захисту підприємництва.

- ⊙ *Економічна безпека підприємництва є одним з необхідних принципів підтримання стійкості економічного і соціального становища, підвищення обороноздатності, виключення можливостей виникнення соціальних, трудових, міжнаціональних та інших конфліктів, які загрожують безпеці держави [93].*

Значне місце в економіці країни займають недержавні господарюючі суб'єкти — акціонерні і комерційні банки, акціонерні товариства, приватні та спільні підприємства, які стійко розвивають власне виробництво продукції і послуг. Будучи порівняно новими структурами у вітчизняній економіці, вони вже здійснили істотний вплив на економіку держави, беруть участь в розвитку сучасних технологій, розширенні експорту, створенні нових робочих місць, збільшенні податкових надходжень до бюджету.

Але повсякденна практика господарюючих суб'єктів свідчить про їх підвищену, в порівнянні з державними структурами, уразливість від протиправних та інших дій зі сторони різного роду кримінальних структур й окремих осіб. Забезпечення безпеки підприємництва стає життєво важливою потребою, одним з базових принципів його функціонування. Напружена криміногенна ситуація в країні, поява в Україні активно діючих структур економічної розвідки, міжнародної організованої злочинності, скрізь застосовуваних жорстких методів впливу на підприємницькі

структури визначають актуальність проблеми безпеки підприємництва на найближчу перспективу [93].

З урахуванням складної політичної та економічної ситуації в Україні вже сформувався інтерес до проблеми захисту об'єктів економіки від намагань організованої злочинності, промислового шпигунства та інших правопорушень, збереження комерційної таємниці, а також функціонування недержавних служб безпеки.

Разом з тим до теперішнього часу не склалася єдина точка зору з питань комплексного, системного підходу до забезпечення безпеки об'єктів економіки, механізмів і принципів створення та функціонування служб безпеки об'єктів, їх взаємодія між собою і з правоохоронними органами. У значного числа керівників підприємницьких структур не сформовано розуміння принципу забезпечення безпеки як одного з базових в економічній діяльності, через що на практиці проблема безпеки нерідко вважається другорядною [93].

В умовах ринкової економіки підприємства функціонують в умовах невизначеності, непередбачуваності. Тривала і глибока економічна криза в нашій країні спричинила багато непередбачуваних небезпек та загроз для ще молодого бізнесу. Крім того, на розвиток підприємництва впливають ще й такі фактори, як нестабільна політична та соціально-економічна ситуація в країні, недосконале комерційне законодавство, криміналізація суспільства, влади та бізнесу, корупція, шахрайство тощо. Все це різко загострило проблему забезпечення економічної безпеки підприємства.

Найчастіше забезпечення економічної безпеки бізнесу зводять до протистояння, захисту від різноманітних економічних злочинів (пограбування, шахрайство, фальсифікація, підпали, недобросовісна конкуренція, промислове та комерційне шпигунство, інформаційна безпека тощо). Безсумнівно, ці загрози дуже важливі і повинні постійно аналізуватись та враховуватись, але поняття економічної безпеки підприємства має більш широке значення.

➔ **Економічна безпека підприємства** [36] — це такий стан господарюючого суб'єкта, при якому він при найбільш ефективному використанні наявних ресурсів досягає запобігання, послаблення або захисту від існуючих небезпек та загроз або інших непередбачуваних обставин і в основному досягає цілей бізнесу в умовах конкуренції та господарського ризику.

Таке визначення економічної безпеки підприємства дозволяє показати, що підприємство, яке знаходиться в ситуації невизначеності, непередбачуваності, зміни як внутрішніх умов господарювання, так і зовнішніх: політичних, макроекономічних, екологічних, правових — приймає ризикові рішення в умовах жорсткої конкуренції, досягає запобігання, послаблення або захисту від існуючих або прогнозованих небезпек та загроз; що в даних умовах воно забезпечує досягнення цілей бізнесу. В даній ситуації ресурси підприємства (земля, капітал, праця, підприємницькі здібності, інформація, інтелектуальна власність, технології тощо) використовуються не лише для запобігання небезпекам та загрозам, а передусім для досягнення цілей бізнесу. Виявлення, попередження небезпек та загроз, використання ресурсів для запобігання нанесенню шкоди, прийняття ризикових рішень, боротьба з конкурентами тощо — це шлях для досягнення стратегічних цілей бізнесу.

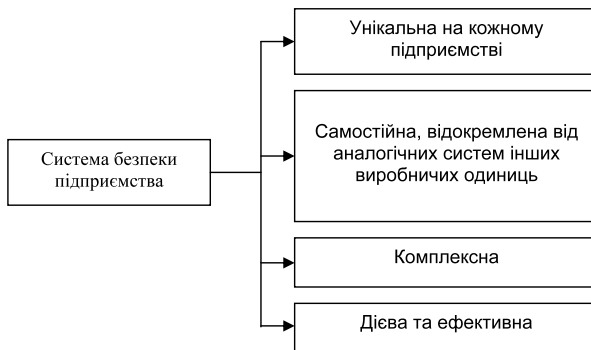
- ⊙ *Перехід до ринкової економіки, створення значної кількості підприємств, виникнення різноманітних способів конкурентної боротьби, недосконале законодавство, слабкість та корумпованість державних структур, криміналізація господарської діяльності та інші причини створили господарюючим суб'єктам умови, в яких вони вимушені приділяти значну увагу питанням забезпечення власної економічної безпеки [36].*

В умовах соціалістичної планової економіки майже всі підприємства базувались на державній формі власності, держава жорсткими централізованими адміністративними заходами регулювала економічні процеси. За таких умов недобросовісна конкуренція, промислове шпигунство, ретет, корупція, організована економічна злочинність, тіньова економіка мали значно менші масштаби, ніж тепер. Для боротьби з такими проявами використовувались державна система правоохоронних органів та державні служби безпеки.

Все це свідчить, що проблема економічної безпеки бізнесу соціалістичної економіки була не настільки актуальною, як в умовах ринкової системи господарювання.

У даній економічній ситуації виробничі одиниці мають повну економічну самостійність, вони самі визначають свою економічну політику, організовують виробництво та збут продукції, повністю відповідають за результати господарської діяльності. Це ще раз говорить про необхідність забезпечення економічної безпеки в сучасних умовах [36].

Забезпечення економічної безпеки підприємства вимагає створення на підприємстві власної системи безпеки. Даючи характеристику системи економічної безпеки підприємства, слід спочатку визначити деякі методологічні положення [36] (рис.1):



**Рис. 1. Характеристика системи економічної безпеки підприємства**

1. Система економічної безпеки підприємства не може бути шаблонною. Вона має бути **унікальною** на кожному підприємстві, оскільки залежить від особливостей кожного підприємства (рівня розвитку, структури, величини, виробничого потенціалу та ефективності його використання, напряму діяльності, кваліфікації кадрів, виробничої дисципліни, конкурентного середовища, місця розташування, ризикованості виробництва, наявності секретних матеріалів та ступеня їх секретності тощо).
2. Система безпеки підприємства повинна бути **самостійною**, відокремленою від аналогічних систем інших виробничих одиниць. Але її відокремленість відносна. Багато завдань, які постають перед системою безпеки підприємства, не можуть бути виконані самостійно, без необхідних рішень, що приймаються на більш високому рівні, передусім на державному. Служба безпеки конкретного підприємства залежить також від активності протидії служб безпеки конкурентів та, в першу чергу, від їх розвідувальних підрозділів. Вона створюється та функціонує на основі прийнятих законодавчих в країні актів, наявності та можливості придбати за собою захисту, рівня підготовки та кваліфікації кадрів тощо.
3. Система безпеки підприємства повинна бути **комплексною**. Вона покликана забезпечити безпеку економічну, науково-технічну,

кадрову, інтелектуальну екологічну, інформаційну, фізичну, техногенну, пожежну, зв'язку тощо. Враховуючи перераховане, до складу системи економічної безпеки повинні входити відповідні елементи, органи, сили, засоби. Лише комплексність системи економічної безпеки може забезпечити відповідну надійність безпеки підприємства.

4. Але основним положенням є *дієвість та ефективність* економічної безпеки, оскільки унікальність, самостійність та комплексність системи економічної безпеки не дає жодної гарантії, що ця система буде діяти, окрім того, діяти ефективно.

Створення системи безпеки підприємства та організація її успішного функціонування повинні ґрунтуватись на методологічних основах наукової теорії безпеки. Повинні бути визначені цілі системи безпеки підприємства: що необхідно здійснити, чого слід досягти; які завдання необхідно вирішити для досягнення поставлених цілей; які основні функції системи безпеки підприємства — визначити коло діяльності цієї системи. Система безпеки будується на основі певних наукових принципів. Все це слугує методологічною основою створення системи безпеки підприємства.

- ➔ Ціллю системи безпеки є своєчасне виявлення та запобігання як зовнішнім, так і внутрішнім небезпекам та загрозам, забезпечення захищеності діяльності підприємства та досягнення ним цілей бізнесу. [36]

Досягти поставлених цілей можна за допомогою вирішення цілого комплексу завдань. До найбільш значних можна віднести [36]:

- виявлення реальних та прогнозування потенційних небезпек та загроз;
- знаходження способів запобігання їм, послаблення або ліквідації наслідків їх дії;
- знаходження сил і засобів, необхідних для забезпечення безпеки підприємства;
- організація взаємодії з правоохоронними та контролюючими органами з метою запобігання та припинення правопорушень, спрямованих проти інтересів підприємства;
- створення власної служби безпеки підприємства, що відповідає виявленим небезпекам та загрозам тощо.

Система безпеки підприємства покликана виконувати певні функції. До найбільш значних з них слід віднести [36]:

- прогнозування, виявлення, попередження, послаблення небезпек та загроз;
- забезпечення захищеності діяльності підприємства та його персоналу, збереження його майна;
- створення сприятливого конкурентного середовища;
- ліквідація наслідків нанесеної шкоди тощо.

Система економічної безпеки підприємства будується на певних принципах. Найважливіші з них [36]:

- Комплексність, або системність.
- Пріоритет заходів попередження (вчасність).
- Безперервність.
- Законність.
- Плановість.
- Економність.
- Взаємодія.
- Компетентність.
- Поєднання гласності та конфіденційності.

**Комплексність, або системність.** Цей принцип передбачає створення такої системи безпеки, яка забезпечить захищеність підприємства, його майна, персоналу, інформації, різних сфер діяльності від будь-яких небезпек та загроз, непередбачуваних обставин. Тобто система безпеки, її складові елементи, сили, засоби повинні бути достатніми, щоб забезпечити економічну, екологічну, науково-технічну, кадрову, пожежну та інші види безпеки.

- ◎ *У забезпеченні безпеки підприємства повинні брати участь не лише штатні працівники та спеціальні служби, й практично всі співробітники підприємства.*

**Пріоритет заходів попередження (вчасність).** Система безпеки повинна бути побудована таким чином, щоб вона могла на ранніх стадіях виявляти різноманітні деструктивні фактори, вживати заходи щодо попередження їх шкідливого впливу та нанесення збитків підприємству. Реалізація даного принципу економічно значно вигідніша, ніж усунення завданої шкоди.

**Безперервність.** Система безпеки повинна бути побудована таким чином, щоб вона діяла, постійно захищаючи інтереси підприємства в умовах ризику та протидії зловмисникам.

**Законність.** Вся робота із забезпечення безпеки підприємства повинна здійснюватись на основі чинного законодавства та не суперечити йому. Ті заходи безпеки, що розробляються на самому підприємстві, також повинні здійснюватись в межах чинних правових норм.

**Плановість.** Даний принцип вносить організованість у функціонування системи безпеки. Він дозволяє кожному учаснику процесу діяти логічно послідовно, чітко виконуючи покладені на нього обов'язки та вирішуючи поставлені перед ним завдання. Діяльність із забезпечення безпеки організується на основі єдиного задуму, що викладений в комплексній програмі та конкретних планах за окремими напрямками та видами безпеки.

**Економність.** Система безпеки повинна бути побудована таким чином, щоб витрати на її забезпечення були економічно доцільними, а вартість витрат повинна бути оптимальною та не перевищувати той рівень, при якому втрачається економічна доцільність їх застосування.

**Взаємодія.** Для забезпечення безпеки підприємства необхідно, щоб зусилля всіх осіб, що її забезпечують, підрозділів, служб були скоординованими. Всі учасники даного процесу повинні взаємодіяти один з одним. Вони повинні чітко знати, хто за що несе відповідальність і яку роботу виконує. Від узгодженості діяльності всіх учасників процесу залежить успіх справи, кінцевий результат та досягнення поставленої мети.

Принцип взаємодії передбачає також встановлення тісних ділових зв'язків та узгодження дій із зовнішніми організаціями (правоохоронними органами, місцевими та районними службами безпеки, органами влади тощо), що здатні надати необхідну допомогу в забезпеченні безпеки підприємства.

**Поєднання гласності та конфіденційності.** Система основних заходів безпеки повинна бути відома всім співробітникам підприємства, з метою забезпечення безпеки її вимоги повинні виконуватись. Це дозволить вчасно виявити потенційні і реальні небезпеки та загрози та запобігти їм. Одночасно цілий ряд способів, сил, засобів, методів забезпечення безпеки повинні бути засекречені та відомі лише вузькому колу осіб. Це дає можливість більш ефективно боротися як з внутрішніми, так і з зовнішніми загрозами, вчасно запобігати нанесенню шкоди підприємству.

**Компетентність.** Питання забезпечення безпеки підприємства є не другорядним, а життєво необхідним. В результаті дій зловмисників, недобросовісної конкуренції, прийняття дуже ризикованих рішень тощо підприємству може бути нанесено непоправної шкоди, тому питаннями забезпечення безпеки підприємства повинні займатись професіонали, що

знають суть проблеми, вміють вчасно оцінити ситуацію та прийняти правильне рішення.

⊙ *Система безпеки підприємства будується у відповідності до політики, що проводиться, та стратегії безпеки.*

➔ **Політика безпеки** підприємства [36] являє собою систему поглядів, заходів, рішень, дій в галузі безпеки, що створюють умови, сприятливе середовище для досягнення цілей бізнесу.

Тобто, політика безпеки, що проводиться, дозволяє підприємству виконувати виробничу програму, виробляти конкурентоспроможну продукцію (товари, роботи, послуги), підвищувати ефективність виробництва, примножувати власність, отримувати необхідний прибуток тощо.

➔ Під **стратегією безпеки** [61] розуміють сукупність найбільш важливих рішень, направлених на забезпечення програмного рівня безпеки функціонування підприємства.

Стратегії безпеки за своїм змістом бувають різноманітними. Можна виокремити три типи.

1. Стратегія, пов'язана з необхідністю раптового реагування на загрози (виробничій діяльності, майну, персоналу тощо), що виникають. Тобто в даному випадку діє принцип “загроза – відбиття”. Створені (найчастіше поспішно) для вирішення цього завдання підрозділи, служби, виділені сили та засоби можуть послабити або запобігти дії загрози, але може виникнути ситуація, коли підприємству буде завдана шкода.
2. Стратегія, орієнтована на прогнозування, завчасне виявлення небезпек та загроз, цілеспрямоване дослідження економічної та криміногенної ситуації як всередині підприємства, так і в оточуючому його середовищі. Виділені для рішення такого завдання спеціалісти, сформовані підрозділи та служби безпеки створюють можливість свідомо і цілеспрямовано проводити роботу з формування сприятливих умов для підприємницької діяльності.
3. Стратегія безпеки, направлена на відшкодування (відновлення, компенсацію) нанесених збитків. Така стратегія може вважатись доцільною лише тоді, коли збитки можна відшкодувати, або коли немає можливості здійснити стратегію першого та другого типів.

У розумінні “системи безпеки підприємства” не існує єдиної думки [61, 87, 95, 96, 99, 105 та ін]. Наприклад, на погляд В.П. Мак-Мака, система безпеки підприємства включає наукову теорію безпеки, політику та стратегію безпеки, засоби та методи забезпечення безпеки і концепцію безпеки підприємства [61].

В.І. Ярочкін визначає систему безпеки як організовану сукупність спеціальних органів, служб, засобів, методів та заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства, держави від внутрішніх та зовнішніх загроз [105, с.9].

➔ На думку О.А. Груніна та С.О. Груніна [36], система безпеки підприємства являє собою обмежену множину взаємопов’язаних елементів, що забезпечують безпеку підприємства та досягнення ним цілей бізнесу.

Складовими елементами такої системи є об’єкт та суб’єкт безпеки, механізм забезпечення безпеки, а також практичні дії щодо забезпечення безпеки. Розглянемо ці елементи детальніше (рис. 2) [36].

**Об’єктом безпеки** виступає все те, на що спрямовані зусилля щодо забезпечення безпеки. До них слід віднести:

- А) різноманітні види діяльності підприємства (виробничу, комерційну, управління, постачання, планування тощо);
- Б) майно та ресурси підприємства (фінансові, матеріально-технічні, інформаційні, інтелектуальні тощо);
- В) персонал підприємства, його керівники, акціонери, власники, різноманітні структурні підрозділи, служби, партнери, співробітники, що володіють інформацією, яка становить комерційну таємницю, та інші.

**Суб’єктами безпеки підприємства** є ті особи, підрозділи, служби, органи, відомства, установи, що безпосередньо займаються забезпеченням безпеки бізнесу. Враховуючи багатоаспектність діяльності із забезпечення безпеки підприємства, охопити її забезпечення за допомогою одного-двох органів недостатньо. Тому до суб’єктів безпеки підприємства віднесено багато органів. Всі вони можуть бути класифіковані за різними ознаками.

За приналежністю суб’єкти безпеки можна розділити на дві групи:

- Перша — служби, що займаються цією діяльністю безпосередньо на підприємстві.
- Друга — зовнішні органи та організації.

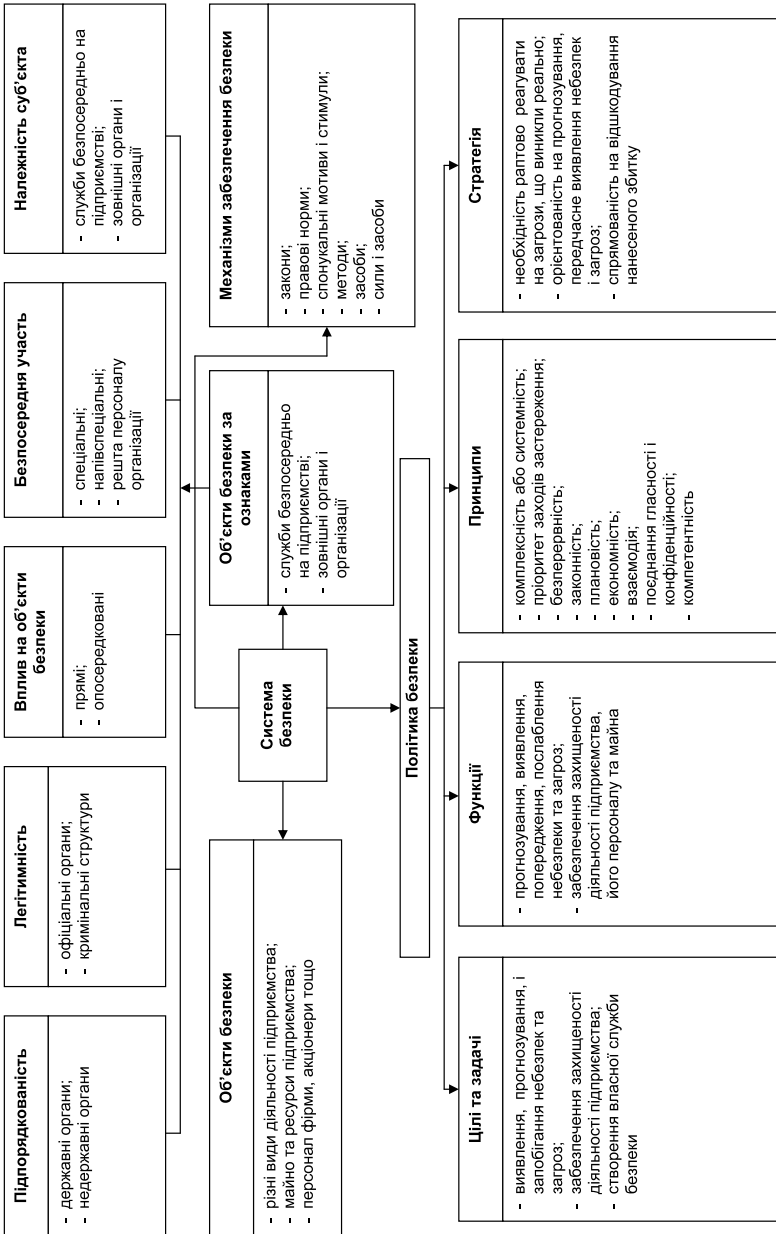


Рис. 2. Система економічної безпеки підприємства

За безпосередньою участю:

- Спеціальні суб'єкти.
- Напівспеціальні.
- Решта персоналу підприємства.

За впливом на об'єкт безпеки:

- Прямого призначення.
- Опосередкованого призначення.

За легітимністю:

- Офіційні органи.
- Кримінальні структури.

За підпорядкованістю:

- Державні органи.
- Недержавні органи.

Синтезувавши подану класифікацію суб'єктів безпеки, можна виокремити дві групи та дати їм характеристику. До першої групи відносяться суб'єкти, що входять до структури самого підприємства та вирішують завдання щодо забезпечення його безпеки. До складу цієї групи входять спеціальні суб'єкти (служба безпеки чи охорона, пожежна команда, рятувальна служба та ін.); напівспеціальні (юридичний відділ, фінансова служба, медична частина та ін.); решта персоналу фірми, який також піклується про безпеку свого підприємства.

До другої групи суб'єктів відносяться ті, що знаходяться за межами підприємства та не підпорядковуються його керівництву [57, 61]. Це передусім державні органи, що створюють умови забезпечення безпеки підприємства. До них відносяться:

- Законодавчі органи, які приймають закони, що створюють правову основу діяльності щодо забезпечення безпеки на рівні держави, регіону, підприємства, особистості.
- Виконавчі органи влади — які проводять політику безпеки, деталізують механізм безпеки.
- Судові органи, які забезпечують дотримання законних прав підприємства та його співробітників.
- Державні інститути, які здійснюють охорону кордонів, митний, валютно-експортний, податковий контроль тощо.
- Правоохоронні органи, які ведуть боротьбу з правопорушеннями та злочинами.
- Система науково-освітніх установ, які реалізують завдання щодо наукового опрацювання проблем безпеки та підготовки кадрів.

З початком ринкових реформ паралельно з державними почали виникати різноманітні приватні охоронні та детективні організації, аналітичні центри, інформаційні служби; навчальні, наукові та консультаційні організації тощо. Вони, як правило, за оплату надають послуги щодо охорони об'єктів, забезпечують захист інформації, комерційної таємниці, накопичують та надають інформацію щодо конкурентів, ненадійних партнерів і т.ін. Світовий досвід свідчить, що в основному саме недержавні організації вирішують завдання щодо забезпечення безпеки підприємства.

- ⊙ *Формування системи безпеки та передусім створення її органів (суб'єктів) залежить від розмірів підприємства, його економічних, фінансових, виробничо-технічних, інформаційних, інтелектуальних, професіональних, організаційних та інших можливостей.*

Як свідчить досвід [99, с.48–53], малі підприємства найчастіше користуються послугами зовнішніх спеціалізованих приватних організацій: консалтингових, охоронних, інформаційних. До них відносяться реєстраційні палати, фірми, що займаються підбором та атестацією кадрів, кредитні бюро, які надають інформаційні послуги щодо ділового реноме партнерів, їх платоспроможності, центри маркетингових досліджень, приватні охоронні й детективні організації та ін.

Середні підприємства можуть використовувати комбіновану систему безпеки: з одного боку, у випадку необхідності отримувати послуги від зовнішніх організацій, з іншого — активно спиратися на можливості власних служб та підрозділів. Наприклад таких, як юридичний та фінансовий відділи, та служб маркетингу, охорони, техніки безпеки, кадрів, економічного аналізу, пропускового режиму, діловодства. З метою підвищення ефективності діяльності служб та підрозділів, які займаються захистом економічних інтересів фірми, на підприємстві повинен бути створений координуючий орган або призначений один з керівників відповідальним за економічну безпеку.

Для великого підприємства доцільним буде створення власної служби безпеки. Як правило, всю діяльність щодо забезпечення безпеки координує один з керівників підприємства. Для вироблення пропозицій та виконання консультативних функцій може створюватись рада з безпеки. Служба безпеки може включати найрізноманітніші відділи, групи, підрозділи. До найбільш значущих слід віднести підрозділи: охорони, режиму, роботи з кадрами, спеціального документообороту з грифом “КТ”,

інженерно-технічного захисту, розвідки та контррозвідки, інформаційно-аналітичної діяльності, оперативного реагування, кризову групу.

Одним з найбільш значимих елементів системи безпеки підприємства є механізм її забезпечення, який являє собою сукупність законодавчих актів, правових норм, рушійних мотивів та стимулів, методів, заходів, сил та засобів, за допомогою яких суб'єкт впливає на об'єкт для досягнення цілей безпеки та вирішення завдань.

Сили та засоби, що використовуються, як правило, розподіляються на декілька груп : фінансові, кадрові, організаційні, технічні, інформаційні, правові, інтелектуальні тощо. За допомогою них вирішуються завдання щодо забезпечення безпеки. Так, наприклад, за допомогою технічних засобів, таких як відео-, радіоапаратура, охоронно-пожежні системи тощо вирішують завдання щодо спостереження за об'єктами. За допомогою організаційних заходів створюють спеціальні підрозділи, зони безпеки, спеціальні пости, патрулі і т. ін. Фінансові засоби необхідні для придбання технічних пристроїв безпеки, утримання служби безпеки, підготовки кадрів, стимулювання праці. Аналогічним чином за призначенням використовуються й інші сили та засоби.

Система безпеки підприємства вирішить завдання, що перед нею поставлені, тоді, коли буде працювати, тобто її невід'ємною складовою є практичні дії щодо забезпечення безпеки бізнесу.

Таким чином, в результаті вивчення сутності економічної безпеки підприємства можна зробити висновок, що вона покликана створити умови для ефективної діяльності підприємства та, в результаті, досягнення цілей бізнесу в умовах конкуренції та господарського ризику, шляхом своєчасного виявлення та послаблення дії різноманітних небезпек та загроз.

### **Питання для самоконтролю**

1. Поняття економічної безпеки.
2. Предмет, об'єкт, суб'єкт економічної безпеки.
3. Економічна безпека держави і регіону.
4. Елементи економічної безпеки держави, регіону.
5. Проблеми забезпечення економічної безпеки держави.
6. Загрози економічній безпеці держави.
7. Загрози економічній безпеці регіону.
8. Поняття економічної безпеки підприємства.

9. Фактори економічної безпеки підприємства.
10. Методологічні положення безпеки підприємства.
11. Принципи системи безпеки.
12. Поняття стратегії безпеки підприємства.
13. Необхідність служби економічної безпеки на підприємстві в сучасних умовах.
14. Досвід зарубіжних держав у забезпеченні безпеки підприємницької діяльності.

## **Розділ 2. ПРАВОВИЙ ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ**

### **2.1. Проблеми правового захисту комерційної таємниці в Україні**

Дане питання розглядалось багатьма авторами, які приділяли увагу темам комерційної таємниці, економічної безпеки та безпеки підприємництва. Найбільш чітко охарактеризувати ситуацію вдалося Г.К. та С.С. Нікіфоровим, бачення яких в основному наведено нижче.

Проблема правового захисту комерційної таємниці в Україні безперечно існує. Вона обумовлюється кількома обставинами: посиленням конкуренції, відсутністю у підприємств достатніх правових знань з організації захисту конфіденційної інформації, а також юридичної літератури та наукових розробок з цієї тематики.

У 1989–2007рр. в Україні виникла значна кількість нових, у тому числі і великих, комерційних та інших структур: різноманітних видів господарських товариств, концернів, довірчих товариств та ін. Навіть поверховий аналіз, свідчить, що багато хто з них поки ще недостатньо серйозно ставиться до забезпечення своєї економічної безпеки, хоча умови, що склалися, та нормативно-правова база об'єктивно зобов'язують керівників підприємств усіх форм власності, підприємців, інших ділових кіл ініціативно та самостійно піклуватись про охорону своїх комерційних таємниць.

Можна бути необ'єктивним, якщо констатувати, що робота з організації забезпечення своєї економічної безпеки підприємницькими структурами взагалі не проводиться. Вона проводиться, але підприємці в більшості випадків використовують лише фізичну й технічну системи охорони.

Однак подібні режимні заходи не дозволяють, чи не повною мірою дозволяють, забезпечити захист конфіденційної наукової, науково-технічної, технологічної інформації, ноу-хау, інтелектуальної власності,

маркетингової, інвестиційної, фінансової та іншої діяльності підприємців, тобто найбільш цінного товару, продукції, послуг у підприємницькій діяльності. А проблема правового захисту цієї інформації важлива вже сьогодні, і її актуальність зростатиме з поглибленням економічних реформ.

Серед підприємців побутує думка, що для організації правового захисту комерційних секретів нині відсутні необхідні умови, зокрема: поки що недостатньо розвинута законодавча база, нібито відсутній предмет захисту та відповідна матеріальна база. Якоюсь мірою таку позицію зрозуміти можна, але для того, щоб її підтримати, немає достатніх підстав. Ось деякі аргументи авторів на противагу такій думці ділових кіл. [67]

**Законодавча база.** Законодавча база існує, хоча не в такому обсязі і не тієї якості, як хотілося б, але вона існує та дозволяє забезпечувати і регулювати правові відносини в питаннях захисту комерційної таємниці. Окремі положення щодо захисту конфіденційної інформації містяться в законах “Про банки та банківську діяльність”, “Про інформацію”, “Про науково-технічну інформацію”, “Про захист економічної конкуренції”, “Про захист від недобросовісної конкуренції”, Господарському кодексі України та інших нормативних актах. Захист комерційної таємниці покликаний забезпечити окремі статті кримінального, цивільного кодексів, кодексу про адміністративні правопорушення та кодексу законів про працю. Достатньо лише полатись на положення нового Кримінального кодексу України, прийнятого Верховною Радою України 5 квітня 2001 р., в якому ст.ст. 231, 232 спрямовані на захист комерційних секретів. [67]

В Україні вже розроблений проект Закону “Про комерційну таємницю” та пройшов перше читання на сесії Верховної Ради України. Хоча подібні цільові закони відсутні в таких країнах з традиційною ринковою економікою, як Великобританія, Франція, Німеччина, Швейцарія, Італія, Канада та ін. У цих країнах захист своїх комерційних секретів фірми забезпечують, як правило, на основі загальних положень кримінального, цивільного та трудового законодавства. На їх основі підприємства створюють власні системи захисту фірмових секретів і конфіденційної інформації й діють вони достатньо ефективно.

Розглядаючи даний аспект, не можна не відзначити разом з тим і ті протиріччя в законодавстві, які стосуються захисту комерційної таємниці. Держава, піклуючись про розвиток ринкових відносин, захищаючи права суб'єктів господарювання на інформацію, в той же час надає представникам багатьох органів державної виконавчої влади право доступу до інформації, що захищається. Достатньо сказати, що більше ніж 30 мі-

ністерств, відомств та державних комітетів наділені правом контролю за окремими сферами діяльності підприємств. Вони виконують покладені на них завдання і функції на підставі цільових законів, які з точки зору правового захисту комерційної таємниці вступили у протиріччя з тими законами, які містять норми, пов'язані з захистом комерційної таємниці підприємства. [67]

**Предмет захисту.** Деякі керівники виробничих та інших підприємств недостатньо обґрунтовано констатують відставання України від розвинутих в економічному відношенні країн і вважають, що вітчизняним підприємствам не слід приховувати від закордонних партнерів, бізнесменів та спеціалістів свої досягнення в галузі науки, техніки, технологій тощо.

Багато технологій, які згадуються американським економістом Томасом Нейлором, — це досягнення вчених та спеціалістів України (зварювання, космічна техніка, виробництво сталі та ін.), і висновки з такої оцінки явні: науковим установам і виробничим підприємствам України є що захищати як комерційну таємницю. До того ж, не можна залишити без захисту сферу зовнішньоекономічної діяльності, послуг, маркетингових досліджень, фінансово-кредитних операцій у банківських та інших системах, тактику і стратегію підприємств на ринку тощо. [67]

**Матеріальні можливості.** Не завжди причиною відмови від організації системи правового захисту комерційної таємниці є відсутність матеріальних засобів. Інколи підприємці просто недооцінюють важливість вкладання коштів у захист своїх секретів, вважаючи, що уникнути витоку інформації вони можуть не звертаючись до засобів захисту.

За інформацією американського журналу “Тайм”, корпорації США щорічно витрачають на забезпечення безпеки понад 1 млрд. доларів, та навіть за цих умов їх збитки від промислового шпигунства становлять 20 млрд доларів на рік. Можна уявити, які б були збитки, якби західні підприємці не вкладали гроші у захист своїх комерційних секретів.

В Україні матеріальні витрати на забезпечення зберігання державних таємниць до останнього часу становили не більше 0,10–0,15% від вартості секретів, що захищаються, що в десятки разів менше, ніж у західних країнах. Даних про витрати на охорону комерційних секретів в Україні по окремих підприємствах поки що немає, але можливо, що вони дещо більші, ніж витрати на захист державних таємниць. Та і цього, мабуть, далеко недостатньо. [67]

## 2.2. Правове регулювання захисту комерційної таємниці за кордоном

У процесі розвитку міжнародного науково-технічного співробітництва з промислово розвинутими країнами питання, пов'язані з купівлею-продажем технології, що включає передачу знань, науково-технічного, комерційного і управлінського досвіду (ноу-хау), набувають актуальності і вимагають комплексного врегулювання, передусім на національному рівні.

У зв'язку з переходом до ринкової економіки в Україні прийнятий пакет важливих законів (про власність, інвестиції, валютне регулювання, банківську діяльність, спільні підприємства тощо). Тому необхідний ефективний захист майнових інтересів володарів ноу-хау не тільки в процесі співпраці із закордонними країнами, й всередині країни, оскільки ліцензійні угоди, угоди про передачу ноу-хау між партнерами стають тим реальним інструментом, на основі якого будуватимуться відносини в галузі обміну науково-технічними досягненнями. [18]

В країні зроблені кроки до становлення інституту комерційної таємниці. Законодавець у цивільному, господарському, кримінальному кодексах, законах про захист економічної конкуренції і захист від недобросовісної конкуренції закріпив основні принципи забезпечення прав володарів такої інформації.

Промислово розвинутими країнами, зокрема ФРН, США, Великобританією, Канадою, Японією, Швейцарією, накопичений великий законодавчий досвід у регламентації відносин щодо захисту комерційної таємниці. Тому вивчення і аналіз форм правового забезпечення майнових інтересів володарів торгових секретів, ноу-хау в таких країнах дозволяють більш цілеспрямовано і продуктивно підійти до моделювання спеціального законодавства, дуже слабкого нині в Україні.

- ➔ Аналіз чинного законодавства в даній галузі права показує, що майнові інтереси власників виробничих, торгових, ділових секретів, ноу-хау охороняються нормами цивільного, торгового, кримінального, трудового права, законодавства про недобросовісну конкуренцію.

У раді країн (наприклад США) діє спеціальне законодавство, що об'єднує правила поведінки зацікавлених осіб в галузі використання торгових або ділових секретів. У країнах прецедентного права (Великобри-

танії, США) для вирішення суперечок сторін притягуються прецедентні судові й адміністративні рішення.

В країнах кодифікуючого права (ФРН) відношення регулюються правилами, включеними в закони, що відносяться до різних законодавчих галузей. У країнах прецедентного права разом з традиційними для них формами регулювання відносин за допомогою прецедентних судових і адміністративних рішень, діють спеціальні закони. [18]

Наведемо перелік нормативних актів і прецедентних рішень, що використовуються для регулювання відносин з приводу вказаних об'єктів.

Країна	Джерела права
<b>США</b>	Уніфікований закон про ділові секрети. §§ 757–759 першого Зведення деліктного права 1939 р. Зведення законів США, ч. 35 § 284. Закон США про економічне шпигунство 1996 р.
<b>ЯПОНІЯ</b>	Цивільний кодекс. Цивільно-процесуальний кодекс. Кримінальний кодекс про припинення недобросовісної конкуренції. Комерційний кодекс. Патентний закон Японії.
<b>ВЕЛИКОБРИТАНІЯ</b>	Основним джерелом є прецедентне право. Закон про обмеження торгової практики. Закон про арбітраж. Закон про порушення конфіденційності.
<b>ФРН</b>	Закон про заборону обмежень конкуренції. Закон про заборону недобросовісної конкуренції. Патентний закон. Закон про винаходи службовців. Торговий кодекс. Кримінальний кодекс. Німецьке цивільне укладення.
<b>ШВЕЙЦАРІЯ</b>	Федеральний Закон “Про недобросовісну конкуренцію”
<b>УГОРЩИНА</b>	Закон про заборону недобросовісної ринкової поведінки
<b>ЧЕХІЯ І СЛОВАЧЧИНА</b>	Торговий кодекс

<b>БОЛГАРІЯ</b>	Закон про захист конкуренції
<b>ПОЛЬЩА</b>	Закон про боротьбу з недобросовісною конкуренцією

Аналіз чинного права показав, що визначення поняття “ноу-хау” є тільки в законодавстві Великобританії, а в інших відібраних для аналізу країнах воно існує в доктрині.

Загальним для всіх визначень поняття є те, що до **ноу-хау відносяться технічні прийоми і виробнича інформація**. [18]

В окремих країнах вважають, що інформація, яка входить в обсяг даного поняття, повинна мати секретний характер (думка Комітету із вивчення патентної системи і патентного права Великобританії) або може бути як секретною, так і несекретною (більшість судових інстанцій Великобританії, доктрина Великобританії, ФРН). [18]

По суті як предмети-носії інформації ноу-хау можуть співпадати з діловими, торговими, виробничими, комерційними секретами, тобто носієм ноу-хау може виступати різна ділова і технічна документація.

На відміну від невизначеної ситуації з поняттям “ноу-хау” поняття “діловий”, “виробничий”, “торговий” секрети більш менш чітко визначаються національними законодавствами США, ФРН, Угорщини.

Зауважимо, що в США регулюються відносини з приводу *ділових секретів*, у ФРН — *виробничих секретів*, в Угорщині — *виробничих і ділових секретів*. У Канаді підготовлений проект Закону про охорону торгових секретів. [18]

З порівняння визначень вказаних понять у законах цих країн видно, що **“діловий секрет”**, за визначенням закону США, включає різні види технічної інформації (формула, пристрій, метод, техніка і спосіб виробництва). Відповідно до угорського закону, технічна інформація входить в поняття “виробничий секрет”. “Діловий секрет” за японським правом включає інформацію про способи виробництва, продаж або будь-яку інформацію про технологію і бізнес. Проте в Канаді інформація, що стосується продажу, охоплюється поняттям “торговий секрет”.

- ⊙ *Таким чином, можна відзначити різноманітність підходів і формулювань, з чим, поза сумнівом, доведеться рахуватись у зовнішньоторговельних операціях.* [18]

Термін **“ноу-хау”** вперше був застосований в США у 1916 р. в судовій справі Дюранда проти Брауна. Він знайшов застосування в правовій

літературі більшості зарубіжних країн [63]. Дослівний переклад терміна означає “знати як” (скорочення від “знати як робити”).

Разом з поняттям “ноу-хау” отримав розповсюдження термін “**trade secret**”. У вітчизняній літературі він переводиться по-різному (торговий секрет, комерційний секрет, фірмовий секрет, діловий секрет тощо).

Іноді терміни “ноу-хау” і “trade secret” використовуються як синоніми. Такий підхід уявляється неправильним, оскільки ці поняття відрізняються одне від одного за змістом. [106] Так, якщо юридична або фізична особа, маючи в розпорядженні яку-небудь цінну конфіденційну інформацію (тобто “діловий секрет”), зберігає її для себе, для власного користування, то ноу-хау є об’єктом передачі і відповідних операцій.

У ФРН деякі фахівці не вважають ноу-хау якою-небудь формою охорони промислової власності, тому що воно не володіє ознаками винаяткового права (для Г. Штумпфа ноу-хау і виробничий секрет одне і те ж). [100]

Іншої думки дотримуються спеціалісти, які характеризують право на виробничий секрет як право на налагоджене і експлуатоване промислове виробництво, відносячи його таким чином до майнових прав. [107]

Уявляється, що оскільки ці відносини регулюються нормами цивільного і конкурентного законодавства, то все-таки йдеться про цивільне право, більш того — про промислове. У ФРН немає централізованого порядку визнання права на виробничі секрети, тобто немає такого визнання права, яке було б дійсним в абсолютному правовідношенні. Це право може бути захищеним тільки у відносних правовідносинах. [18]

У ряді положень законів разом з виробничими секретами згадуються комерційний і діловий секрети.

- ◎ *Фахівці вважають, що між цими видами факторів, тобто між виробничими, діловими і комерційними секретами, є тільки термінологічна, але не юридична відмінність (R.Krasser).*

Закони Угорщини не містять згадки про ноу-хау в прямій формі. Фахівці, посилаючись на тлумачення законів адміністративною і судовою практикою, вважають, що вказані положення можна напряму віднести до секретних ноу-хау. [108]

Отже, в США створений спеціальний статус власника секрету, що дозволяє дотримувати інтереси не тільки власника об’єкта, й його кредиторів та спадкоємців. [18]

В Японії право на ноу-хау кваліфікується цивільним правом як право на нематеріальне майно. Воно вважається недоторканим і захищається від незаконного збагачення відшкодуванням збитків. [109]

Оскільки відносини з приводу ноу-хау (секретів виробництва) регулюються нормами цивільного і комерційного кодексів, законом про припинення недобросовісної конкуренції, то можна стверджувати, що мається на увазі цивільне право. [18]

В Угорщині право на секретність кваліфікується цивільним кодексом як особисте. Уявляється, що це право є самостійним і може захищатися й тоді, коли воно не носить майнового характеру. Знання і досвід можуть бути захищені і в тому випадку, якщо вони не мають ознаки секретності, але володіють майновою цінністю.

Знання, досвід, технічна і комерційна інформація зазвичай використовуються вільно, оскільки немає обмежень, передбачених законом.

Інтерес для дослідження являють собою ті відносини, які виникають з приводу знань секретного характеру. Йдеться про регулювання законом передачі і використання об'єктів секретності. Правомірність передачі і використання об'єктів секретності є змістом прав на виробничий та інші секрети.

Метою законодавчого регулювання є створення правових засобів запобігання використанню або передачі певних знань, досвіду й інформації без дозволу особи, що володіє ними. Цими правовими засобами є засоби, що присікають порушення, а у разі спричинення збитку — направлені на його відшкодування, а також засоби покарання порушників.[18 ]

У ФРН немає централізованого порядку визнання права на виробничі та інші секрети.

З порівняння положень законів Угорщини виходить, що закон захищає право володаря виробничими і діловими секретами на секретність, право на використання технічної, економічної і ділової інформації у виробничій і діловій діяльності, право на публікацію.

Зазначене властиве законодавству таких країн, як Угорщина, Великобританія, США та ін. [18]

- ◎ *Виробничі, комерційні і ділові секрети можуть бути предметом договорів відчуження і використання. Договори називаються ліцензійними або договорами передачі ноу-хау.*

Предметом передачі можуть бути і несекретні ноу-хау. Це можливо, коли набувач розраховує на швидкий, ефективний спосіб досягнення того

стану, який забезпечується застосуванням несекретного ноу-хау. В таких договорах центр ваги переміщується з ноу-хау як такого на додаткову діяльність, за допомогою якої забезпечується більш ефективно його використання.

Відносини, пов'язані з секретністю, як правило, регулюються картельним і цивільним законодавством.

Об'єктом передачі може бути секрет, подальша передача або розголошення якого небажані. У такому разі в договір включається зобов'язання про конфіденційність. Порухення цього зобов'язання карається за допомогою позову про припинення. Іноді зобов'язання про конфіденційність продовжуються після закінчення дії договору, що зазначається в договорі. Порухення післядоговірних зобов'язань регулюється трудовим або картельним законодавством.

У разі спричинення шкоди в результаті порушення зобов'язань про конфіденційність вона відшкодовується за правилами цивільного права. [18]

- ⊙ *Законодавство промислово розвинутих країн передбачає відповідні заходи захисту як цивільного, так і кримінально-правового характеру проти незаконного розкриття, привласнення і використання ноу-хау, торгових та ділових секретів.*

Дія заходів відповідальності розповсюджується на сферу відносин, що регулюються і охороняються цивільним, кримінальним та іншим законодавством, і своїм змістом направлена на запобігання порушенням, виявленим (встановленим) під час відправлення прав у даній області. [18]

## США

Згідно з §1(1) Уніфікованого закону про ділові секрети (Uniform Trade Secrets Act, надалі — Закон) як неправомірний засіб розглядаються крадіжка, хабарництво, введення в оману, порушення або схилення до порушення конфіденційності, шпигунство з використанням електронних або інших засобів. Даний перелік зовсім не вичерпує всі можливі варіанти. Прецедентна практика достатньо широко тлумачить поняття “неправомірні засоби”. Придбання ділового секрету може бути визнано неправомірним, хоча при цьому не порушується кримінальне або цивільне законодавство, тобто не скоюються незаконні дії.



**Прикладом** може бути судова суперечка “Дюпон де Немур энд К”” проти “Крістофер К”. [111] Під час будівництва позивачем хімічного заводу в Техасі третя сторона (не розкрита в ході розгляду) найняла відповідача для здійснення аерофотознімання даного об’єкта. Дослідивши такі знімки, кваліфікований фахівець міг отримати інформацію про розроблений позивачем і такий, що знаходився в секреті, процес виробництва метилового спирту, оскільки заводське устаткування не було підведене під дах. Суд ухвалив, що позивач має право на охорону інформації, що розглядалася як діловий секрет. Суд визнав також аерофотознімання заводу неправомірним засобом отримання інформації і характеризував її як незаконне привласнення інформації. При вирішенні питання про те, чи були прийняті позивачем необхідні заходи для збереження секретності, суд взяв до уваги важкість запобігання такого роду спостереженню і невинувато великі витрати на спорудження даху над незавершеним об’єктом. Таким чином, закону, на перший погляд, поведінку відповідача суд розцінив як неправомірний засіб. Варто відзначити, що суд може використовувати будь-які обставини, що відносяться до справи, для встановлення ступеня розумності заходів щодо забезпечення секретності інформації, які зроблені або могли бути зроблені власником. [18]

Як правомірні дії щодо отримання інформації в Законі згадується виявлення її в результаті незалежного дослідження, спостереження за об’єктом у відкритому застосуванні, вивчення опублікованих даних тощо. [18]

Згідно з § 1(2) Закону правопорушення визначається, виходячи з незаконного привласнення, яке може проявлятися двояко:

- або в придбанні ділового секрету неправомірними засобами;
- або в розкритті чи використанні його без висловленої згоди або такої, що мається на увазі.

Таким чином, незаконним визнається привласнення ділового секрету з використанням неправомірних засобів або використання ділового секрету із знанням того, що він отриманий іншими особами неправомірними шляхами. Незаконне привласнення має місце також у разі порушення конфіденційності. Відповідальність настає і тоді, коли відповідач порушує зобов’язання конфіденційності сам або використовує секрет, знаючи, що він отриманий в результаті такого порушення. [18]

Згідно з § 1(2) Закону незаконне привласнення має місце тоді, коли відповідач, що отримав діловий секрет від третьої особи, знає або має достатньо підстав знати, що даний секрет незаконно привласнений третьою особою.

Що стосується випадкового використання інформації, яке може призвести до незаконного привласнення, то згідно з § 1(2) (ii) (c) Закону воно не повинне бути наслідком недостатньої ефективності заходів щодо охорони секрету.

Не несе відповідальності також особа, що отримала діловий секрет ненавмисно без попередження. Проте, відповідно до Закону, використання ділового секрету такою особою визнається незаконним після того, як вона дізналась, що передана інформація носить конфіденційний характер. Останнє справедливо в тому випадку, якщо одержувач не знає про це у момент передачі інформації, за умови, що його матеріальне положення не змінилося за час користування секретом. Закон передбачає захист ділового секрету від незаконного привласнення в результаті випадкового розкриття. [18]

У § 3(a) Закону у разі неправомірного привласнення ділового секрету передбачаються такі засоби захисту, як заборона подальшого використання і відшкодування збитків.

Так, службовцю, посвяченому в ділові секрети фірми, при звільненні може бути заборонено їх використання або розкриття. Від нього можуть також зажадати повернення креслень або інших документів, що містять інформацію про діловий секрет. Такі ж санкції можуть бути застосовані до особи, яка отримала секретну інформацію в конфіденційній бесіді, але за умови, що вона спробує використати або розкрити її. Як правило, заборона незаконного привласнення секрету не спричиняє значних витрат часу і засобів, пов'язаних з судовим розглядом. [18]

Якщо відшкодування збитків визнається недостатнім засобом захисту права, особа, що незаконно привласнила діловий секрет, позбавляється придбаних переваг щонайменше на термін, який необхідний іншим конкурентам для самостійної підготовки аналогічної інформації, або який достатній для того, щоб відповідач міг розкрити діловий секрет законними засобами шляхом незалежної розробки або інженерного аналізу виробу позивача. При цьому особа, що незаконно його привласнила, опиняється в рівному становищі з іншими конкурентами.

У разі, коли заборона використання ділового секрету вважається нерозумною (1 — наявність публічного інтересу до продовження використання ділового секрету особою — інформації, що має значення для військових і інших галузей, пов'язаних з державною безпекою [110]; 2 — упевненість особи, що придбаває інформацію сумлінно, але з нанесенням збитку, в тому, що вона може використовувати діловий секрет до тих пір, поки їй не повідомили, що діловий секрет придбаний неправомірно), передбачається виплата позивачу відповідного гонорару.

Важливим засобом правового захисту ділових секретів є також відшкодування збитків, що не перевищують розмір шкоди, а також стягнення штрафних санкцій, розмір яких не перевищує подвійного розміру відшкодування, якщо має місце умисне і зловмисне привласнення.

У разі виникнення труднощів при встановленні особи, що має право на грошову компенсацію, коментар до Закону містить пояснення: “якщо право на захист ділового секрету відносно однієї і тієї ж інформації мають більше однієї особи, то тільки та особа, у якої відбулося незаконне привласнення ділового секрету, має право на судовий захист”. [111]

- ➔ Таким чином, якщо декілька конкурентів користуються діловим секретом, який був незаконно переданий третій особі одним з них, то всі вони можуть понести фактичний збиток. Проте право на відшкодування має лише той з них, чий діловий секрет був незаконно привласнений. [18]

Згідно з поправками, внесеними в Закон у 1985 р., “у виключних обставинах” як відшкодування збитків може застосовуватись примусовий продаж ліцензій незаконним користувачам ділових секретів. Параграф 3(а) доповнений положенням про встановлення норм відрахування від прибутку як відшкодування збитків власника ділових секретів. Підкреслюється, що збитки власників секретів від їх незаконного використання включають як втрачену вигоду позивача, так і безпідставне збагачення відповідача. [112]

Згідно § 6 позов про незаконне привласнення повинен бути пред’явлений протягом 3-х років після встановлення факту незаконного привласнення або з моменту, коли потерпіла особа знайде або отримає достатню можливість для виявлення факту незаконного привласнення.

З ухваленням у 1979 р. в деяких штатах США Уніфікованого закону про ділові секрети і на основі рішень, винесених судами, ділові секрети офіційно визнані видом власності. Новий статус власника ділових секретів створює і новий інструмент для захисту інтересів не лише самого власника нематеріального об’єкта, а й його кредиторів і спадкоємців. [113]

Ділові секрети в США охороняються Законом про економічне шпигунство (EA) від 1996 р. і Уніфікованим законом про ділові секрети (UTSA). За порушення першого закону може наступити кримінальна відповідальність, за порушення другого — цивільна, причому одне не виключає іншого.

Особливий інтерес до цієї проблеми пояснюється підвищеною роллю технологій в американській економіці і випадками використання комп'ютерів та Інтернету для проникнення в конфіденційні бази даних, що останнім часом почастишали. [18]

Випадки фактичного або передбачуваного протиправного використання ділових секретів регулюються UTSA, а ЕА охоплює також випадки умисного незаконного привласнення ділових секретів, у тому числі конспіративними способами. На порушників ЕА може накладатись штраф до 500 тис. дол. і застосовуватись ув'язнення строком до 10 років (корпорація або інша організація може бути оштрафована на 5 млн. дол.).

Якщо ж злочин умисно скоюється на користь іноземної держави, то максимальний термін ув'язнення може скласти 15 років, а штраф — 10 млн. дол. У червні 1997 р. за спробу продати дискети, креслення та інші матеріали з конфіденційною інформацією компанії, яка сама сповістила зацікавлену сторону про підготовлювану протиправну дію, до 15 місяців ув'язнення був засуджений колишній співробітник компанії "PPG Industries".

Оскільки порушники ЕА можуть понести кримінальне покарання, законом передбачаються і більш суворі умови представлення доказів, тобто вони повинні бути неспростовними. Крім того, для порушення кримінальної справи необхідне підтвердження умисності протиправних дій, тому в більшості випадків порушуються цивільні справи.

Наприклад, у справі "PepsiCo v Redmond" найскладнішим виявилось встановлення наявності ділового секрету як такого. При цьому суд брав до уваги ступінь обізнаності про секрет за межами компанії-позивача, ступінь посвячення співробітників компанії "PepsiCo" та інших залучених в її діяльність осіб, строгість вживаних заходів інформаційної безпеки, цінність конфіденційної інформації як для позивача, так і для конкурентів, обсяги витрат і, нарешті, чи могли інші особи отримати або відтворити цю інформацію.

Хоча для ділових секретів вимога новизни не є обов'язковою умовою, вони повинні бути недоступною для громадськості інформацією або комбінацією елементів інформації, кожний з яких окремо не складає секрету. При цьому власник інформації зобов'язаний вжити розумних заходів дотримання конфіденційності.

Після розгляду справи "PepsiCo v Redmond" поняття загрози незаконного привласнення ділового секрету включило доктрину так названого "неминучого розкриття". Через шість днів після того, як посвячений в деталі розвитку виробництва віце-президент Північноамериканського

відділення “PepsiCo” звільнився з неї і мав намір перейти на роботу в конкуруючу компанію “Quaker”, “PepsiCo” подала позов до суду, вимагаючи заборони на такий перехід, оскільки це було пов’язано в ризиком “неминучого розкриття” надзвичайно важливих питань цінової і маркетингової політики. Суд першої інстанції задовольнив позов “PepsiCo” і зобов’язав відповідача не приступати до роботи в компанії “Quaker” протягом шести місяців. Апеляційний суд підтримав рішення суду першої інстанції. [18]

## ЯПОНІЯ

Питання захисту службових ділових секретів наймача від незаконного привласнення їх службовцями після закінчення терміну служби регулюються і в Японії. Наймач може за допомогою договору зобов’язати свого службовця не розкривати інформацію, яку він придбав протягом терміну служби. Типова угода про службові винаходи, підготовлена патентним відомством, містить такий пункт: “Винахідники і службовці відділу по винаходах службовців повинні зберігати таємницю змісту винаходів і інших матеріалів, що відносяться до інтересу компанії, на необхідний період часу”. [18]

➔ Наймач може обмежити поведінку службовців після закінчення служби на певний період.

У зв’язку з тим, що таке доповнення може певною мірою порушити гарантію свободи вибору якогось виду занять (професії) відповідно до ст. 22 Конституції, службовцям, які в період дії такого обмеження не можуть знайти посаду (роботу), із оплатою, яка б їх задовольняла, передбачається виплата відповідної компенсації. [18]

Належна увага надається також захисту ділових секретів у процесі конфіденційних відносин. Відповідні норми законів накладають на певних осіб, згідно з займаним ними положенням або професією, обов’язок щодо збереження конфіденційності. Так, у Цивільному кодексі передбачається обов’язок уважно відноситися до справ, у Комерційному кодексі передбачається обов’язок лояльності директора корпорацій, що також включає обов’язок збереження конфіденційності, а також визначаються обов’язки директора корпорації не конкурувати зі своїми корпораціями.

Кримінальний кодекс передбачає покарання для осіб окремих професій, які розкривають секрети клієнтів або споживачів: особа, яка є або

було лікарем, фармацевтом, аптекарем, акушеркою, юристом, адвокатом або нотаріусом і яка без відповідної підстави розкрила секрет, що став їй відомий завдяки професійній діяльності, підлягає покаранню у вигляді ув'язнення строком до шести місяців або штрафу до 20000 тис. єн.

Згідно з Законом про адвокатуру (Закон № 205, 1949) передбачається наступне: адвокат або особа, яка раніше була адвокатом, має право і обов'язок зберігати в секреті будь-які факти, які стали йому (їй) відомі при здійсненні своєї діяльності, за умови, що це не буде предметом яких-небудь протилежних правових розпоряджень.

- ⊙ *Згідно з Цивільно-процесуальним кодексом, свідок звільняється від надання свідчень за матеріалами, що зачіпають ділові секрети.*

Кримінальний кодекс не містить яких-небудь положень, що передбачають покарання за незаконне розкриття або незаконне використання ділових секретів або промислове шпигунство. Проте положення Кримінального кодексу (ст.ст. 222, 233, 235, 246, 247), що стосуються погроз (шантажу), перешкоджання чий-небудь діяльності, крадіжки, обману, порушення довір'я, можуть бути застосовані і до вищеназваних правопорушень. [18]



Так, у справі "Japan v Німці" відповідач, член технологічного відділу провідної хімічної компанії в Осаке, залишив свою службу, взявши з собою матеріал, призначений для використання у виробництві вінілхлориду, а також теку документів, що містять повідомлення про нові способи виробництва вінілхлориду. Всі матеріали компанія зберігала в таємниці. Суд визнав цінність таких матеріалів і застосував ст. 235 Кримінального кодексу.

У 1990 р. і 1993 р. в Закон Японії про припинення недобросовісної конкуренції були внесені поправки, що враховують пропозиції на переговорах в рамках ГАТТ і міжнародну гармонізацію в цій галузі. Зокрема, були введені нові статті, що стосуються незаконного заволодіння комерційною таємницею, її використання або розголошення. Крім того, вони регулюють випадки, коли особа знає про незаконне отримання комерційної таємниці, але продовжує використовувати її. Як комерційна таємниця охороняється інформація технічного або комерційного характеру, що має економічне значення, невідома громадськості і яка зберігається в таємниці. Винний в здійсненні акту несумлінної конкуренції засуджується до тюремного ув'язнення на термін, що не перевищує трьох

років, або до виплати штрафу не більше 3 млн. єн. Якщо закон порушила фірма, то штраф значно більший — 100 млн. єн, а її співробітник, винний в навмисному здійсненні неправомірних дій, засуджується до тюремного ув'язнення. [18]

## ВЕЛИКОБРИТАНІЯ

Нині охорона ноу-хау і торгових секретів в рамках кримінального права не регулюється. В основному вона будується на базі прецедентного права. Це відноситься навіть до таких протиправних діянь, як крадіжка секретних документів, матеріалів і т. ін., не дивлячись на те, що теоретично ці діяння можуть підпадати під дію Закону про крадіжки 1968 р. Таке положення в корені відрізняється від законодавства країн континентального права (Франції, Італії та ін.), де кримінальними кодексами передбачені спеціальні статті, що містять санкції за неправомірне розкриття і використання промислових секретів. [18]

Згідно з англійським правом відносно ноу-хау і торгових секретів можливе застосування норм, під які підпадає таке злочинне діяння, як злочинна змова. Під ним мається на увазі угода двох або більше осіб про здійснення протиправного діяння або здійснення правомірного діяння злочинними засобами. Підбурювання до таких дій також вважається злочином.

➔ Цивільно-правова відповідальність в галузі ноу-хау і торгових секретів багато в чому має невизначений характер і ґрунтується на прецедентному праві.

Коментатори вказують, що поняття недобросовісної конкуренції, яке добре відоме в європейському континентальному праві, не знайшло свого відображення в англійському праві. Це відноситься і до неправомірних дій відносно ноу-хау, торгових секретів та конфіденційної інформації. Суди практично не розглядали справи, пов'язані з недобросовісною конкуренцією, в яких зачіпалися питання правової охорони даних об'єктів.

За відсутності ясних і докладних нормативних положень, що регулюють правовідносини, пов'язані з ноу-хау, англійські суди при розгляді справ ґрунтуються на теорії квазі-договору (договір на основі конклюдентних дій) або порушенні конфіденційності. Проте багато, якщо не більшість, дій, що підпадають за європейським законодавством під недо-

бросовісну конкуренцію (ведення справ під чужим ім'ям, знищення чужої продукції, зловживання або введення в оману контрагента відносно ноу-хау і торговий секрет), є неправомірними і у Великобританії і кваліфікуються як порушення конфіденційності або договірних зобов'язань. [18]

- ⊙ *Для того, щоб дія підпала під порушення конфіденційності, позивач повинен довести суду, що:*
  - 1) *інформація є торговим секретом (ноу-хау, конфіденційною інформацією);*
  - 2) *існують зобов'язальні відносини, пов'язані з конфіденційністю, між позивачем і відповідачем;*
  - 3) *в наявності дійсне порушення зобов'язань про конфіденційність, яке виражене в неправомірному розкритті, використанні або привласненні інформації [18].*

В англійському праві використовуються три принципи, які застосовуються до будь-якого порушення конфіденційності:

- 1) якщо інформація передається на умовах конфіденційності, то особа, що одержала її, не має права використовувати або розкривати цю інформацію з метою створення конкуренції власнику інформації;
- 2) якщо доведено, що відповідач умисно або ненавмисно розкрив конфіденційну інформацію без згоди власника, він визнається винним в порушенні прав власника інформації;
- 3) особа, що отримала конфіденційну інформацію, не має права використовувати її раніше, ніж власник інформації, для заняття найбільш вигідних позицій, навіть якщо зміст цієї інформації був опублікований або може бути встановлений третіми особами шляхом власних досліджень. Передбачається, що власник конфіденційної інформації повинен мати певну перевагу перед всією рештою осіб і бути упевненим, що не запізниться на старті в умовах жорсткої конкуренції [18].

Ці принципи носять узагальнений характер і можуть змінюватися і доповнюватися залежно від конкретних справ.

**При порушенні конфіденційності до порушника застосовуються такі заходи:**

- 1) винесення ухвали суду, яка може мати "проміжну" (служе лише для запобігання подальшому спричиненню шкоди до прийняття остаточного рішення по справі) або "постійну" дію;

- 2) взяття відповідачем зобов'язання під присягою передати позивачу або знищити фізичні об'єкти, в які втілені ноу-хау або торговий секрет (позивач може на свій розсуд вибрати ту або іншу міру);
- 3) компенсація за збитки або упущену вигоду, які стали результатом порушення зобов'язань про конфіденційність.

*Третя міра* полягає у відшкодуванні збитків, викликаних порушенням конфіденційності.

В англійському прецедентному праві відомі такі категорії збитків:

- прості, або загальні, які можуть бути легко встановлені з достатньою точністю;
- спеціальні, які також можуть бути встановлені з достатньою точністю, але на них повинно бути спеціально звернуто увагу суду, оскільки вони не такі очевидні;
- обтяжливі, які можуть розглядатися як компенсація за не гідні методи, за допомогою яких відбулося порушення конфіденційності;
- “зражкові”, відшкодування яких повинне слугувати ніби наочним прикладом і застереженням для відповідача від подібних порушень у майбутньому;
- умовні, коли передбачається виплата позивачу визначеної суми за порушення його прав та інтересів, навіть якщо позивач взагалі не претендує на яку-небудь компенсацію збитків.[18]

## **ФРН**

У положеннях Закону про заборону недобросовісної конкуренції (UWG) ФРН сформульовані склади злочинів і міри відповідальності у разі порушення прав:

- визначається покарання службовцю, робочому або учню підприємства за неправомірне розголошення секрету фірми, підприємства, довіреного йому, або що став доступним через службові відносини. Покарання визначається, якщо дію вчинено з корисливою ціллю, в цілях конкуренції, з наміром завдати збитку; воно застосовується, якщо дію вчинено протягом терміну дії службових відносин;
- визначається покарання особі, яка використовує або повідомить іншій особі неправомірно секрет фірми або підприємства, здобутий з повідомлень, довірених йому або що стали доступними через службові відносини, або в результаті протизаконної дії або дії, що порушує загальноприйняті норми поведінки;

- визначається покарання за неправомірне використання або повідомлення кому-небудь в цілях конкуренції або з корисливою ціллю конфіденційної інформації, довіреної йому через ділові відносини;
- визначається обов'язок порушника по відшкодуванню збитку, якщо такий заподіяний діями, вказаними вище.

Відповідно до принципів Німецького цивільного укладення (BGB) права власника секрету можуть захищатися позовом про припинення також позовом про відшкодування збитку.

Нарешті, до порушника можуть бути застосовані положення кримінального кодексу, якщо він є носієм певних службових функцій.

Додатково до кримінального покарання застосовуються позови про припинення і про відшкодування шкоди на підставі § 823 (абз. 2) BGB.

З трудової угоди витікає, що найнятий фахівець, який працює під час дії трудових правовідносин, зобов'язаний дотримуватися секретності. Якщо він неправомірно і умисно передає довірений або доступний йому виробничий або діловий секрет службовцю аналогічного підприємства або сторонній особі, його дії порушують договір.

Обов'язок по відшкодуванню збитку настає як тоді, коли порушник діє умисно, так і у разі недбалої дії.

Роботодавець має право відмовитись від послуг службовця, який порушив обов'язок збереження секретності і не виправдав довіри роботодавця.

Варіантом охорони секрету після закінчення трудового договору може бути підписання угоди, яка спеціально визначає обов'язок колишнього службовця щодо збереження секретності. Заборона передачі або використання рівнозначне забороні несумлінної конкуренції.[18]

Якщо з'ясується, що обов'язок збереження таємниці може створити конфліктну ситуацію на новому місці роботи колишнього службовця, то може бути укладена додаткова домовленість з дією на термін не більше двох років (письмово) з одночасною виплатою винагороди службовцю за збереження цієї інформації.[18]

У відносинах, пов'язаних із створенням службових винаходів, застосовуються особливі правила.

Якщо секрет є службовим винаходом в значенні Закону про службове винахідництво, то винахідник-службовець зобов'язаний зберігати секрет, поки винахід не стане використовуватись вільно.

Особа, що отримала знання незалежно від власника секрету, використовує їх вільно в своїх інтересах, а той, хто придбав знання правомірно

у власника секрету, мимоволі вступає з ним у зобов'язальні відносини, які, як правило, оформляються договором.

Дії службовця щодо передачі і використання неправомірно отриманих знань кваліфікуються як порушення позадоговірних зобов'язань.

## ШВЕЙЦАРІЯ

У Швейцарії склалася чітка і достатньо ефективно працююча система нормативних актів, що становить основу правового режиму добросовісної конкуренції. Така дієвість пояснюється наступними причинами [18]:

- по-перше, множинністю актів, які регулюють різноманітні аспекти конкуренції (що привело до безперечної повноти законодавчого регулювання);
- по-друге, угрупованням нормативних актів і окремих норм доповнювального або загального характеру навкруги певного “ядра” — спеціального комплексного (що містить норми як цивільного, так і кримінального права) нормативного акту, що грає роль основного регулятора відносин недобросовісної конкуренції і забезпечує охорону конкуренцію в ході її здійснення.

Як таке “ядро” виступає федеральний Закон “Про недобросовісну конкуренцію” від 19 грудня 1986 р. (далі — Закон 1986 р.), що змінив чинний раніше однойменний Закон від 30 вересня 1943 р. і значно розширив сферу правового регулювання відносин конкуренції в їх динаміці.

У ст. 2 Закону 1986 р. міститься визначення недобросовісної конкуренції. В ньому законодавцем поставлений знак рівності між недобросовісною і незаконною конкуренцією: “Вважаються недобросовісними і незаконними всяка поведінка або комерційна практика, що вводять в оману або яким-небудь іншим чином суперечать звичаям доброї торгової практики і мають місце у відносинах між конкуруючими суб'єктами або у відносинах суб'єктів комерційної діяльності з клієнтурою”.

Разом із загальним визначенням недобросовісної конкуренції Закон 1986 р. містить докладний незамкнутий перелік недобросовісних конкурентних дій.

У швейцарському праві передбачені цивільно-правові і кримінально-правові санкції за порушення правил добросовісної конкуренції. При цьому наявність збитку для конкурента (клієнтури) далеко не завжди є умовою настання відповідальності: незаконними можуть вважатися також дії, що не призвели до виникнення збитку, але загрожують його спри-

чинити. Що стосується вини порушника, то вона розглядається судовою практикою як умова відповідальності постільки, оскільки початковим критерієм для її накладання виступає добра торгова практика або добра воля, тобто об'єктивний критерій. Таким чином, як умова настання відповідальності за порушення правил добросовісної конкуренції виступає протиправність і винність дій порушника. Це означає (якщо врахувати легальне визначення недобросовісних конкурентних дій) суперечність їх закону і звичаям доброї торгової практики.[18]

Захист порушених (або таких, що знаходяться під загрозою порушення) інтересів конкурента (клієнтури) відбувається в позовному порядку. Позовна заява може бути подана як самим конкурентом або клієнтом, так і іншими особами, зокрема: економічними і професійними асоціаціями, іншими організаціями федерального або кантонального масштабу, що здійснюють захист прав споживача (за умови, що подібні дії входять в їх компетенцію згідно з статутом).

Особа, інтереси якої порушені (або відносно інтересів якого існує загроза порушення), а також інші перераховані особи мають право вимагати за судом заборони здійснення недобросовісних конкурентних дій (або, відповідно, їх припинення), констатації незаконності таких дій, спростування або іншого доведення рішення до зведення невизначеного (або обмеженого) кола осіб. Крім того, така особа має право пред'являти до порушника позов про позадоговірне спричинення шкоди і вимагати відшкодування заподіяного матеріального, економічного і (або) морального збитку. Крім передбачених таким чином цивільно-правових санкцій, закон встановлює санкції кримінального характеру: ув'язнення або штраф розміром до 100 тис. швейцарських франків. [18]

## УГОРЩИНА

Положення Закону "Про заборону недобросовісної ринкової поведінки" 1990 р. (далі — Закон 1990 р.) застосовуються до господарської діяльності, здійснюваної підприємцями на території Угорської Республіки.

Накладається заборона на порушення комерційної таємниці, її незаконне розголошення або використання. Згідно з Законом, **комерційною таємницею вважається будь-яке пов'язане з господарською діяльністю рішення, фактична інформація або відомості, збереження секретності яких забезпечують правомочній особі можливість охорони його майнових інтересів.**

**Комерційна таємниця вважається отриманою недобросовісно** у випадках, коли комерційна інформація придбана:

- без згоди особи, що має право на комерційну таємницю;
- за посередництвом особи, що знаходиться з власником комерційної таємниці в довірчих відносинах або має з ним комерційні зв'язки. [18]

Законом “Про заборону недобросовісної ринкової поведінки” 1990 р. передбачені цивільно-правові і адміністративні санкції за недобросовісну конкурентну діяльність. В судовому порядку можуть бути розглянуті позови щодо відшкодування заподіяного збитку, щодо винесення судової заборони на здійснення подібних дій, а також щодо задоволення у формі заяви тощо.

В рамках адміністративного провадження розглядаються заяви щодо порушення споживачем зобов'язання про дотримання свободи здійснення конкуренції. Розгляд заяв проводиться Управлінням з економічної конкуренції, яке має право також порушувати провадження у разі порушення угоди, що обмежує економічну конкуренцію або забороняє зловживання економічною перевагою. [18]

Управління має право порушувати провадження як на підставі заяви зацікавленої особи, так і за власною ініціативою. Процедура винесення рішення складається з двох стадій: розгляди заяв і винесення рішення. В обґрунтованих випадках на засіданні, де ухвалюється рішення, може заслуховуватись думка компетентного органу. Винесене рішення публікується в офіційному виданні Управління.

## ЧЕХІЯ І СЛОВАЧЧИНА

У Чехії і Словаччині недобросовісній конкуренції присвячений спеціальний розділ Торгового кодексу 1991 р. (§ 44–55). Під **недобросовісною** розуміється *конкуренція, яка суперечить добрим звичаям, прийнятним в діловому обороті, яка може заподіяти шкоду конкурентам або споживачам.*

В Торговому кодексі даний вичерпний перелік конкурентних дій, що визнаються недобросовісними.

У визначенні **ділового секрету**, що міститься в положеннях §§ 17–20 Торгового кодексу, йдеться про охорону секретів комерційного (наприклад, що стосуються умов торгівлі, клієнтури, підприємців), виробничого і технічного характеру (наприклад, інструкцій щодо використанню

ноу-хау, креслень, програм для ЕОМ, винаходів і промислових зразків підприємства). Ці секрети безпосередньо пов'язані з підприємством, мають дійсну або потенційну цінність матеріального або нематеріального характеру і не повинні бути доступними для відповідних комерційних кіл, особливо конкурентів. Перелік секретів, що охороняються, визначається самим підприємцем, виходячи з інтересів справи. [18]

Власник ділового секрету має виняткове право на нього, тобто може не тільки використовувати його в своїй діяльності, а й давати іншим особам дозвіл на його використання. Оскільки в Торговому кодексі не визначена форма такого дозволу, то можна припустити, що власник ділового секрету передає право на його використання письмовим договором. [18]

Відповідно до Торгового кодексу фактичними порушеннями вважаються випадки, коли особа, що знаходиться у виробничих або інших відносинах з підприємцем, незаконно повідомить, передасть іншій особі діловий секрет підприємця, про предмет якого його було повідомлено або він довідався, маючи доступ до креслень, моделей, макетів тощо, і який може бути використаний конкурентами. Особа, що розкриває діловий секрет, може дізнатися про його предмет також при виконанні інших функцій, наприклад, будучи притягнутим судом або іншим органом до участі в розгляді власної або чужої справи. Факт передачі ділового секрету визнається недобросовісною дією незалежно від часу здійснення і не обмежується періодом знаходження даної особи у виробничо-правових або правових відносинах з підприємцем, в процесі яких йому став відомий предмет ділового секрету. Підприємець має право зажадати від нього припинення протиправної дії і відшкодування збитку, наприклад у вигляді виплати грошової компенсації або незаконного доходу.

- ⊙ *При публічному розгляді справи в суді, в ході якого виникає вірогідність розкриття ділового секрету, може бути ухвалене рішення про закриття слухання. [18]*

## **БОЛГАРІЯ**

Болгарське законодавство щодо боротьби з недобросовісною конкуренцією знаходиться на початковому етапі розвитку. Першим нормативним актом у цій галузі став Закон “Про захист конкуренції”, прийнятий Великим народним зібранням 2 травня 1991 р. [18]

Стаття 12 Закону дає таке визначення недобросовісної конкуренції: “Недобросовісною конкуренцією є всяка дія або поведінка при здійсненні господарської діяльності, яка суперечить добросовісній торгівій практиці і заподіює або може заподіяти збиток інтересам конкурентів у відносинах між ними або в їх відносинах із споживачами”.

Закон “Про захист конкуренції” 1991 р. дає зразковий перелік дій, в яких виражається недобросовісна конкуренція.

Спеціальний підрозділ Закону містить правила, що забороняють недобросовісне використання в конкурентній боротьбі співробітників організації-конкурента. Заборонено одночасно брати участь у складі органів управління і контролю конкуруючих підприємств. Ця заборона зберігається протягом трьох років після виходу зі складу цих органів. Без згоди працедавця працівник не має права займатися господарською діяльністю, конкурентною по відношенню до працедавця, протягом трьох років після припинення трудових відносин, якщо договором не було встановлено інше. [18]

Здійснення дій, що кваліфікуються як недобросовісна конкуренція за болгарським Законом “Про захист конкуренції”, спричиняє за собою відповідальність, передбачену цим Законом. При порушенні правил щодо боротьби з недобросовісною конкуренцією в окружний суд можуть звернутися особи, чії інтереси порушені, а також Комісії по захисту конкуренції і окружний прокурор.

Суд у зв’язку зі зверненням може [18]:

- припинити господарську діяльність до припинення порушення;
- визнати недійсними операції або рішення, що порушують закон;
- зобов’язати порушника припинити порушення. Якщо порушником отриманий прибуток, суд може вилучити його в дохід держави.

Передбачені також майнові санкції, що накладаються судом на порушника в порядку, встановленому Законом про адміністративні порушення і покарання. Майнові санкції застосовуються відносно фірм і підприємств, а також фізичних осіб.

## ПОЛЬЩА

У Законі про боротьбу з недобросовісною конкуренцією 1993 р. передбачена охорона виробничих секретів підприємства. Відповідно до Закону під **виробничим секретом** розуміється необнародована технічна,

технологічна, комерційна або організаційна інформація підприємства, відносно якої підприємець вжив заходів щодо охорони конфіденційності.

При цьому недобросовісною конкуренцією є передача, обнародування або використання інформації, що є виробничим секретом, або її отримання від не уповноваженої особи, якщо це загрожує істотним інтересам підприємства. Дана норма застосовується також до особи, що виконувала роботу на основі трудових або інших правовідносин, протягом трьох років з моменту її звільнення, якщо договір не передбачає іншого, або виробничий секрет відмінений. [18]

Разом з тим дана норма не застосовується до тих осіб, які отримали таку інформацію сумлінно, на відшкодувальній основі. Проте і в цьому випадку суд може зобов'язати одержувача інформації виплатити відповідну винагороду за її використання.

За здійснення недобросовісних конкурентних дій польський Закон передбачає адміністративну, цивільно-правову і кримінальну відповідальність.

Умови настання адміністративної відповідальності в Законі не розкриті. В ст. 27 згадується лише про можливість адміністративного переслідування провини у сфері недобросовісної конкуренції. [18]

Цивільно-правові санкції викладені в ст. 18 Закону, згідно з якою підприємець, чий інтереси порушені або знаходяться під загрозою, має право вимагати:

- припинення протиправних дій;
- усунення наслідків протиправних дій;
- виклад заяв відповідного змісту і у відповідній формі;
- компенсації заподіяної шкоди на загальних підставах;
- повернення необґрунтовано отриманого прибутку на загальних підставах.

Термін позовної давності у справах про недобросовісну конкуренцію складає три роки і обчислюється окремо для кожного правопорушення.

У справах про припинення недобросовісної конкуренції підприємець, чий інтереси порушені або знаходяться під загрозою порушення, може клопотати в суді про видачу тимчасового розпорядження, наприклад, про заборону збуту певних товарів.

Кримінальна відповідальність передбачена не для всіх складів правопорушень у сфері недобросовісної конкуренції.

Розголошення або використання для власних господарських цілей інформації, що є виробничим секретом підприємства, якщо це заподіює істотну шкоду підприємцю, тягне для винної особи позбавлення волі на

строк до двох років, обмеження свободи або штраф. Такому ж покаранню підлягає особа, яка після отримання чужої секретної інформації розголошує її або використовує з власною метою. [18]

## АЗІЯ

Багато аспектів азіатських законів щодо охорони комерційних секретів співставні із законодавством США. Схожість підходів до цієї проблеми в Гонконгу, Малайзії і Сінгапурі пояснюється британським походженням чинного там законодавства. Проте загальним їх елементом є відсутність вимоги новизни інформації, що охороняється, бо її власник не зобов'язаний бути першим володарем секрету. У всіх країнах міститься умова відносної, а не абсолютної секретності. Майже скрізь охороняється технічна інформація, включаючи робочі креслення, технологічні процеси і формули. Але відношення до підприємницької інформації неоднакове. На відміну від патентних законів не встановлюються тимчасові обмеження для комерційних секретів, їх існування припиняється тільки після розкриття громадськості. Ще одна особливість: дані об'єкти не перешкоджають іншим особам мати в своєму розпорядженні аналогічну інформацію. Так, не забороняється розбирання пристроїв з метою їх вивчення і відтворення. [18]

Також необхідно враховувати відмінності в тлумаченні поняття “комерційні секрети”. Так у Китаї, Японії, Південній Кореї і на Тайвані до останніх відносяться поштові відправлення, відомості про цінові знижки і методи ведення бізнесу. В Південній Кореї також охороняють “управлінську інформацію”, в Китаї — “оперативну”, а на Тайвані — “торгову”. В Малайзії, Сінгапурі і Гонконгу такі види інформації не підпадають під дію спеціальних законів, і потрібно керуватися законом про конфіденційність.

У Малайзії, Сінгапурі і Гонконгу відповідальність за використання секрету не знімається і з третіх осіб, якщо вони знали або повинні були знати, що подальше застосування технології порушує права його власника. В інших країнах відповідальність третіх осіб може розрізнятись: в Японії, на Тайвані і в Південній Кореї вимоги більш жорсткі, в Китаї дещо пом'якшені. [18]

Процедура відшкодування збитку за розкриття секрету включає ряд умов: судове підтвердження фактичних збитків, визначення суми, що підлягає відшкодуванню, покриття витрат на послуги адвокатів тощо. Час-

тіше за все виходять з ринкової вартості відомостей. Проте на Тайвані допускається покарання винного за допомогою стягнення триразового розміру збитку. В Малайзії, Сингапурі, Гонконгу і Японії порушник оплачує витрати потерпілого на роботу адвокатів.

Новий Закон КНР про недобросовісну конкуренцію (ст. 25) передбачає накладення штрафу. В Південній Кореї накладається ув'язнення строком до трьох років і штраф, на Тайвані — ув'язнення до одного року або штраф. У Сингапурі, Гонконгу і Малайзії дані порушення кримінальному переслідуванню не підлягають. [18]

По-різному трактують і питання ліцензування технологій. В Південній Кореї та низці інших країн ліцензування деяких комерційних секретів повинне проводитися з схвалення компетентних державних органів. У Китаї подібному узгодженню підлягають ліцензії з терміном дії понад 10 років.

Враховуючи висловлене, при укладанні ліцензійних угод з представниками країн Азії рекомендується уважно вивчати особливості національних законодавств і культурних традицій, детально обговорювати види і обсяг ліцензованої технологічної а також іншої інформації [114].

## РОСІЯ

Інститут комерційної таємниці добре розвинутий і захищений в сучасному російському законодавстві. Законодавство Російської Федерації про комерційну таємницю складається з Цивільного кодексу РФ, Федерального закону РФ від 29 липня 2004 р. “Про комерційну таємницю”, інших федеральних законів.

Нормативне визначення поняття “комерційна таємниця” міститься в ст. 3 Федерального закону “Про комерційну таємницю”, згідно з якою комерційна таємниця — конфіденційність інформації, що дозволяє її власнику за наявних або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти становище на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду. Дія даного Закону не поширюється на відомості, що становлять державну таємницю, по відношенню до якої застосовується законодавство РФ про державну таємницю.

Права власника інформації, що складає комерційну таємницю, виникають з моменту встановлення ним відносно такої інформації режиму комерційної таємниці, тобто правових, організаційних, технічних та інших заходів по охороні її конфіденційності. Режим комерційної таємниці не

може бути встановлений суб'єктами підприємництва, згідно зі ст. 5 даного Федерального закону, щодо відомостей:

- 1) які містяться в установчих документах, а також документах, що підтверджують внесення записів про юридичних та фізичних осіб підприємців до відповідних державних реєстрів;
- 2) які містяться в дозвільних документах на здійснення підприємницької діяльності;
- 3) про склад майна державних чи муніципальних унітарних підприємств, державних установ і щодо використання ними коштів відповідних бюджетів;
- 4) про забруднення навколишнього середовища, стан протипожежної безпеки, санітарно-епідеміологічну і радіаційну ситуацію, безпеку харчових продуктів та інші фактори, які негативно впливають на безпечне функціонування виробничих об'єктів, безпеки кожного громадянина і населення в цілому;
- 5) про чисельність, склад працівників, системи оплати праці, умови праці, охорону праці, показники виробничого травматизму та професійної захворюваності, про наявність вакансій;
- 6) про заборгованість по заробітній платі або інших соціальних виплатах;
- 7) про порушення законодавства РФ і факти притягнення до відповідальності за скоєння правопорушень;
- 8) про умови конкурсів або аукціонів по приватизації державної чи муніципальної (комунальної) власності;
- 9) про розмір та структуру доходів некомерційних організацій, розмір і склад їх майна, про їх витрати, про чисельність і оплату праці їх працівників, про використання безоплатної праці громадян в діяльності некомерційних організацій;
- 10) про перелік осіб, які мають право діяти без довіреності від імені юридичних осіб;
- 11) про обов'язковість на розголошення яких або недопустимість обмеженого доступу до яких встановлена іншими федеральними законами.

Федеральний закон "Про комерційну таємницю" регулює питання комерційної таємниці в межах трудових відносин, цивільно-правових відносин, відносин з органами державної влади, місцевого самоврядування, при виконанні державних контрактів для державних потреб, встановлює перелік заходів по охороні конфіденційності інформації, що повинні бути застосовані її власником, а також передбачає відповідальність за порушення даного Федерального закону.

Власник інформації, що складає комерційну таємницю, має не лише права, визначені законом, а й обов'язок надавати дану інформацію державним органам влади, органам місцевого самоврядування, а у випадку ненадання або перешкоджання в отриманні такої інформації несе відповідальність відповідно до ст. 15 Федерального закону.

Новим положенням у даному Законі є також обов'язок працівника, що перебував у трудових відносинах з власником комерційної таємниці і якому така інформація стала відома у зв'язку з виконанням ним трудових обов'язків, не розголошувати і не використовувати жодним протиправним чином дану інформацію протягом трьох років з моменту припинення трудових відносин.

Органи державної влади, місцевого самоврядування, інші державні органи зобов'язані створити умови, які забезпечують охорону конфіденційності інформації, що надається їм юридичними особами та індивідуальними підприємцями, а посадові особи даних органів не мають права розголошувати або передавати інформацію третім особам, використовувати її в корисливих або інших особистих цілях без згоди власника інформації, що складає комерційну таємницю.

Порушення даного Федерального закону тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність у відповідності до законодавства Російської Федерації.

Отже, законодавство РФ про комерційну таємницю регулює відносини, пов'язані з віднесенням інформації до комерційної таємниці, передачею такої інформації, охороною її конфіденційності з метою забезпечення балансу інтересів власників інформації, що складає комерційну таємницю, та інших учасників регульованих відносин, в тому числі держави, на ринку товарів, робіт, послуг та попередження недобросовісної конкуренції, а також визначає відомості, що не мають належати до комерційної таємниці.

### **2.3. Поняття та ознаки комерційної таємниці. Об'єкти та суб'єкти права власності на комерційну таємницю**

Комерційна таємниця, як засіб захисту господарської, торговельної та іншої діяльності, існувала ще в царській Росії. Вона була безпосередньо пов'язана з виробництвом, купівлею, продажем різноманітних продуктів, сировини, їх зберіганням, а також окремими аспектами фі-

нансової діяльності заводів, фабрик, купців, майстрів та інших суб'єктів господарювання.

В умовах планової економіки, яка склалася в подальшому і базувалася на державній власності, монополії держави в економічній сфері, широкому розповсюдженні та запровадженні в господарську діяльність досвіду провідних підприємств, новаторів в різноманітних галузях виробництва, питання про комерційну таємницю само собою відпало. Захист інформації при необхідності здійснювався за допомогою інститутів державної та службової таємниці.

Перехід до ринкової економіки та прийняття Україною західної (капіталістичної) моделі розвитку економіки і суспільства викликали потребу в нормативному закріпленні комерційної таємниці як невід'ємного елемента ринкових відносин, яким притаманні такі негативні явища, як недобросовісна конкуренція, підприємницьке шпигунство та інші. [67]

Для правового регулювання відносин суб'єктів підприємницької діяльності в цих умовах, захисту їх інтересів від неправомірних дій конкурентів необхідно було створити відповідну правову базу.

В зв'язку з цим Верховна Рада прийняла ряд важливих законів в галузі захисту підприємницької діяльності, серед них: “Про власність” від 7 лютого 1991 р., “Про підприємства в Україні” від 27 березня 1991 р. “Про банки і банківську діяльність” від 7 грудня 2000 р., “Про господарські товариства” від 19 вересня 1991 р., “Про інформацію” від 2 жовтня 1992 р., “Про державну таємницю” від 21 січня 1994 р., “Про захист від недобросовісної конкуренції” від 01 липня 1996р., “Про захист економічної конкуренції” від 11 січня 2001 р.

З прийняттям, зокрема, законів “Про підприємства в Україні” (втратив чинність у зв'язку з введенням в дію Господарського кодексу України 1 січня 2004 р.), “Про банки і банківську діяльність”, “Про державну таємницю” весь масив секретної інформації, що існував раніше, поділився на той період на два основних підмасиви:

- таємниці, що належать підприємствам, які не підпадають під державне управління (маються на увазі відомості, що становлять комерційну та банківську таємницю концернів, асоціацій, господарських товариств, комерційних банків і т.ін.);
- таємниці, що належать державі, тобто та інформація, яка становить державну таємницю.

Закон “Про інформацію” (далі — Закон) вніс деякі корективи до вказаного умовного підходу до класифікації секретів, встановивши поняття

“інформація з обмеженим доступом”, яка за своїм правовим режимом поділяється на:

- конфіденційну інформацію;
- таємну інформацію.

До таємної ст.30 Закону відносить інформацію: “яка містить відомості, що складають державну та іншу передбачену законом таємницю, розголошення якої може заподіяти шкоду особі, суспільству та державі”.

Положення даної статті чітко визначає суб’єкт, якому наноситься шкода в результаті розголошення секретної інформації. В переліку цих суб’єктів підприємство, як “самостійний суб’єкт господарювання, створений компетентним органом державної влади або органом місцевого самоврядування, або іншими суб’єктами для задоволення суспільних та особистих потреб шляхом систематичного здійснення виробничої, науково-дослідної, торговельної, іншої господарської діяльності” (ст. 62 ГКУ) відсутне.

З цього випливає, що комерційна таємниця не належить до секретної інформації.

Аналізуючи ст.30 цього ж Закону, слід зробити висновок про те, що до інформації з обмеженим доступом відноситься:

- інформація, яка містить комерційну таємницю;
- інформація, яка складає банківську таємницю;
- конфіденційна інформація, характер якої ст. 30 Закону не визначає.

Інститут комерційної таємниці є однією з важливих складових системи стійкості ринку, обмеження монополізму у виробничо-економічних відносинах, сфері надання послуг. Від того, наскільки ефективно він буде діяти, залежить успіх реформ, які здійснюються в Україні, та в кінцевому рахунку — благополуччя та процвітання підприємств і працюючих на них колективів людей.

Досвід багатьох західних фірм свідчить, що своєму становленню та розвитку вони багато в чому зобов’язані високому рівню організації та здійснення заходів, спрямованих на збереження своїх фірмових таємниць (“Кока-кола”, “Жиллет”, “Кодак”, “ІВМ” та багато інших). [67]

Однак слід відзначити, що не кожні підприємницькі стосунки обов’язково є конфіденційними. Не кожна інформація, розкрита в конфіденційних відносинах, обов’язково є комерційною таємницею. Тому важливо встановити, що становить зміст комерційної таємниці.

Поняття комерційної таємниці підприємства та його право на її захист юридично закріплене в ст.36 ГК: “відомості, пов’язані з виробництвом,

технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею”, а також в ст. 505 ЦК.

Можна припустити, що вказане визначення комерційної таємниці по мірі накопичення досвіду в практиці підприємництва може бути уточнене або скориговане.

Так, у тижневику “Аргументы и факты” (№28 за 1991 р.) автори публікації, пов'язаної з комерційною таємницею, пропонують поділити її на три види:

- власну комерційну таємницю;
- промислову таємницю;
- фінансово-кредитну таємницю.

До промислової таємниці вони, зокрема, пропонують віднести секрети виробництва, ноу-хау, відкриття, хімічну формулу будь-якої речовини, методи та засоби керівництва виробництвом, маркетинг і т.ін.

До фінансово-кредитної таємниці автори відносять — інформацію, яка міститься в бухгалтерських та інших фінансових документах. На їх думку, збереження в таємниці цієї інформації від усіх сторонніх суб'єктів господарювання є невід'ємною умовою в боротьбі з конкурентами, та її захист доцільний в зв'язку з небезпекою промислового шпигунства. [67]

У проєкті Закону “Про комерційну таємницю”, який пройшов перше читання у Верховній Раді України, ст.4 “Поняття комерційної таємниці” викладена в такій редакції: “Комерційна таємниця — це різновид інформації з обмеженим доступом ділового, комерційного характеру, яка має самостійну дійсну або потенційну економічну вартість завдяки тому, що не є загальновідомою або доступною іншим особам, які можуть використовувати її з комерційною метою, і належить юридичній або фізичній особам, є об'єктом розумних зусиль по її захисту, розголошення (передача, розкрадання, витік) якої може завдати матеріальної шкоди їх інтересам або сприяти успіху конкурентів”.

Слід зазначити, що ст.4 проєкту закону та ст.30 закону “Про інформацію” містять вказівку на те, що суб'єктами права власності на комерційну таємницю є як юридичні, так і фізичні особи.

Майновими правами інтелектуальної власності на комерційну таємницю є:

- 1) право на використання комерційної таємниці;
- 2) виключне право дозволяти використання комерційної таємниці;

- 3) виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;
- 4) інші майнові права інтелектуальної власності, встановлені законом.

Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною таємницею, якщо інше не встановлено договором. (ст.506 ЦК)

Своєрідно практикують поняття комерційної таємниці в західних країнах.

У США під комерційною (торговельною) таємницею розуміють будь-яку комерційну цінну інформацію або у формі винаходу, або у формі теоретичної промислової, або комерційної ідеї, або плану. [67]

У Німеччині поняття комерційної і виробничої таємниці сформульовано в законі “Про акціонерні товариства” і законі “Про підприємства”. Під ці поняття підпадають комерційні задуми, комерційно-політичні цілі фірми, предмет і результати нарад та засідань органів управління фірм, розміри і умови банківського кредиту, розрахунків цін, баланси і бухгалтерські книги, таємні компаньйони товариств, комп’ютерні програми, списки представників або посередників, картотеки клієнтів та інше. [67]

У Китаї згідно з законом проти недобросовісної конкуренції термін “підприємницької таємниці” належить до технічної або бізнес-інформації, що не є публічною, може давати економічні вигоди особі, яка має право на ці таємниці, є практичною і щодо якої особа вживала заходів для захисту її конфіденційності. [67]

У вітчизняній та зарубіжній літературі, практичній діяльності трапляються такі терміни, як “виробнича таємниця”, “ділова конфіденційна інформація”, “промислова таємниця”, “торговельний секрет”, “секрет фірми”, ноу-хау, тощо. На думку вчених, це не що інше, як секрети підприємства, що мають належати до комерційної таємниці.

У зв’язку з цим слід відзначити наступне [67]:

По-перше, комерційною таємницею підприємства може бути все, що не заборонено законом, корисно у підприємницькій діяльності та дає перевагу над конкурентами, які не володіють нею.

По-друге, інформація, яка складає комерційну таємницю підприємства, повинна мати певні ознаки та відповідно до Господарського кодексу, закону “Про інформацію” відповідати таким вимогам:

- бути власністю підприємства;
- бути засекреченою власником підприємства в його інтересах на визначений термін, у визначеному обсязі;

- мати дійсну або потенційну вартість з комерційних міркувань;
- не бути загальновідомою чи загальнодоступною згідно з законодавством України;
- надійно захищатися її власником або уповноваженою ним особою через систему кваліфікації інформації, розробку внутрішніх правил засекречення, схову, обігу, знищення та запобігання розголошенню, введення відповідного кодування носіїв інформації тощо;
- не захищатися авторським і патентним правом;
- не стосуватися негативної діяльності підприємства, здатної завдати шкоду суспільству (порушень законів, адміністративних помилок, забруднення навколишнього середовища тощо).

Крім цього, для комерційної таємниці характерно те, що вона [67]:

- реально або потенційно створює переваги в конкурентній боротьбі;
- із всієї власності підприємства, в тому числі і майнової, може бути найбільш цінною;
- з часом може втратити свою вартість, якщо не буде використана.

Комерційна таємниця, відповідно до законодавства України, є товаром, вона може продаватися або передаватися на договірній основі іншому підприємству за умови її нерозголошення.

Загальноvizнаним є положення про те, що до комерційної таємниці не слід відносити фундаментальні наукові дослідження, оскільки вони не приносять прибутку. Якщо ж ці дослідження набувають прикладного значення, вони можуть класифікуватись в якості комерційної таємниці. [67]

У певних випадках науково-технічну та ділову інформацію недоцільно класифікувати як комерційну таємницю через великі матеріальні витрати на її захист, труднощів проведення охоронних заходів, а також у зв'язку з її використанням в рекламній діяльності, або для підвищення іміджу підприємства. [67]

Вартість інформації, яка складає комерційну таємницю підприємства, визначається, як правило, її власником або уповноваженою ним особою або органом. При відсутності на підприємстві кваліфікованих спеціалістів для оцінки вартості інформації, яка може класифікуватись як комерційна таємниця, можуть залучатися на договірних засадах відповідні експерти.

Згідно з проектом закону “Про комерційну таємницю” вартість інформації, що складає комерційну таємницю, може вимірюватись “прямою дійсною шкодою, що заподіяна її розголошенням, або в розмірі відшкодування, встановленого сторонами при складенні угоди про збереження комерційної таємниці незалежно від спричинення заподіяної шкоди”.

Однією з основних ознак комерційної таємниці, уже зазначалось, є те, що вона є власністю юридичної або фізичної особи. Під правом власності на комерційну таємницю, як різновид права власності, слід розуміти врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією, що її складає, яка прирівнюється в правовідносинах до майна і захищається законодавством, як і право власності на майно і в тому ж порядку. Комерційна таємниця є об'єктом права інтелектуальної власності (гл. 16 ГК, гл. 46 ЦК).

Право власності на комерційну таємницю виникає з моменту її класифікації як такої у визначеному законом порядку і діє до закінчення терміну її засекречення або відчуження у встановленому законодавством порядку. В разі прийняття підприємством рішення про відчуження вказаного права воно здійснюється в тому ж порядку, що й відчуження права майнової та інтелектуальної власності.

Власник комерційної таємниці може володіти, користуватися та розпоряджатися нею на власний розсуд. Він може використовувати її для здійснення підприємницької та іншої, не забороненої законом, діяльності, передавати її без оплати або за плату у володіння та користування іншим особам, встановлювати будь-який ступінь і режим її секретності, способи захисту, включаючи обмеження або заборону доступу до неї (крім випадків, передбачених законодавством). Власник комерційної таємниці має право ані підтверджувати, ані заперечувати сам факт існування або відсутності її в нього. [67]

Згідно з закордонним досвідом та практикою підприємницької діяльності в Україні об'єктами права власності на інформацію, яка складає комерційну таємницю, можуть бути комерційні інтереси, включаючи формулу, склад, комбінацію, програму, пристосування, метод, техніку або процес, тощо та майно будь-якої цінності, яке являє собою документи, записи, звіти, протоколи, креслення, матеріали, штами мікроорганізмів, моделі, прилади, речовини тощо, а також різні ідеї у торгівлі, виробництві чи управлінні ними, та інші джерела інформації, які належать власникові комерційної таємниці, в тому числі у вигляді неоформлених або неповних патентів, формул, технічних проектів, ноу-хау, результатів досліджень, в тому числі програмних продуктів, різноманітних виробів, а також калькуляції витрат виробництва, структури ціни, зміст договорів, контрактів, даних про постачальників і клієнтів, ринки збуту, відомості про конфіденційні ділові переговори, огляди ринку, маркетингові дослідження, плани розвитку підприємств, їх інвестицій та інші відомості, які являють під-

приємницький, або інший інтерес, порушення якого може завдати збитків її власникові. [67]

Суб'єктом права власності на комерційну таємницю, відповідно до чинного законодавства України, зокрема Господарського кодексу, Цивільного кодексу, законів “Про інформацію”, “Про науково-технічну інформацію” тощо, є: держава, громадяни України, інших держав, підприємства, установи, організації всіх форм власності, які здійснюють свою діяльність відповідно до законодавства України і визначили інформацію, яка складає їх комерційну таємницю, або придбали її у встановленому законодавством порядку, як комерційну таємницю.

## **2.4. Система правового захисту комерційної таємниці підприємства, її елементи та складові**

Перехід до ринкової економіки обумовив появу в українському законодавстві, юридичній та економічній літературі ряду нових понять, таких як комерційна таємниця, ділова інформація, секрет виробництва, торговельний секрет, ноу-хау, конфіденційна інформація, інформація обмеженого доступу. Ці поняття можна об'єднати найбільш вживаним терміном — комерційна таємниця. [67]

Закони України “Про інформацію” від 2 жовтня 1992 р., “Про захист від недобросовісної конкуренції” від 7 червня 1996 р., “Про банки і банківську діяльність” від 7 грудня 2000 р., “Про захист економічної конкуренції” від 11 січня 2001 р. та інші, а також Господарський та Цивільний кодекси регулюють спеціальний правовий режим охорони комерційної таємниці та інших видів інформації, пов'язаної з необхідністю захисту законних інтересів суб'єктів підприємницької діяльності.

Вказані та інші законодавчі акти, спрямовані на розвиток правил чесної конкуренції, в той же час забороняють вторгнення в сферу чужих технологічних та комерційних секретів недозволеними методами. Вони дають підприємствам підґрунтя для створення правових систем захисту комерційної таємниці, які дозволяють організувати охорону відомостей, які складають комерційну таємницю, що належать їм. Одночасно вказані та інші закони України містять правові основи відшкодування підприємствам матеріальної та моральної шкоди, яку можуть заподіяти підприємству своїми неправомірними діями конкуренти, персонал підприємства,

представники контрольно-спостережних та інших органів державної влади і управління. [67]

З метою захисту своїх законних прав та інтересів щодо захисту комерційної таємниці суб'єкти господарювання можуть на законодавчій основі створювати систему захисту комерційної таємниці підприємства.

Мотивами порушення питання про створення такої системи можуть бути: досягнутий підприємством високий рівень науково-виробничої діяльності, виконання будь-яких унікальних робіт, надання кваліфікованих послуг, поява нових технологій на основі ноу-хау, оригінальні комп'ютерні програми, розроблені стратегічні програми розвитку підприємства, планування рекламних заходів і т.ін., що потребують застосування захисних режимних заходів.

Ще одним мотивом створення правової системи захисту комерційної таємниці повинно бути чітке розуміння керівником підприємства, що без створення такої системи будь-які юридичні претензії до недобросовісних конкурентів, клієнтів, штатних співробітників підприємства, посадових осіб органів державного управління виявляться безпідставними і не будуть мати юридичної сили. [67]

Накопичений практичний досвід свідчить, що підготовку до створення системи правового захисту комерційної таємниці підприємства слід починати зі здійснення поглибленого аналізу всієї господарської, науково-виробничої, фінансової, управлінської, маркетингової та іншої діяльності підприємства.

Виходячи з досвіду захисту секретів західними фірмами, можна рекомендувати здійснити такий аналіз шляхом відповідей на питання, які містяться у зразку анкети підприємства-конкурента з виділенням також інформації, яка може класифікуватись як секретна.

До проведення аналізу доцільно залучати найбільш кваліфікованих робітників всіх структурних підрозділів підприємства: наукових співробітників, економістів, інженерно-технічний склад, менеджерів, маркетингологів, фінансистів, юристів і т.ін.

Важливо, щоб документ, підготований за результатами аналізу, найбільш повно віддзеркалював "обличчя" підприємства, розкривав його місце на ринку, перспективи розвитку та слугував переконливою основою для організації роботи по створенню на підприємстві системи правового захисту комерційної таємниці. [67]

Після проведеного детального аналізу діяльності підприємства та в залежності від його результатів керівник підприємства на основі ст.30 Закону "Про інформацію", ст. 52 Закону "Про банки і банківську

діяльність” може прийняти рішення про встановлення режиму доступу до інформації ділового, професійного, виробничого, банківського та іншого характеру, яка може бути віднесена, на підставі зазначених законів, до категорій “комерційна таємниця”, “банківська таємниця”, “конфіденційна інформація”.

Теоретичні розробки спеціалістів в галузі захисту інформації В.М. Чаплигіна, В.А. Рубанова, Е. Солов'йова (Російська Федерація), І. Давидова, А.А. Чернявського, Г.О. Андрощука, П.П. Крайньова, Г.К. Нікіфорова, С.С. Нікіфорова (Україна), Л. Хофмана (США), Ж. Бержъє (Франція), а також практика збереження секретів західними фірмами інформації обмеженого доступу свідчить про те, що основними елементами та складовими системи правового захисту комерційної таємниці є:

1. **Юридичне закріплення** в основоположних документах підприємства: статуті, засновницькому та колективному договорах, правилах внутрішнього трудового розпорядку права на комерційну таємницю. Основою для юридичного закріплення права підприємства на комерційну таємницю є положення, що містяться в Господарському та Цивільному кодексах, законах України “Про інформацію”, “Про колективні договори та угоди”, а також Кодексі законів про працю України.
2. **Визначення відомостей**, які підлягають захисту як комерційна таємниця, розробка переліку таких відомостей, затвердження його як офіційного нормативного документа підприємства, доведення його до відома персоналу підприємства, який має безпосереднє відношення до цих відомостей за посадою чи характером виконуваної роботи. Основою для визначення відомостей, які будуть захищатись як комерційна таємниця, є також положення, що містяться в Господарському та Цивільному кодексах, законах України “Про інформацію”, “Про колективні договори та угоди”, Кодексі законів про працю України.
3. **Якісний підбір персоналу** підприємства для роботи з відомостями категорії “комерційна таємниця”, виховання та навчання співробітників у зв'язку з їх роботою з такого роду інформацією, підготовка для них методичних положень, інструкцій, пам'яток, пов'язаних з поводженням з комерційною таємницею, створення матеріальних і моральних стимулів, що спрямовані на збереження комерційної таємниці.
4. **Визначення порядку допуску та доступу** до комерційної таємниці підприємства його співробітників, представників органів

державного управління, партнерів, клієнтів, отримання від них юридичних документів, які зобов'язують їх на правовій основі зберігати комерційну таємницю. Ця вимога базується на конституційних положеннях, законах про органи виконавчої влади (“Про міліцію”, “Про службу безпеки України”, “Про державну податкову службу”) та інших.

5. **Встановлення порядку збереження** комерційної таємниці при укладанні господарських та інших підприємницьких договорів, а також ведення ділових переговорів, відвідання підприємства перед укладенням договорів. Цей елемент систем захисту комерційної таємниці базується на вимогах Цивільного кодексу України, ряді указів Президента України, постанов Кабінету Міністрів України, міжнародних договорах України.
6. **Створення на підприємстві** відповідно до закону “Про інформацію” порядку поводження з інформацією обмеженого користування, який виключає можливість витоку інформації при роботі з комерційною таємницею, при розробленні рекламних матеріалів, при веденні співробітниками ділових переговорів, під час наукових конференцій, семінарів, виступів у пресі. Даний елемент системи правового захисту комерційної таємниці повинен враховувати вимоги закону “Про інформацію”, закону “Про науково-технічну інформацію” від 25 червня 1993 р., закону “Про основи державної політики в сфері науки і науково-технічної діяльності” від 13 грудня 1991 р.
7. **Визначення порядку взаємодії** підприємства з представниками правоохоронних органів, контрольно-спостережних органів виконавчої влади, які на законодавчій основі можуть мати доступ до комерційної таємниці при виконанні ними своїх службових завдань та функцій. Даний елемент системи правового захисту комерційної таємниці повинен будуватися з урахуванням вимог законів: “Про місцеве самоврядування в Україні” від 21 травня 1996 р., “Про міліцію” від 20 грудня 1990 р., “Про прокуратуру” від 5 листопада 1991 р., “Про службу безпеки України” від 25 березня 1992 р., “Про державну контрольно-ревізійну службу в Україні” від 26 січня 1993 р. та інших.
8. **Організація спеціального діловодства** документів категорії “комерційна таємниця”. Цей елемент системи захисту комерційної таємниці регулює порядок роботи та поводження з такими документами, їх підготовкою, обліком, розмноженням, пересиланням,

зберіганням, періодичною перевіркою їх наявності та знищення. Цей елемент системи захисту комерційної таємниці повинен враховувати вимоги Декрету Кабінету Міністрів України “Про стандартизацію і сертифікацію” від 10.05.93 р. № 46–93, “Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави”, затвердженої постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

Викладені елементи та складові системи правового захисту комерційної таємниці повинні бути задіяні та використані в повній єдності та взаємодії. Якщо хоча б одна із складових викладеної вище системи не буде задіяна, то система не виконає свого призначення, оскільки може статися витік відомостей, які складають комерційну таємницю, та підприємство може втратити юридичні підстави для підняття питання про відшкодування нанесених конкурентом або персоналом підприємства матеріальних збитків [67]

## **2.5. Юридичне закріплення права підприємства на комерційну таємницю**

### **Статут підприємства**

Стаття 62 Господарського кодексу констатує, що підприємство, якщо закон не встановлює інше, діє на основі статуту.

В розроблених Міністерством праці, Міністерством економіки та Фондом державного майна зразках статутів міститься розділ “Права та обов’язки підприємства”. Якщо підприємство має намір закріпити за собою право на володіння та захист комерційної таємниці, в цьому розділі статуту необхідно обов’язково зафіксувати положення, які витікають із Цивільного та Господарського кодексів про те, що підприємство має право: класифікувати інформацію, яка йому належить, як комерційну таємницю, визначати її склад, обсяг та порядок захисту.

Також слід зазначити, ким визначається порядок захисту вказаної інформації (як правило, керівником або власником підприємства), та хто має право вимагати від співробітників виконання встановленого на підприємстві порядку та правил збереження комерційної таємниці.

Важливо зафіксувати, що підприємство має право не виконувати вимоги правоохоронних органів, а також інших органів державного управління, якщо ці вимоги виходять за межі їх повноважень, пов'язаних з доступом до комерційної таємниці.

Перелік обов'язків повинен містити вимоги про забезпечення підприємством збереження конфіденційних комерційних відомостей, пов'язаних з виробництвом, технологічною інформацією, управлінням, фінансами, маркетингом, науковою роботою та іншою діяльністю підприємства.

Зафіксовані в статуті положення дають підприємству право: вимагати захисту інтересів підприємства перед державними і судовими органами; включати вимоги по захисту конфіденційної інформації в усі види договорів підприємницького характеру; користуватися цією інформацією для отримання прибутків; домагатися відшкодування нанесених конкурентами або персоналом підприємства економічних збитків у випадку витоку інформації; видавати документи з питань забезпечення збереження комерційної таємниці, створювати структурні підрозділи економічної безпеки. Підстави для внесення перерахованих положень — Цивільний кодекс, Господарський кодекс, а також Закон “Про інформацію” від 2 жовтня 1992 р. (ВВР. — 1992. — №48), Закон “Про захист від недобросовісної конкуренції” від 7 червня 1996 р. (ВВР. — 1996. — №27), Закон “Про захист економічної конкуренції” від 11 січня 2001 р. №2210-III.

Практика показує, що не всі підприємства відповідально підходять до ретельного опрацювання проробки в статуті тих нормативних положень, які дійсно закріплюють право підприємства на комерційну таємницю та організацію роботи по її захисту. [67]

### **Засновницький договір**

Господарські товариства, корпорації, асоціації, підприємства з іноземними інвестиціями та деякі інші види підприємств відповідно до законодавства України здійснюють свою діяльність не лише на підставі статуту, а й засновницького договору.

В засновницькому договорі таких структур зокрема зазначається склад засновників, розмір та порядок утворення статутного фонду, порядок оцінки нематеріальних внесків, порядок прийняття рішень по управлінню товариством та інші.

Нерідко внеском в їх статутний фонд є інтелектуальна власність, яка захищається законодавством: нові технології, ноу-хау, унікальне обладнання, комп'ютерні програми, які складають (або можуть складати) ко-

мерційну таємницю одного чи кількох засновників та потребують встановлення відповідного порядку її захисту.

В зв'язку з цим у засновницькому договорі на підставі Господарського кодексу, закону “Про господарські товариства” від 19 вересня 1991 р. (ВВР. — 1991. — №49), слід визначити права засновників таких підприємств на інтелектуальну власність, ноу-хау, порядок доступу до неї інших засновників та учасників.

- ⊙ *Основні положення, які закріплюють право на комерційну таємницю в статуті, повинні бути відображені і в засновницькому договорі, перш за все тих підприємств, в яких відсутні статуту: договірних об'єднаннях, повних і командитних товариствах та інших.*

При закріпленні права на комерційну таємницю об'єднань слід враховувати, що підприємства, які входять до їх складу, в тому числі інших держав (ст. 121 Господарського кодексу), зберігають за собою статус, а відповідно і права юридичної особи.

Дане правове положення слід розглядати як можливість входження в об'єднання будь-якого із його засновників з власною системою захисту комерційної таємниці, але може бути прийняте рішення про спільну власність на комерційну таємницю всіх або частини засновників об'єднання на умовах, передбачених засновницьким договором. [67]

### **Колективний договір**

В умовах ринкових відносин значення колективних договорів не лише зменшується, а, навпаки, зростає. Оскільки захист комерційної таємниці спрямований на забезпечення економічних та матеріальних інтересів всього колективу підприємства, в забезпеченні його безпеки, тією чи іншою мірою повинні брати участь всі співробітники підприємства. [67]

Відповідно до Кодексу законів про працю України (КЗпП) й Закону “Про колективні договори та угоди” від 1 липня 1993 р. (ВВР. — 1993. — №36) колективний договір повинен укладатися на всіх підприємствах, які використовують найману працю, між власником або уповноваженим ним органом і трудовим колективом.

У колективному договорі з позицій правового захисту комерційної таємниці необхідно передбачити положення, які містять взаємні обов'язки адміністрації та колективу співробітників підприємства щодо забезпечення збереження комерційної таємниці.

В договорі доцільно передбачити порядок робіт з комерційною інформацією (з документами, виробами, продукцією) з боку співробітників, які залучаються до роботи з ними, а також визначити відповідальність за порушення порядку роботи з комерційною таємницею, а також зобов'язати адміністрацію забезпечити працівників підприємства, які мають відношення до комерційної таємниці, необхідними методичними матеріалами і інструкціями, пам'ятками, проводити навчання працівників з проблем захисту комерційної таємниці.

Можна рекомендувати зафіксувати в колективному договорі: “Для запобігання нанесення економічних збитків підприємству адміністрація зобов'язується організувати та забезпечити систему заходів по захисту комерційної таємниці”, а колектив (або його частина, яка має доступ до конфіденційної комерційної інформації) “зобов'язується дотримуватись встановлених на підприємстві порядку та правил збереження комерційної таємниці”. [67]

Відповідальність за порушення встановленого на підприємстві порядку роботи з відомостями, які складають комерційну таємницю, в договорі може бути визначена досить чітко. Наприклад, позбавляти порушників порядку роботи з конфіденційною комерційною таємницею, різноманітних премій, винагород, відстороняти від роботи з такою інформацією, притягати до дисциплінарної та іншої відповідальності, передбаченої КЗпП України і т.ін. [67]

Зобов'язання колективу мають виключно важливе значення, оскільки покладають на кожного співробітника відповідальність за весь колектив, і в цьому суттєва відмінність системи захисту комерційної таємниці від системи захисту державних секретів (де відповідальність за розголошення несе сам співробітник і, можливо, його керівник, а збитки наносяться державі). Якщо ж з вини співробітника відбувся виток комерційної таємниці, економічні збитки наносяться безпосередньо підприємству, його трудовому колективу, кожному співробітникові підприємства, а за певних умов можуть спричинити банкрутство підприємства.

Як показує практика, процес прийняття колективного договору, в якому закладаються положення про збереження комерційної таємниці, не завжди проходить гладко, особливо в наукових колективах. Тому при підготовці до укладення договору повинна бути проведена велика роз'яснювальна робота серед колективу підприємства. Головна мета — переконати членів колективу в необхідності забезпечення захисту комерційної таємниці як найважливішого елемента економічного процвітання підприємства та особистого благополуччя кожного працівника. [67]

Підстави для включення зазначених положень — Господарський кодекс, КЗпП України (глава II), Закон України “Про колективні договори і угоди”.

### **Правила внутрішнього трудового розпорядку**

Основні положення, які повинні знайти відображення в правилах внутрішнього трудового розпорядку підприємства, якщо воно має намір закріпити право на комерційну таємницю та організацію роботи по попередженню витоку конфіденційної комерційної інформації, зводяться до обов’язків як адміністрації, так і співробітників підприємства.

Зокрема, обов’язки адміністрації повинні зводитись до наступного:

- створити необхідні умови для виконання працівниками встановлених на підприємстві порядку та правил забезпечення збереження конфіденційної комерційної інформації;
- інструктувати працівників, пов’язаних з комерційною таємницею, про правила її збереження з оформленням письмових зобов’язань про її нерозголошення (при прийнятті на роботу, при звільненні або переводі на іншу роботу, пов’язану з комерційною таємницею);
- проводити комплекс організаційних, економічних, інженерно-технічних та виховно-профілактичних заходів, спрямованих на попередження витоку конфіденційної комерційної інформації, нейтралізацію загрози економічної безпеки підприємства;
- включати в посадові інструкції працівників обов’язки по збереженню комерційних секретів підприємства;
- здійснювати контроль за виконанням працівниками підприємства встановлених вимог збереження комерційної таємниці підприємства;
- притягати до дисциплінарної відповідальності порушників вимог по захисту комерційної таємниці, відповідно до ст. 147 КЗпП України. [67]

Обов’язки робітників можна викласти в такій редакції:

- суворо дотримуватись вимог по забезпеченню збереження комерційної таємниці, встановлених на підприємстві відповідними внутрішніми нормативними документами (положеннями, правилами, інструкціями);
- вживати заходів щодо виявлення причин та обставин, які можуть нанести економічні збитки підприємству;

- надійно зберігати інформацію, яка міститься в носіях комерційної таємниці (документах, рукописах, кресленнях, дискетах, магнітних стрічках і т.ін.). [67]

## **2.6. Визначення відомостей, що складають комерційну таємницю підприємства**

Однією з першочергових проблем у вирішенні завдань по захисту комерційної таємниці підприємства є правильне та своєчасне визначення інформації, яка буде захищатись як комерційна таємниця. Правильне і своєчасне визначення відомостей, які складають комерційну таємницю, є одним з центральних елементів у системі заходів, які повинні здійснюватись підприємством по захисту своєї власності та забезпеченню його економічної безпеки. За інших умов ефективність та дієвість системи правового захисту комерційної таємниці підприємства значно знизиться.

Віднесення відомостей до комерційної таємниці диктується перш за все необхідністю забезпечення економічної безпеки підприємств, що здійснюють свою діяльність в умовах конкурентної боротьби, недобросовісної конкуренції. [67]

Оскільки секретність певної інформації може сприяти досягненню максимального прибутку, як комерційну таємницю доцільно захищати ті відомості підприємства, які дозволяють підвищити конкурентоспроможність його товарів та послуг на ринку.

При організації роботи по визначенню відомостей, які підлягають захисту як комерційної таємниці, слід вирішувати два основних завдання, які стоять перед підприємством: по-перше, на правовій основі визначити найбільш цінну інформацію комерційного характеру з метою попередження її витоку до конкурентів, та, по-друге, виділити таку, яка б сприяла підвищенню пріоритету, іміджу підприємства на ринку та могла б бути використана в рекламних цілях. [67]

При організації цієї роботи слід виходити зі статей 505 Цивільного кодексу та 36 Господарського кодексу, а також з того, що в Україні відсутній загальнодержавний перелік відомостей, які складають комерційну таємницю, яким можна було б керуватися підприємствам.

Такого переліку, виходячи зі змісту Господарського та Цивільного кодексів, закону України “Про інформацію”, бути не може (на противагу Переліку відомостей, що складають державну таємницю).

При організації роботи по визначенню відомостей, що складають комерційну таємницю, необхідно враховувати чинні нормативно-правові акти, які регулюють відносини в галузі інформації, а також ряд інших обставин. [67]

По-перше, необхідно керуватися вимогами постанови Кабінету Міністрів України № 611 від 9 серпня 1993 р. “Про перелік відомостей, які не є комерційною таємницею” (Збірник постанов Уряду України. — 1993. — № 12), яка встановлює 7 блоків відомостей, що не можуть складати комерційну таємницю, в тому числі:

- установчі та інші документи, які дозволяють займатися підприємницькою діяльністю;
- відомості, необхідні для перевірки обчислення і сплати податків та інших обов’язкових платежів;
- відомості про чисельність та склад працюючих, їх заробітну платню в цілому та за професіями і посадами;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізації продукції, яка наносить шкоду здоров’ю, розміри заподіяної при цьому шкоди і т. ін.

По-друге, при визначенні відомостей, що складають комерційну таємницю, слід враховувати положення Закону “Про інформацію” про те, що не може встановлюватися режим обмеженого доступу до інформації, якщо вона загальновідома, загальнодоступна на законних підставах і не потребує захисту.

По-третє, не підлягають захисту як комерційна таємниця винаходи, раціоналізаторські пропозиції та інша інформація промислового характеру, право власності на які оформлені патентом, авторським свідоцтвом, оскільки ця інтелектуальна власність юридичних або фізичних осіб вже захищена патентним або авторським правом.

Визначальною ознакою (обов’язковим реквізитом) документів, які містять комерційну таємницю, є наявність в них обмежувальних грифів типу “Комерційна таємниця — особливо важливо”, “Комерційна таємниця — суворо конфіденційно”, “Комерційна таємниця — конфіденційно” та інших (за винятком обмежуючих грифів, які належать до державної таємниці: “Цілкою таємно”, “Таємно” і т. ін.).

По-четверте, до комерційної таємниці не можуть належати відомості, які складають державну таємницю. Відповідно до ст. 12 Закону України “Про державну таємницю” від 21 вересня 1999 р. (ВВР. — 1994. — № 16) такі відомості концентруються в Переліку відомостей, що складають дер-

жавну таємницю, який формує та оприлюднює в офіційних виданнях Служба безпеки України на підставі рішень державних експертів з питань таємниць.

Крім того, відповідно до зазначеної статті цього ж закону відомості, що складають державну таємницю, крім Переліку можуть міститися в галузевих, відомчих, міжгалузевих або міжвідомчих розгорнутих переліках відомостей, що складають державну таємницю а також переліках окремих підприємств. [67]

Слід мати на увазі, що Закон “Про державну таємницю” (ст. 15) регламентує порядок розсекречення відомостей, які складають державну таємницю. Дана правова норма не виключає можливість, за певних обставин (відмова держави від секретів, конверсія підприємств військово-промислового комплексу і т. ін.), переростанні державної таємниці в комерційну та її використання підприємством у виробничих та інших цілях. [67]

Нарешті, при визначенні відомостей, які складають комерційну таємницю, слід враховувати цікавість та прагнення конкурентів, які завжди націлені на отримання необхідної інформації про суперника для виживання в конкурентній боротьбі.

Практика показує, що основні спрямування конкурентів зводяться до отримання інформації про:

- фінансове становище підприємства-конкурента;
- наукові розробки, ідеї;
- керівництво та розробників продукції, устаткування, ідей, стратегій тощо;
- прогнози його розвитку в майбутньому;
- умови контрактів та угод;
- відомості щодо технологічної та технічної специфікації вироблюваної та перспективної продукції;
- маркетинг та стратегію цін;
- майбутні рекламні компанії;
- систему та організацію безпеки підприємства.

Організацію роботи по визначенню відомостей можна умовно поділити на три етапи. [67]

**Перший етап.** Він передбачав видання на підставі ст. 162 Господарського кодексу та статуту підприємства наказу про визначення відомостей, які складають комерційну таємницю підприємства.

В ньому повинні бути передбачені організаційні заходи, пов'язані з проведенням даної роботи, зокрема:

- створення постійно діючої комісії підприємства по комерційній таємниці;
- визначення осіб, яким надається право попередньо класифікувати інформацію як комерційну таємницю (інженерно-технічний склад, наукові співробітники, менеджери, маркетологи, економісти, юристи і т. ін.);
- методика проведення роботи по визначенню відомостей, які можуть складати комерційну таємницю;
- порядок документації всієї роботи по визначенню відомостей, що складають комерційну таємницю підприємства;
- строки підготовки переліку відомостей, що складають комерційну таємницю підприємства та його подання на затвердження керівнику підприємства.

Як правило, пропозиції про включення конкретних відомостей в список на розгляд постійно діючої комісії вносять керівники структурних підрозділів (начальники цехів, управлінь, відділів, лабораторій, бюро і т. ін.) в письмовій формі у вигляді доповідних або службових записок, подань і т. ін. Пропозиції повинні бути аргументованими, містити відповідні юридичні та маркетингові обґрунтування.

Якщо на підприємстві відсутні достатньо кваліфіковані фахівці в галузі захисту інформації, до цієї роботи на договірній основі можуть бути залучені спеціалісти або експерти інших підприємств, установ та організацій.

**Другий етап.** Він полягає в тому, що постійно діюча комісія повинна зробити оцінку можливого розміру збитків, якщо підприємство своєчасно не “засекретить” важливу інформацію як комерційну таємницю і з цієї причини станеться її витікання.

На цьому ж етапі необхідно сформулювати та визначити можливі негативні наслідки для підприємства у випадку відкритого використання тих чи інших відомостей, які включені в список для розгляду як комерційна таємниця, але за деяких об'єктивних або суб'єктивних причин не отримали статус комерційної таємниці.

Негативними наслідками в цих випадках можуть бути:

- втрата пріоритету в наукових дослідженнях, фактична неможливість патентування та продажу ліцензій на науково-технічні досягнення;
- зрив вигідних контрактів та угод;
- необхідність проведення додаткових маркетингових досліджень та розробки нової ринкової стратегії;

- скорочення конкурентами матеріальних витрат на проведення науково-дослідних та дослідно-конструкторських робіт;
- розірвання ділових відносин з одним або кількома партнерами і т. ін. [67]

**Третій етап.** Він полягає в формуванні переліку відомостей, що складають комерційну таємницю підприємства, та введення його в дію.

Аналіз закордонної практики й робіт російських та українських авторів з питань правового захисту комерційної таємниці дозволяє визначити оптимальну структуру переліку відомостей, які складають комерційну таємницю підприємства.

Його структурні елементи пов'язані з певними сторонами діяльності підприємства та включають в себе відомості про:

- виробництво;
- стан ринку;
- управління;
- партнерів;
- плани;
- контракти;
- наради;
- ціни;
- фінанси;
- науково-технічні досягнення;
- власну безпеку підприємства.

У переліку необхідно зазначити контрольні терміни або обставини, при настанні яких може постати питання про розсекречення певних відомостей, що втратили своє значення. Також слід враховувати, що ступінь конфіденційності конкретних відомостей може змінюватись від етапу діяльності підприємства та зміни цінності інформації в часі. [67]

Розроблений постійно діючою комісією перелік повинен бути поданий керівникові підприємства на затвердження. Якщо останній згоден з ним, перелік вводиться в дію наказом по підприємству як офіційний документ. Він повинен бути обов'язково доведений до виконавців в частині, що їх стосується, під власний підпис.

Остання обставина дає підстави підприємству на правовій основі застосовувати будь-які заходи до співробітника підприємства у випадку розголошення ним комерційної таємниці, з якою він був ознайомлений.

Перелік відомостей повинен періодично коригуватись. З нього повинні виключатися ті відомості, які втратили своє значення та одночасно вноситися інші, які потребують правового захисту. [67]

## 2.7. Допуск та доступ до комерційної таємниці

На підприємстві обов'язково на законодавчій основі повинні бути вжиті заходи по регулюванню прав володіння, користування та розпорядження конфіденційною інформацією, що складає його комерційну таємницю. Для запобігання витіканню конфіденційної інформації необхідно встановити порядок допуску до комерційних секретів певних осіб персоналу підприємства.

За основу організації роботи по допуску до комерційної таємниці доцільно взяти вимоги, які належать до порядку допуску до державних секретів. Порядок допуску до державних секретів досить чітко регламентований Законом України “Про державну таємницю” (ст. 22–30).

Під **допуском до комерційної таємниці** слід розуміти письмове розпорядження керівника (власника) підприємства або уповноваженої ним особи, яке надає конкретному співробітникові підприємства право на роботу або ознайомлення з документами, виробами та іншими носіями інформації, які класифіковані підприємством як комерційна таємниця [67].

- ➔ На підприємстві, як правило, встановлюється триступенева система важливості комерційної таємниці, яка позначається такими обмежувальними грифами:
- “Комерційна таємниця — особливо важливо” (“КТ–ОВ”)
  - “Комерційна таємниця — суворо конфіденційно” (“КТ–СК”)
  - “Комерційна таємниця — конфіденційно” (“КТ–К”).

З урахуванням цього допуск конкретному співробітникові оформлюється до одного із вказаних ступенів важливості відомостей в залежності від посади співробітника або характеру виконуваної ним роботи.

Допуск до комерційної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, комерційної, наукової чи іншої діяльності. Допуск вважається правомірним, що має юридичну силу, якщо він надається співробітнику підприємства наказом керівника (власника) підприємства або уповноваженої ним особи.

Надання допуску передбачає:

- перевірку співробітника в зв'язку з допуском до комерційної таємниці;
- ознайомлення співробітника зі ступенем відповідальності за порушення законодавства, пов'язаної з розголошенням ним комерційної таємниці.

При вирішенні питання про надання допуску до комерційної таємниці слід враховувати такі фактори:

- наявність у співробітника підприємства обґрунтованої необхідності в роботі з комерційною таємницею;
- відсутність у співробітника судимості за тяжкі злочини і, перш за все, за протиправні дії, пов'язані з комерційним шпигунством, розголошенням державної та комерційної таємниці, зловживаннями в сфері кредитно-фінансової і економічної діяльності;
- відсутність у співробітника психічних захворювань або розладів, вживання наркотичних засобів, алкоголю;
- повідомлення про себе недостовірних відомостей в процесі підготовки матеріалів до оформлення допуску;
- відсутність в оформлюваного зв'язків з числа співробітників конкуруючих фірм.

Співробітник підприємства, якому наданий допуск до комерційної таємниці, зобов'язаний:

- не допускати розголошення будь-яким способом комерційної таємниці, яка йому довірена або стала відома у зв'язку з виконанням службових обов'язків;
- не сприяти вітчизняним та іноземним конкурентам у здійсненні діяльності, яка завдає шкоди інтересам підприємства;
- виконувати вимоги режиму, який встановлений "Положенням про комерційну таємницю підприємства та правила її збереження";
- дотримуватись інших вимог законодавства про комерційну таємницю.

Оформлення допуску співробітника підприємства до комерційної таємниці передбачає і можливість його позбавлення на законних підставах. Причинами та підставами позбавлення допуску можуть бути [67]:

- розголошення співробітником довіреної йому комерційної таємниці;
- грубе порушення співробітником "Положення про комерційну таємницю підприємства та правила її збереження";
- втрата співробітником документів та інших матеріальних носіїв, які містять комерційну таємницю;
- надходження відносно співробітника відомостей, що компрометують його, які він приховував і які не могли бути враховані при вирішенні питання про його допуск;
- переведення співробітника на іншу ділянку роботи або посаду, що не пов'язана з необхідністю допуску до відомостей, які складають комерційну таємницю.

Позбавляти співробітника допуску мають право ті ж особи, які санкціонували йому допуск до комерційної таємниці. Якщо співробітник не згоден з таким рішенням власника підприємства або уповноваженої ним особи, він, відповідно до конституційного, цивільного та трудового права може оскаржити його в судовому порядку.

Власник підприємства або уповноважена ним особа мають право розробляти та використовувати власну, але таку що не суперечить чинному законодавству, методологію вивчення та перевірки кандидата для роботи, пов'язаної з відомостями, що складають комерційну таємницю [67].

А.В. Крисін, автор науково-виробничого видання “Безопасность предпринимательской деятельности” (Москва, 1996), рекомендує використовувати для вивчення та перевірки кандидатів різноманітні тестові методики, зокрема: особистісні опитувальні аркуші, бланкові тести: СМІЛ, КЕТТЕЛА, АЗЕНКА, РСК, УСК, ТОМАСА тощо. [52]

Правомірне використання у вивченні та перевірці кандидатів на допуск до комерційних секретів поліграфа (детектора брехні, ідея якого належить відомому українському вченому Олександру Романовичу Лур'є з Харкова), але його застосування можливо лише з особистої згоди особи, що перевіряється.

Результати перевірки не повинні приховуватись від кандидата на роботу з комерційною таємницею (згідно зі ст. 32 Конституції України і ст. 9 закону “Про інформацію”).

Організація роботи по оформленню допуску до комерційної таємниці повинна бути покладена на підрозділ безпеки. Доцільно, щоб цим підрозділом, спільно з керівниками інших підрозділів, передбачених статутом або положенням про підприємства, був розроблений перелік посад співробітників, які за своїм службовим становищем або за родом виконуваної роботи обов'язково повинні мати допуск до тієї чи іншої категорії важливості відомостей, які становлять комерційну таємницю підприємства. Керівник (власник) підприємства або уповноважена ним особа повинні затвердити даний перелік [67].

Від співробітника, якому оформлений допуск до комерційної таємниці, береться письмове зобов'язання про нерозголошення комерційної таємниці, яка буде йому довірена. Зобов'язання може мати довільну форму, але воно повинно мати такі реквізити:

- прізвище, ім'я, по-батькові співробітника;
- займана посада;
- зобов'язання не розголошувати відомості, що складають комерційну таємницю;

- попередження про те, що у випадку розголошення довірених секретів з працівником може бути розірвана трудова угода за ініціативою власника підприємства, або він може бути притягнутий до відповідальності в порядку, встановленому законодавством України;
- дата та власноручний підпис співробітника, який дав зобов'язання;
- підпис представника служби безпеки, який проінструктував співробітника, що підписав зобов'язання (типовий зразок зобов'язання додається).

При звільненні співробітника підприємства, який мав допуск до комерційної таємниці і дійсно володів нею, у нього слід, згідно зі ст. 34 Конституції України і “Положення про комерційну таємницю підприємства та правила її збереження”, відібрати так зване попередження-зобов'язання про нерозголошення ним після звільнення комерційних секретів, до яких він мав доступ (типовий зразок попередження-зобов'язання додається).

Мета відбору такого попередження-зобов'язання [67]:

- застерегти співробітника від розголошення комерційних секретів, які стали йому відомі під час роботи на підприємстві;
- створити юридичні гарантії для попередження можливого витікання комерційної таємниці до конкурентів через колишнього співробітника підприємства;
- юридично гарантувати право підприємства на відшкодування можливих матеріальних або моральних збитків у випадку порушення колишнім співробітником своїх зобов'язань перед підприємством.

**Доступ до комерційної таємниці** — це письмова санкція власника підприємства або уповноваженої ним особи на ознайомлення або роботу з конкретними відомостями, що складають комерційну таємницю, співробітників підприємства та представників сторонніх організацій (під представниками сторонніх організацій слід розуміти співробітників органів державної влади і управління, аудиторських структур, українських та зарубіжних партнерів, клієнтів, контрагентів, конкурентів) [67].

➔ Допуск і доступ до комерційної таємниці являють собою дві різні юридичні категорії.

Допуск штатного співробітника підприємства до комерційної таємниці відрізняється від доступу тим, що останній, маючи допуск навіть найви-

щого рівня (“Комерційна таємниця — особливо важливо”) не може отримати доступ до інформації більш нижчого рівня секретності за власною ініціативою або за вказівкою безпосереднього начальника без письмової санкції на це керівника підприємства. Іншими словами, співробітник підприємства може отримати право на ознайомлення з будь-якою комерційною таємницею лише в тому випадку, якщо вона дійсно необхідна йому в зв’язку з виконанням ним службових обов’язків або для виконання окремого доручення керівника підприємства.

Рішення про надання доступу до конкретної комерційної таємниці і її матеріальних носіїв здійснюється у вигляді резолюції власника підприємства на документі, з яким знайомиться представник сторонньої організації, або шляхом оформлення окремого письмового розпорядження.

З метою попередження витоку відомостей, з якими були ознайомлені особи, що отримали доступ до комерційної таємниці, від цих осіб береться зобов’язання про її збереження.

Закон “Про інформацію” (далі — Закон) вводить поняття режиму доступу до інформації. Відповідно до ст. 28 Закону “Режим доступу до інформації — це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Держава здійснює контроль за режимом доступу до інформації. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержанні вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями”.

Стаття 30 Закону містить такі положення, пов’язані з режимом доступу до комерційної таємниці: “Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту”.

Питання юридичних гарантій збереження в таємниці конфіденційної інформації підприємства, до якої отримали доступ представники органів державного управління та ділових кіл, може бути вирішене наступними способами. [67]

**По-перше**, шляхом взяття у осіб, які ознайомились з відомостями, що складають комерційну таємницю підприємства, зобов’язання про

збереження ними в таємниці відомостей, які стали їм відомі. Таким юридичним документом може бути угода про конфіденційність, яка підписується особою, яка отримала доступ до інформації, що охороняється, і представником підприємства — власника комерційної таємниці (типовий зразок додається). Цей юридичний документ ґрунтується на інституті зобов'язального права України. Він широко використовується в світовій практиці підприємництва.

**По-друге**, шляхом передачі (при необхідності) представникові сторонньої організації копії документа, що містить комерційну таємницю, під розписку на оригіналі.

**По-третє**, шляхом передачі інших матеріальних носіїв комерційної таємниці під розписку про їх отримання та попередження в письмовій або усній формі про необхідність збереження в таємниці відомостей, які містяться в переданому документі або іншому матеріальному носії комерційної таємниці.

Порядок доступу до комерційної таємниці повинен визначитися “Положенням про дозвільну систему доступу співробітників підприємства і представників сторонніх організацій до відомостей, що складають, комерційну таємницю підприємства” (типовий зразок додається). При розробці дозвільної системи особливо ретельно слід відпрацювати положення, пов'язані з доступом до інформації, що охороняється, представників правоохоронних органів, органів державного управління, які здійснюють контроль за господарською діяльністю підприємств і згідно з законодавством мають право доступу до комерційної таємниці. В Положенні необхідно чітко визначити характер та обсяг інформації, з якою дозволяється або доцільно знайомити представників сторонніх організацій, а також посадових осіб підприємства, яким надається право вирішувати питання доступу до комерційної таємниці. [67]

На підприємстві доцільно створити систему накопичення інформації про осіб, які мали доступ до конкретних відомостей, що складають комерційну таємницю. Її основне призначення — забезпечення оперативності, виграш в часі у випадку виявлення факту витікання інформації, що захищається. Вона дозволить при службовому розгляді факту витікання інформації визначити, хто і коли мав до неї відношення.

Система може передбачати:

- ведення на кожного співробітника підприємства, що має доступ до комерційної таємниці, особового рахунку, в який заносяться дані про всі відомості, з якими він знайомився у процесі роботи;

- ведення картотеки на найбільш важливі для підприємства відомості, що складають комерційну таємницю, і хто конкретно знайомився з ними.

Як показує практика, така система виправдовує себе. Вона дає можливість швидко і з максимальним успіхом відреагувати на факт витоку інформації. Її також можна використовувати для проведення різноманітних аналітичних досліджень, пов'язаних зі станом захисту комерційної таємниці підприємства [67].

## **2.8. Правове регулювання порядку збереження комерційної таємниці при укладанні господарських договорів, веденні ділових переговорів. Перевірка ділових партнерів**

В умовах ринку є не лише виправданою, а й актуальною орієнтація юридичних та фізичних осіб на їх особливу відповідальність за передачу діловим партнерам або їх представникам економічних, науково-технічних та інших відомостей, що складають комерційну таємницю.

Колектив авторів розробки “Рекомендації по організації захисту комерційної таємниці в ІЕЗ ім. Є.О. Патона” (науковий керівник В.М. Серіков) вважає, що комерційною таємницею договору або контракту можуть бути [79]:

- сам факт укладання договору (контракту);
- предмет договору (контракту);
- умови їх виконання.

При укладанні **угод між суб'єктами господарювання в межах України** в тексті угоди доцільно відобразити:

- конкретні відомості, які складають комерційну таємницю угоди;
- види матеріальних носіїв, в яких містяться такі відомості (електронні носії, документи, вироби тощо);
- вимоги щодо захисту відомостей, що складають комерційну таємницю;
- права сторін на використання інформації, що містить комерційну таємницю;
- зобов'язання сторін про нерозголошення (неправомірну передачу) відомостей, що охороняються;
- санкції за розголошення, неправомірну передачу або використання відомостей, що складають комерційну таємницю.

В умовах договору доцільно обумовити можливість припинення його дії у випадку невиконання (неналежного виконання) вимог однією із сторін щодо захисту комерційної таємниці, а також звернення з позовом про відшкодування шкоди в судах. [67]

Перед укладанням угод з іноземною фірмою доцільно, із залученням юристів-міжнародників, досконало вивчити національне законодавство країни, з представником якої передбачається укласти угоду.

В угоді з іноземною фірмою доцільно передбачити:

- зобов'язання сторін вживати всі необхідні заходи для запобігання розголошенню комерційної таємниці;
- документи або дослідні зразки виробів повинні розглядатись сторонами як суворо конфіденційні;
- зобов'язання сторін вживати необхідні заходи для запобігання порушення прав користування цими документами або дослідними зразками виробів;
- зобов'язання сторін не передавати без попередньої згоди іншої сторони оригіналів документів або дослідних зразків виробів, або їх копій третім особам;
- зобов'язання сторін забезпечити ознайомлення з комерційною таємницею предмета та умов угоди лише суворо обмеженого кола своїх співробітників.

Практика свідчить, що при укладанні угод з іноземною фірмою не завжди застосовується термінологія, прийнята міжнародними правилами. З цієї причини між партнерами виникають конфліктні ситуації, які викликані тим, що одна із сторін по-своєму (нерідко навмисно) розуміла договірно-правові терміни та їх значення. Ці обставини призводять до невиконання або неналежного виконання договірних зобов'язань. [67]

- ◎ *У зв'язку з цим при укладенні зовнішньоекономічних угод необхідно керуватись положеннями “Міжнародних правил інтерпретації комерційних термінів” (Правила “Інкотермс”). Ці Правила дають вичерпний перелік не лише обов'язкових, а й факультативних умов угоди та регулюють весь комплекс взаємопов'язаних операцій щодо їх виконання.*

Певною мірою підвищити надійність та ефективність угод, їх правовий захист допоможе письмова угода сторін про збереження в таємниці певної інформації. Підписання аналогічних угод виправдане і у випадках, коли діловий партнер висловлює побажання про надання йому всієї кон-

фіденційної інформації для оцінки реального стану контрагента з метою прийняття рішення про укладення угоди. Однак до задоволення таких бажань слід ставитись дуже обережно.

Угода необхідна також на той випадок, коли в діловій бесіді один з партнерів повідомив іншому конфіденційні відомості, після чого останній, отримавши необхідну інформацію, відмовляється від укладення угоди, мотивуючи це різними обставинами, в тому числі і тим, що повідомлені конфіденційні відомості йому нібито були вже відомі. [67]

**Перевірка ділових партнерів.** Обережність у виборі партнерів, перевірка та переперевірка відомостей про них, особливо у випадках, коли викликає сумніви щирість пропозицій, що надійшли, та намірів, є обов'язковими елементами сучасної ділової практики.

На заході вже багато десятиріч функціонує галузь інформаційного бізнесу. Цим бізнесом займаються спеціальні фірми. Надання ними послуг інформаційного характеру про партнера, який цікавить, коштує в межах 500–2000 \$ за видачу бізнес-довідки.

Крім того, відомості про виробничу, науково-дослідну, фінансову, збутову та іншу діяльність фірм містяться в каталогах, рекламних проспектах, періодичних бюлетенях, прейскурантах, різноманітних довідкових виданнях, що видаються приватними спеціалізованими виданнями, спілками підприємців та торговельними палатами.

В Україні платні послуги, пов'язані з отриманням інформації про суб'єктів підприємницької діяльності України та зарубіжних країн, надають:

- Торговельно-промислова палата України;
- Українська федерація працівників недержавних служб безпеки (підрозділ “Інфоцентр”);
- Міжбанківська служба безпеки “СКИФ”;
- Фірма “Сакура”, яка надає інформацію про надійність та платоспроможність українських і зарубіжних партнерів, дає гарантії виконання партнерами умов комерційних угод.

Навести довідки про іноземного партнера можна у торговельного аташе посольства відповідної країни.

Перевірку партнера можна здійснити, використовуючи можливість самого підприємства (власна служба безпеки). Можна довідатись про адресу партнера, тривалість роботи на ринку, показники виробництва, балансові показники тощо.

Ще одним шляхам одержання інформації про ділового партнера є систематичне відслідковування і аналіз періодичних видань, таких як

“Бізнес”, “Галицькі контракти”, “Діловий вісник”, “Закон і бізнес” тощо. Доцільно на підприємстві вести картотеку на наявних та потенційних ділових партнерів, конкурентів на основі певного переліку необхідних відомостей (анкети) (зразок анкети додається).

## 2.9. Відповідальність за порушення законодавства про комерційну таємницю

Законодавство України, гарантуючи право підприємства на комерційну таємницю і її захист, певною мірою регулює і питання юридичної відповідальності за правопорушення в цій сфері.

За порушення законодавства про комерційну таємницю встановлені такі види відповідальності:

- кримінальна;
- цивільно-правова;
- адміністративна;
- дисциплінарна.

**Кримінальна відповідальність** встановлена за такі види злочинів:

- незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю — ст. 231 КК України;
- розголошення комерційної таємниці — ст. 232 КК України.

Ці два склади злочину віднесені прийнятим 5 квітня 2001 р. Кримінальним кодексом України до злочинів у сфері господарської діяльності.

*Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю (ст. 231).* Умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності, — карається штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк до п’яти років, або позбавленням волі на строк до трьох років.

Зі змісту даної статті видно, що вона містить два склади злочину:

- 1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю;
- 2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це завдало великої матеріальної шкоди суб’єкту підприємницької діяльності.

Суб'єктом незаконного використання відомостей, що містять комерційну таємницю, може бути особа, яка досягла 16-річного віку. При цьому не має значення, ким зібрані використовувані незаконно відомості, які становлять комерційну таємницю. [67]

*Розголошення комерційної таємниці (ст. 232).* Умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, — карається штрафом 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 виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

Порушувати кримінальні справи за фактами комерційного шпигунства або розголошення комерційної таємниці відповідно до ст. 4 Кримінального процесуального кодексу України мають право суд, прокуратура і орган дізнання на підставі заяви потерпілої особи. Відповідно до ст. 49 КПК України потерпілою особою (юридичною або фізичною) визнається та, у відношенні до якої порушене право на комерційну таємницю і якій завдано великого матеріального збитку. Ця ж особа на підставі ст. 50 КПК вважається і цивільним позивачем.

Розглядаючи питання про кримінальну відповідальність за порушення прав на комерційну таємницю, слід враховувати, що підприємство не може вимагати від державних органів гарантій на захист комерційної таємниці, якщо воно не набуло на це право згідно з встановленим законодавством України порядком [67] (див. Розділи 2.4, 2.5).

**Цивільно-правова відповідальність.** Цивільно-правовою санкцією є відшкодування збитків. Збитки, заподіяні внаслідок вчинення дій, визначених законодавством як неправомірне збирання, розголошення та використання комерційної таємниці, підлягають відшкодуванню за позовами заінтересованих осіб у порядку, визначеному Цивільним законодавством України (ст. 255 Господарського кодексу, ст. 24 Закону “Про захист від недобросовісної конкуренції”).

Підприємства постійно стикаються з різного роду ревізіями та перевітками окремих аспектів їх господарської та іншої діяльності представниками податкових, аудиторських, контрольно-ревізійних, правоохоронних та інших органів, які мають право доступу до інформації, що охороняється. У зв'язку з цим слід зазначити, що ЦК України передбачає відповідальність за шкоду, заподіяну незаконними діями державних

та громадських організацій, а також посадових осіб при виконання ними службових обов'язків в галузі адміністративного управління, і відшкодується вона на загальних підставах.

Органи державної влади зобов'язані охороняти від недобросовісного комерційного використання інформацію, яка є комерційною таємницею та створення якої потребує значних зусиль і яка надана їм з метою отримання встановленого законом дозволу на діяльність, пов'язану з фармацевтичними, сільськогосподарськими, хімічними продуктами, що містять нові хімічні сполуки. Ця інформація охороняється органами державної влади також від розголошення, крім випадків, коли розголошення необхідне для забезпечення захисту населення або не вжито заходів щодо її охорони від недобросовісного комерційного використання. Органи державної влади зобов'язані охороняти комерційну таємницю також в інших випадках, передбачених законом. (ст. 507 ЦК)

**Адміністративна відповідальність.** У сфері порушення прав на комерційну таємницю вона передбачена і регулюється двома нормативно-правовими актами: Кодексом про адміністративні правопорушення і Законом України “Про захист від недобросовісної конкуренції”.

Так, ст. 1643 Кодексу про адміністративні правопорушення встановлює, що отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця становить адміністративне правопорушення і тягне за собою адміністративне стягнення у вигляді накладення штрафу від 5 до 9 неоподатковуваних мінімумів доходів громадян.

Закон “Про захист від недобросовісної конкуренції” передбачає адміністративну відповідальність за неправомірне збирання комерційної таємниці (ст. 16), розголошення комерційної таємниці (ст. 17), схилення до розголошення комерційної таємниці (ст. 18), неправомірне використання комерційної таємниці (ст. 19). За вказані порушення настає адміністративна відповідальність у вигляді штрафів, які накладаються Антимонопольним комітетом України.

Суб'єктами цих правопорушень є як юридичні, так і фізичні особи. [67]

**Дисциплінарна відповідальність.** Відповідно до Кодексу законів про працю України стосовно штатних співробітників підприємства, що пропустили порушення встановлених на підприємстві режиму, порядку і правил збереження комерційної таємниці, можуть застосовуватись такі види стягнень:

- догана;
- звільнення;

- переведення на іншу роботу, не пов'язану з комерційною таємницею;
- позбавлення премій, передбачених системою оплати праці;
- позбавлення винагород за результатами роботи за рік;
- зміна часу надання чергової відпустки.

Підстави застосування зазначених дисциплінарних стягнень відповідно до ст. 147 КЗпП України повинні бути чітко передбачені “Положенням про комерційну таємницю підприємства і правила її збереження” (типовий зразок додається). [67]

### **Питання для самоконтролю**

1. Законодавство України про захист підприємництва.
2. Поняття та ознаки комерційної таємниці.
3. Правове регулювання захисту комерційної таємниці за кордоном.
4. Проблеми правового захисту комерційної таємниці в Україні.
5. Об'єкти та суб'єкти права власності на комерційну таємницю.
6. Елементи та складові системи правового захисту комерційної таємниці підприємства.
7. Правові документи, що закріплюють права підприємства на комерційну таємницю.
8. Визначення відомостей, які складають комерційну таємницю підприємства.
9. Інсайдерська угода.
10. Угода про нерозголошення комерційної і виробничої таємниці.
11. Збереження комерційної таємниці при укладанні господарських договорів.
12. Відповідальність за збереження комерційної таємниці в засновницьких документах.
13. Відповідальність персоналу за збереження комерційної таємниці в документах підприємства.
14. Відповідальність за викрадення комерційної інформації в Україні.
15. Система доступу та допуску до комерційної таємниці підприємства.

## **Розділ 3. ЕКОНОМІЧНА РОЗВІДКА (економічне шпигунство)**

### **3.1. Економічна розвідка як фактор у конкурентній боротьбі**

**Місце і роль економічної розвідки в конкурентній боротьбі.** Русійським механізмом сучасного економічного прогресу є конкуренція. Саме вона примушує всіх суб'єктів економічної діяльності слідувати законам підвищення ефективності виробництва. Економічний прогрес суспільства дає переваги тим, хто пропонує продукцію з меншими витратами, кращої якості. Прогрес вимагає, щоб сферу економічної діяльності покинули ті, хто виробляє гіршу за якістю продукцію з великими витратами. Ці проблеми в конкуренції розв'язуються жорстким механізмом: одна частина одержує додаткові вигоди, інша частина розоряється.

Нерівність доходів, додаткові вигоди і є тією основою, на якій виникла економічна таємниця, тобто інформація про способи отримання додаткових вигод. Якщо поява додаткових вигод породила таємницю; то остання породила прагнення у частини людей володіти нею, так само, як у власників таємниці — зберегти і захистити її: ФБР США нині веде 800 справ економічного шпигунства [70].

- ⊙ *Загальновідомо, що всі види розвідки оцінюються іншою стороною як шпигунство.*

Розкрадання таємниці, тобто економічна розвідка, сягає коренями в сиву давнину. Історії відомо, наприклад, що араби близько чотирьохсот років полювали за секретами “грецького вогню”. Секрети китайського фарфору і шовку свого часу були також важливими об'єктами економічної розвідки. Як відомо, северський фарфор у вісімнадцятому столітті став не чим іншим, як результатом застосування викрадених секретів китай-

ської імператорської фарфорової мануфактури. Так само севрські фарфорові секрети були викрадені у французів англійцями.

З історії також відомо, що шпигунство чималу роль зіграло в становленні англійської сталеливарної промисловості. Англійцям за допомогою шпигунства вдалося зібрати секрети сталеливарної справи, які свого часу мали в своєму розпорядженні Бельгія, Німеччина, Італія, Іспанія [31]. .



В Москві і сьогодні працює фабрика “Сакко і Ванцетті”, що виробляє олівці. Як повідомляли радянські газети в 1926 р., вона була відкрита до травневих святкувань. Але газети практично нічого не писали про те, як вона була побудована. Свого часу молодий американський підприємець А. Хаммер, будучи знайомим з Ленінін і допомагаючи Радянському Союзу відновити зруйновану війною економіку, гуляючи Московою, звернув увагу на те, що в магазинах продаються олівці за ціною, в багато разів вищою, ніж у Сполучених Штатах Америки. Бажання отримати додаткові вигоди привело до підписання контракту між А.Хаммером і Радянським урядом про будівництво олівцевої фабрики. СРСР не мав ні технології виробництва олівців, ні устаткування. Між іншим А. Хаммер також не мав ні того, ні іншого. Проте все що було необхідне для виробництва олівців було в Німеччині, яка зовсім не бажала ділитися технологічними секретами з третіми особами. А. Хаммер отримав секрети разом з німецьким інженером Р. Бейером, запропонувавши останньому надзвичайно високу заробітну платню і преміальні в декілька центів з кожного виробленого олівця. Решта проблем організації виробництва олівців для А. Хаммера не становила секретів [22].

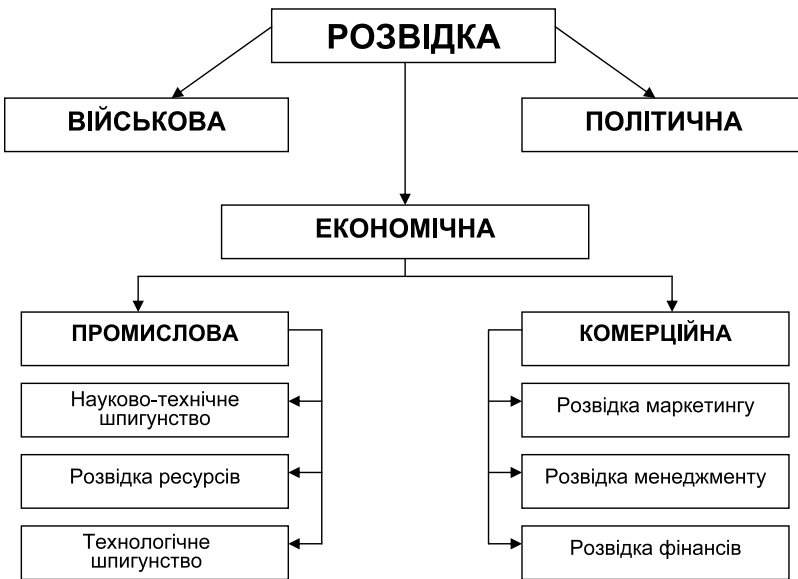
Особливо широке розповсюдження шпигунство отримало в галузі військової економіки у зв'язку з виробництвом і продажами новітніх озброєнь. Яскраві приклади такого шпигунства спостерігалися в процесі виробництва кулемета “Максим”, коли грек Базіль Захаров вів підривному шпигунську роботу проти інженера-винахідника Максима.

Ці приклади можна продовжувати до нескінченності. Вони лише підтверджують сказане раніше: економічне шпигунство супроводжує конкуренцію, в яких би сферах і формах вона не здійснювалася.

Говорячи про місце і роль економічного шпигунства в конкурентній боротьбі, не можна не зупинитися ще на одній стороні проблеми — кількісного вимірювання вигод і втрат від шпигунства. За підрахунками американських економістів, до середини 80-х рр. корпорації США зазнавали збитків приблизно в обсязі 20 млрд доларів [31], що складало близько 1/5 частину нерозподіленого прибутку корпорацій. Але якщо для одних корпорацій це втрати, то для інших — вигоди, і чималі. Якщо на традиційних технологіях бізнесмен може отримати 10–20% прибутку, на

новітніх в період розвитку продукту — до 100–200%, то в окремих випадках інвестиції в шпигунство приносять до 1000% прибутку. Проте, враховуючи особливий ризик в цій галузі, не можна не попередити, що нерідко трапляється і чистий збиток [70].

**Класифікація економічної розвідки.** В популярній літературі про розвідку поширені такі поняття, як економічна розвідка, промислове шпигунство, комерційна розвідка, військова розвідка, політична розвідка, космічна розвідка і т.ін. Ми назвали різні види розвідки, які з одного боку, зв'язані між собою, а з іншого — несуть в собі понятійні відмінності. Тому на первинному рівні виділяються економічна, військова і політична розвідки. Кожна з них, у свою чергу, ділиться на складові частини (рис. 3) [46].



*Рис. 3. Структура розвідки*

Економічна розвідка найбільш складна за своєю структурою. Нерідко економічну і промислову розвідку ставлять поряд або ж намагаються показати як незалежні одна від одної. Необхідно мати на увазі, що економічна розвідка цікавиться всією інформацією, що має життєво важливе значення і забезпечує переваги конкуренту, і яка стосується таких сторін його господарської діяльності:

- ресурсів, наявних у розпорядженні;
- процесів виробництва економічних благ, тобто технологій;
- процесів розподілу і обігу;
- процесів споживання;
- процесів моделювання виробництва і економічних явищ;
- дослідницьких процесів.

⊙ *Деякі автори в рамках економічної розвідки виділяють промислову і комерційну розвідку [22, 31].*

**Промислова** розвідка охоплює наукові дослідження, технології, організацію виробничих процесів, розвідку ресурсів.

Тут чітко визначилися свої напрями. Першим і найважливішим з них можна назвати науково-технічну розвідку. В її рамках формуються свої підсистеми: розвідка в галузі фундаментальних наук і в дослідно-конструкторських роботах. Якщо перший напрям визначає принципові напрями рішення окремих проблем, то другий забезпечує реальні підходи до отримання можливих вигод за допомогою виробництва новітніх комп'ютерів, літаків, автомобілів, холодильників і т.ін.

Відносно самостійним напрямом промислової розвідки є технологічне шпигунство. Нерідко розгортаються справді драматичні баталії, коли готові до застосування технології раптом опиняються в руках конкурентів [46].

Особливе місце в галузі промислового шпигунства займає розвідка ресурсів. Безумовно, ресурси завжди є тільки потенційним джерелом високих доходів. Але вони можуть відігравати важливу роль в умовах і високо-, і низькотехнологічних виробництв.

➔ **Комерційне** шпигунство направлене на дослідження витрат, менеджменту, маркетингу.

В рамках останнього особлива увага надається розробці конкурентом продукту, організації реклами, продажів, ринків і т.ін. Також можна виділити і такий важливий напрям, який стосується фінансів підприємства, регіону, галузі, країни.

Відзначена класифікація вельми умовна і, неважко помітити, спирається на функціональні особливості об'єкта розвідки, тобто конкурента.

Класифікація розвідки може визначатися і об'єктом шпигунства або суб'єктом економічних і правових відносин. Економічна розвідка організовується проти окремих громадян, тобто фізичних осіб; проти окремих

фірм, підприємств і організацій або юридичних осіб і, нарешті, проти держави. Всі ці види розвідки взаємозв'язані між собою. Але в даному випадку нас цікавить в більшій мірі економічна розвідка проти конкурентів-підприємств, тобто юридичних осіб.

**Об'єкти економічної розвідки.** Якщо ваш конкурент солідний і має науково-дослідні і дослідно-конструкторські підрозділи, великий інтерес для вас повинні представляти фундаментальні і прикладні розробки продукту і технологій.

Крім того, відносно продукту або послуги конкурента для вас цікавими будуть такі показники, як обсяги і тенденції розвитку виробництва, майбутні зміни в номенклатурі продукції, технології і устаткуванні, якості і ефективності виробів.

В галузі маркетингу конкурента особливий інтерес має його ринок (структура, сегменти, місткість, тенденції розвитку, як складаються відносини вашого конкурента із споживачами, організація реклами, упаковка, доставка і продажі продукту, чисельність і розміщення торгових агентів, канали, політика і методи збуту). Особлива увага при дослідженні маркетингової діяльності конкурента повинна надаватися цінovій політиці [46].

В галузі менеджменту, вживаного вашим конкурентом, особливий інтерес становить структура організації, її комунікації, їх ефективність, надійність; коло осіб, що приймають ключові рішення, їх філософія, особливості і склад характеру, захоплення, хобі, заняття спортом; морально-етичний стан колективу. Всі ці особливості вашого суперника можуть бути використані в конкурентній боротьбі з ним.

В галузі кадрів повинні представляти інтерес всі подробиці особистого життя всіх носіїв інформації, якими можуть бути не тільки особи, що приймають ключові рішення. Тут мають значення їх здорові смаки, звички — явні та таємні вади, склад сім'ї, звички членів сім'ї, їх спосіб життя, близькі друзі носіїв інформації та їх спосіб життя.

Важливе значення має дослідження інфраструктури бізнесу вашого конкурента. Тут з'ясовується його розташування, під'їзні шляхи, системи зовнішнього зв'язку, водо- і енергопостачання, зв'язки з постачальниками, склади, устаткування, виробничі особливості і т.ін. Ці відомості можуть бути також ефективно використані в конкурентній боротьбі.

Особливе місце і найважливіше значення серед об'єктів економічної розвідки займають фінанси підприємства, організації. В них концентруються всі найважливіші особливості роботи підприємства. Крім того, в них відображається стан взаємовідносин підприємства з державою, спо-

живачами, постачальниками. Слід мати на увазі те, що фінансова звітність регламентується міжнародними і національними стандартами, забезпечуються інтереси зовнішніх користувачів інформації. Зі всієї сукупності фінансових показників підприємства особливий інтерес становить ефективність функціонування капіталу, прибутковість і рентабельність, стан ліквідності і платоспроможності, використання позикових засобів тощо. Особливе місце серед фінансових показників займають грошові обороти і витрати.

**Принципи економічної розвідки.** Принципи і засоби, вживані в своїй діяльності економічною розвідкою, визначаються завданням, що необхідно вирішити.

- ➔ В **завданні** можна виділити дві укрупнені складові частини [40]:
1. Добування необхідної інформації про конкурента.
  2. Охорона власної інформації від розвідки конкурентів.

Вся розвідувальна діяльність для вирішення цих складових загального завдання пов'язана із збором, обробкою, узагальненням і захистом інформації, вона повинна спиратися на ряд принципів, які забезпечують її ефективне функціонування.

Першим і найважливішим принципом організації будь-якої розвідувальної діяльності, у тому числі і економічної, є **неупередженість у відборі, систематизації, обробці і передачі адресату здобутої інформації**.

- ⊙ *Історії відомі багато трагічних наслідків упередженого відношення до даних розвідки.*

Трагічні наслідки упередженого відношення до даних розвідки загальновідомі. Як підкреслює А. Даллес, подібної помилки припустилися американці в оцінці результатів розвідки про намір японців атакувати Пірл-Харбор [40], а також коли для них повною несподіванкою виявився перший в світі штучний супутник землі, запущений Радянським Союзом. Нині принцип **неупередженості** в розвідувальній роботі є одним з визначальних.

Наступним принципом є **системність інформації**, здобутої економічною розвідкою. На основі цього принципу забезпечується достовірність інформації, а отже якість і ефективність розвідки.

Якщо ви отримали інформацію про добрий фінансовий стан суперника, то це ще зовсім не означає, що у нього міцні конкурентні позиції.

Цілком можливо, що це фінансове здоров'я базується на застарілій технології, коли життєвий цикл основних товарів і технологій фірми минув етап зрілості і переходить в спад, а фірма не інвестує капітали в оновлення виробництва. Вихід на ринок фірми з новітніми технологіями може швидко відкинути цього конкурента назад.

- ⊙ *Дані економічної розвідки повинні бути взаємопов'язаними по складових підсистемах. Тільки в цьому випадку можна зробити безпомилкові висновки. Фінансові показники повинні підтверджуватися маркетинговими, а маркетингові — у свою чергу — виробничими, технологічними.*

Третій принцип — **конфіденційність**. Економічна розвідка, разом з відкритою, має справу і з секретною інформацією. У межах цього принципу формуються свої правила. Перш за все, добування будь-якої інформації з напівлегальних або нелегальних джерел повинно носити закритий характер. Річ у тому, що законодавства деяких країн забороняють збирати інформацію на фізичних осіб. Наприклад, частина 4 ст. 23 Закону України “Про інформацію” забороняє збір відомостей про особу без її попередньої згоди за винятком випадків, передбачених законом.

- ⊙ *Конфіденційність економічної розвідки означає, що добування інформації у конкурента повинне залишатися для нього таємницею.*

Наступне правило зводиться до необхідності охорони життєво важливих секретів фірми.

- ➔ З приведених вище внутрішніх правил конфіденційності витікає наступне. Воно свідчить: — **не робити таємниці з того, що відомо всім і кожному і абсолютно очевидно для друга і ворога [46].**

Зайва секретність для корпорації заважатиме навіть рекламній роботі. Вона гальмуватиме нормальні технологічні процеси, науково-дослідну і конструкторську роботу [40].

## 3.2. Організація та ефективність економічної розвідки

**Інформація як основний фактор ефективної діяльності підприємства в умовах ринкової економіки.** До початку 90-х рр. минулого століття (радянський період) вітчизняні підприємства, зокрема підприємства АПК, практично не відчували ніяких ризиків у своїй діяльності, оскільки вони знаходились в державній власності та були пов'язані договорами-зобов'язаннями держзамовлення. В свою чергу, державні інтереси в галузі економіки жорстко захищались правоохоронними органами та спецслужбами.

Тепер ситуація кардинально змінилась. Будь-який господарюючий суб'єкт, незалежно від обсягу його робочих активів, знаходиться в оточенні різноманітних ризиків, які здатні миттєво знищити фінансові та матеріальні ресурси. Водночас державні структури, що мають стояти на захисті підприємництва, фактично не діють.

- ➔ Якщо спробувати провести аналіз причин провалу більшості великих і малих підприємств України, зокрема й підприємств АПК, то можна дійти висновку: основна причина невдач — це невміння, не усвідомлення важливості, а також іноді не бажання займатися збиранням, обробленням та аналізом інформації стосовно оточуючого середовища підприємства.

Окрім того можна відзначити недостатній рівень наукових розробок в даній галузі. Так, в Україні цим питанням займається лише декілька фахівців, серед яких А.А. Чернявський, Г.А. Андрощук, П.П. Крайнів, Г.К. Нікіфоров. Дещо краща ситуація в Росії, де останнім часом спостерігається зростання кількості наукових та практичних розробок в галузі інформаційно-аналітичної роботи на підприємстві. На жаль, лише зараз на цю проблему почали звертати увагу деякі українські підприємці, але мало хто з них може визначити тип необхідної для підприємства інформації, кваліфіковано організувати її пошук, уникнути ефекту дезінформації, уміло використати отриману інформацію при прийнятті рішень та для організації поточного контролю фінансово-господарської діяльності.

- ⊙ *В умовах ринкової економіки підприємство не може ефективно працювати без глибокого розуміння її рушійних сил, не маючи найновішої інформації про стан ринку, на якому воно працює. При цьому необхідно враховувати можливості підприємства, а також інтер-*

*еси інших учасників ринку та окремих осіб, які можуть не завжди керуватись лише вимогами ринку.*

Виходячи з викладеного, стає зрозумілою необхідність створення на підприємстві такого структурного підрозділу, на який будуть покладені функції інформаційного центра із завданнями збирання, обробки та аналізу інформації, яка буде забезпечувати прийняття керівництвом важених управлінських рішень. На сучасному українському підприємстві таким підрозділом може бути підрозділ (служба) економічної розвідки підприємства.

Основними цілями даного підрозділу можуть бути:

1. Вчасне забезпечення керівництва надійною та повною інформацією про зовнішнє середовище підприємства. Виявлення факторів ризику для підприємства.
2. Організація максимально ефективної інформаційної роботи, що виключатиме дублювання функцій різними підрозділами.
3. Відпрацювання короткострокових та довгострокових прогнозів впливу зовнішнього середовища на господарську діяльність агропромислового підприємства. Розроблення рекомендацій щодо локалізації та нейтралізації виявлених ризиків.
4. Підсилення сприятливих та зниження несприятливих впливів зовнішнього середовища на господарську діяльність підприємства
5. Пошук нових ідей, технологічних розробок, методів роботи тощо, які можуть бути впроваджені на підприємстві та дадуть можливість досягнути переваг в конкуренції.

⊙ *Для продуктивного ведення господарської діяльності керівництву підприємства необхідно приймати рішення різного рівня, інформаційну підтримку яких забезпечує система економічної розвідки.*

Управління великою компанією може передбачати такі рівні: управління всередині компанії, управління діяльністю компанії на внутрішньому ринку країни, управління діяльністю на міжнародному ринку, управління поточною діяльністю та управління стратегічним розвитком. Але як мінімум будь-яке підприємство включає управління поточною діяльністю та управління стратегічним розвитком.

Характер інформації для кожного рівня рішень, що приймаються, буде значно відрізнятись. Відповідно роботу підрозділу економічної розвідки підприємства доцільно розділити хоча б на дві складові.

- ➔ **Стратегічна складова** економічної розвідки займається збиранням та аналізом стратегічної інформації про глобальні процеси в економіці, політиці, технології тощо, які можуть вплинути на розвиток підприємства.

Основними принципами планування розвідувальної діяльності в економіці є спочатку визначення цілей проведення розвідування, потім визначаються потреби в інформації, і вже після цього визначаються джерела отримання необхідної інформації.

Ціллю стратегічного рівня прийняття рішень (розширення виробництва, диверсифікація, перехід в іншу галузь, впровадження нового продукту тощо) є визначення напрямлення подальшого розвитку підприємства. Такі рішення визначають потребу зорієнтуватись на ринку та проаналізувати перспективи його розвитку.

На жаль, в нашій країні керівники підприємств дуже мало уваги приділяють стратегічному управлінню, і це призводить до того, що понад 90% робочого часу витрачається на розв'язання несподіваних проблем, ускладнень, залагодження зривів справ.

- ➔ **Оперативно-тактична складова** економічної розвідки займається збиранням та аналізом оперативно-тактичної інформації для прийняття керівництвом обґрунтованих рішень стосовно поточних проблем підприємства.

Ціллю оперативно-тактичного рівня прийняття рішень (реконструкція цехів, закупівля нового обладнання, навчання працівників для випуску нової продукції чи виконання нового виду робіт) при видимому направленні подальшого розвитку є вибір оптимального шляху його досягнення та мінімізація витрат при цьому.

Цілі розвідувальної діяльності жорстко структуровані. Кожна ціль визначається ціллю вищого порядку, залишаючись при цьому незалежною за характером своїх потреб і джерелами інформації. Так, після стратегічної цілі — визначення напрямлення — визначається оперативно-тактична ціль — вибір найкращого шляху розвитку та просування по ньому.

Попереднє планування розвідувальної діяльності необхідне також, щоб в майбутньому не відбулось перевантаження інформацією, що накопичується. Кожне підприємство має свою специфіку, тому певна інформація для одного підприємства є життєво важливою, для іншого — абсолютно непотрібною.

Особливо важливо, щоб на підприємстві існував замкнутий цикл підготовки матеріалів, починаючи від визначення показників збору інформації, її класифікації, автоматизованої обробки і закінчуючи її аналізом, розробленням прогнозів та практичних рекомендацій. Такий розвідувальний цикл можна поділити на складові:

- планування та направлення на виконання — складання завдання розвідки, підготовка плану збирання інформації, віддавання наказу виконавцям завдання та контроль за ходом виконання;
- збирання — добування інформації та передача її спеціалістам для обробки;
- оброблення — початкове оброблення зібраної інформації, надання їй визначеної форми (переклад, переформатування комп'ютерних даних);
- оцінка — перетворення зібраної інформації в дані розвідки (узгалянення, аналіз та синтез, всебічна оцінка);
- висновки — створення прогнозів, вироблення практичних рекомендацій, моделювання ситуацій;
- розповсюдження — передача даних розвідки замовникам.

Але необхідна інформація може надходити в значних кількостях. Тому для спрощення доступу та ефективної роботи з нею необхідно формувати комп'ютерні інформаційні бази даних для збереження та обробки наявної розвідувальної інформації. Вигляд і форма таких інформаційних баз даних може розроблятися на кожному підприємстві самостійно з урахуванням його вимог та особливостей (програмістами підприємства або на замовлення сторонньою організацією).

Особливу увагу слід приділяти вивченню доступних джерел інформації та отриманню необхідних даних із офіційних джерел інформації. З одного боку, це економічно вигідно, оскільки потребує значно менших витрат коштів, ніж застосування напівлегальних та нелегальних методів вивідання даних, з іншого боку, саме легальні джерела дають близько 95% всієї необхідної інформації (навіть у військовій справі).

Також необхідно з'ясувати, хто із співробітників на підприємстві має інформаційні зв'язки в державних органах управління, міністерствах, відомствах, банківських структурах, правоохоронних органах, засобах масової інформації тощо. Аналіз таких зв'язків проводиться з метою врахування можливостей їх ефективного використання.

- ◎ *Таким чином стає зрозумілим, що робота з пошуку необхідної для підприємства інформації не повинна покладатись лише на праців-*

*ників підрозділу економічної розвідки. До такої роботи повинні долучатись також (відповідно до можливостей) працівники інших підрозділів. Але необхідно зазначити, що така робота повинна всіляко заохочуватись, що дасть змогу підвищити якість інформації та швидкість її надходження.*

Оскільки для роботи керівникам підприємства потрібна інформація різного характеру (загальнополітична, економічна, технологічна, банківська, ринкова, галузева тощо), буде доцільним, окрім підписки на спеціалізовані періодичні видання, встановлення відділом економічної розвідки контактів зі спеціалізованими фірмами, які накопичують та опрацьовують інформацію за певною тематикою.

В цілому про ефективність розвідки можна судити не за чисельністю співробітників, кількістю відділів, технічною оснащеністю, а за трьома показниками:

1. Своєчасність одержуваної інформації.
2. Точність інформації.
3. Адекватність наступним подіям.

Ефективність будь-якої діяльності визначається за схемою “витрати–ефект”, так, для розвідувальної діяльності можна назвати чотири види ефекту:

- прибуток;
- економія ресурсів;
- утримання ринкових позицій в кризових ситуаціях (мінімальні збитки);
- попередження матеріальної та моральної шкоди.

Оскільки на підприємстві більша частина інформації, що використовується, не є секретною, то створення комп'ютерної локальної мережі, яка пов'язуватиме різні підрозділи, вирішить проблему вчасного розповсюдження відкритих інформаційних документів.

Інформація оперативно-тактичного та стратегічного характеру повинна надаватись посадовим особам, які займаються плануванням та несуть відповідальність за прийняття рішень, відповідно до наявного у них допуску до конфіденційної інформації.

- ◎ Система економічної розвідки повинна не лише забезпечувати необхідною інформацією всіх зацікавлених осіб, а й одночасно забезпечувати контроль за її цільовим використанням. До ознайомлення з конфіденційними документами співробітники підприємства мо-

*жуть допускатись лише після перевірки на лояльність та при наявності виробничої необхідності.*

В наш час, коли роль інформації як виробничого ресурсу постійно зростає, не можна залишати сферу інформаційного забезпечення управління підприємницькою діяльністю без достатньої уваги. Дане питання потребує нагальних теоретичних та практичних розробок. Робота системи економічної розвідки підприємства дасть певний мультиплікаційний ефект, поєднуючи інтереси забезпечення економічної безпеки підприємства з розв'язанням питань маркетингу, оскільки на її основі виробляється ефективна економічна політика підприємства.

### **Схема організації економічної розвідки у великих корпораціях.**

Більшість великих корпорацій, як правило, є олігополістами і мають на ринку 2–4 подібних собі конкуренти. Маючи великі капіталовкладення і могутню виробничу інфраструктуру, вони не можуть піти в ринкову нішу як, наприклад, “Кока-Кола” чи “Жиллет”, і приречені долею на вічну конкурентну боротьбу між собою. Тому усі вони мають добре розгалужені мережі економічної розвідки і служби безпеки. На початку 80-х рр. корпорації США зазнавали збитків від економічного шпигунства близько 20 млрд доларів щорічно. За деякими даним, у той же час великі корпорації на організацію розвідки витрачали близько 1,5 млрд доларів, тобто на кожен долар витрат по добуванню секретної інформації отримано понад 13 доларів доходу [22, 31]. В традиційному бізнесі хорошим вважається прибуток у розмірі 15–25 центів, у венчурному підприємстві — 1–2 долари прибутку на долар витрат. Як бачимо, сфера діяльності розвідки настільки вигідна, що не може залишатися поза увагою великих корпорацій. Деякі корпорації мають тисячі і навіть десятки тисяч агентів економічної розвідки і служби безпеки [31]. Ефективність розвідки багато в чому залежить від організації.

Розвідувальна служба великої корпорації найчастіше відокремлена у формі холдингової компанії, штаб-квартира якої також знаходиться подалі від очей співробітників компанії. Компанії з річними оборотами у десятки мільярдів доларів мають ринки усередині країни базування й у десятках закордонних держав. Тому усі спецслужби розвідувальної організації корпорації поділяються на дві групи [46]:

- 1) спецслужби країни базування;
- 2) спецслужби в закордонних країнах.

Спецслужби в країні базування, як і закордонні, ведуть роботу за різними напрямками: зв'язок з державними розвідувальними служба-

ми, лобізм у державних і місцевих законодавчих та виконавчих органах влади, безпосередня розвідка конкурента. Передусім розвідка корпорації намагається встановити зв'язок з державною розвідувальною службою. Ці зв'язки встановлюються на основі особистих, коли в спецслужбі корпорацій приймаються на роботу розвідники, що ідуть у відставку, з державних служб. Державні спецслужби можуть передавати “побічну” продукцію розвідки корпораціям, що не представляє цінності з погляду військово-політичних цілей і яка має важливе значення для фірми.

Лобізм формується за допомогою забезпечення політичної кар’єри відданих фірмі кандидатів у депутати парламенту і місцевих органів влади. Функцію лобіста може виконувати і радник парламентарія, урядового функціонера [49, 64].

Безпосередня розвідка конкурента в організаційному плані здійснюється через діяльність філій розвідувальної служби корпорації, розміщених по окремих регіонах країни базування. При цьому вони можуть спеціалізуватися за окремими напрямками економічної розвідки: фінансової, технологічної, кадрової і т.ін.

Поряд з філіями центральної штаб-квартири спецслужби корпорації у її системі можуть бути і відносно самостійні агентства, що також працюють за багатьма напрямками. На відміну від філій агентства можуть виконувати і замовлення на секретну інформацію ззовні, хоча всю основну діяльність, зрозуміло, підпорядковують інтересам корпорації.

Як штаб-квартира розвідувальної служби, так і її агентства мають самостійних агентів і резидентів з відповідним підпорядкуванням. Цих розвідників, що виконують різноманітні самостійні завдання, класифікував ще 400 років до н.е. китайський полководець Сунь-Цзи, і ця класифікація, за словами А. Даллеса, залишається актуальною до наших днів [40, 89]. Сунь-Цзи виокремив **п’ять категорій розвідників**.

**“Місцеві розвідники”** — сучасною мовою — це агенти з рядових працівників підприємства, організації конкурента, що мають доступ до інформації. **“Внутрішні”** розвідники, названі Сунь-Цзи, також є завербованими агентами, але з управлінського персоналу об’єкта розвідки. Місцеві і внутрішні розвідники класифікуються тепер, як агенти на місці об’єкта. Розвідники, **“що повертаються”**, за класифікацією Сунь-Цзи, — це, як правило, розкриті службою безпеки і переверовані агенти супротивника (конкурента). Їх називають *“подвійними агентами”*. Вони використовуються для дезінформації конкуруючої сторони. **“Розвідники смерті”** — сучасною мовою *“агенти, що не повертаються”*, доставляють помилкову інформацію супротивнику, і можуть загинути. В економічній розвідці не

використовуються. Нарешті, “розвідники життя” чи “проникаючі агенти” у сучасному понятті. Вони проникають на об’єкт, добувають необхідну інформацію і повертаються з нею в штаб-квартиру. Цей вид агентів також використовується в економічному шпигунстві. До цих п’яти груп агентів, а точніше, замість “агенти, що не повертаються” варто ввести нову категорію: агента-експерта, що, обробляючи легальні матеріали, відшукує необхідну економічну інформацію про конкурента.



Наприклад, міжгалузеві баланси, що готував Держкомстат СРСР, були таємницею і публікувалися в статистичних збірниках з розривом приблизно в п’ятнадцять — двадцять років. Президент компанії “Интеллидженд Десижи Системс” з Берклі (США) Д. Стайнберг міжгалузевий баланс СРСР 1988 р. реконструював за два тижні (правда, на баланси за 1970–1987 рр. потрібно було по 6–7 місяців [46]). Як відомо, у бюджетах СРСР, які публікувалися, військові витрати визначалися в розмірі 20 млрд руб. Д. Стайнберг встановив, що в 1987 р. військові витрати СРСР склали 119,5 млрд руб. у поточних цінах. За словами М.С.Горбачова питома вага військових витрат складала 18% національного доходу країни, що рівнозначно 114 млрд руб. Як бачимо, дослідження експерта виявилося дуже точним [46].

Особливе місце в організації розвідувальної роботи корпорації займає створення різного роду благодійних фондів, товариств. Особливу роль фонди і товариства відіграють у забезпеченні лобізму [78, 91].

Наступною складовою частиною організації економічної розвідки є її закордонна мережа. В першу чергу вона розгортається в країнах базування філій корпорації — ринків капіталу, сировини і збуту продукції. Потім — у країнах, де є потенційні ринки, на які планується вихід корпорації. Розгортання розвідувальної мережі здійснюється також за декількома напрямками.

Передусім, організуються філантропічні фонди, як правило, у країнах, які переживають серйозні соціально-політичні і структурні економічні кризи. Внутрішні ринки цих країн потенційно-перспективні, тут дешева робоча сила і гострий нестаток закордонних інвестицій. Тому благодійні фонди дають прекрасну можливість для вербування агентів зі збирання необхідної інформації і відповідного їх винагородження, забезпечення лобізму [46].

Для забезпечення більш солідних внутрішніх агентів створюються різного роду дорадчі комітети, комітети підтримки окремих акцій. Вони організуються в країнах з різним рівнем розвитку економіки для забезпечення контактів з банківськими, промисловими і політичними колами

країни, що становить інтерес для корпорації. Зрозуміло, вони їх притягують високими гонорарами, за що одержують “делікатну” інформацію. Різного роду комітети створюють “Форд моторз компани”, “Дженерал моторз” та ін. Останнім створений в 1974 р. “Європейський дорадчий комітет”, бюджет якого дорівнював бюджету державної розвідувальної служби Франції [31].

Завдання лобі зводиться до створення сприятливої атмосфери в зовнішньому середовищі корпорації і нейтралізації впливу несприятливих факторів цього середовища. Тому лобізм розгортається в політичній, економічній, соціальній сферах, у засобах масової інформації.

Важливу роль в організації розвідувальної роботи корпорацій за кордоном відіграють її філії. Переважна більшість співробітників, у тому числі й серед управлінського персоналу, є громадянами країни базування філії. Оскільки їх добробут забезпечується закордонною фірмою, їхні економічні інтереси мимоволі схиляються на користь закордонної корпорації.

Нарешті, за кордоном можуть працювати самостійні агентства й агенти. Агентства займаються вербуванням “місцевих” і “внутрішніх” агентів. Проникаючі агенти найчастіше вербуються з “місцевих” і “внутрішніх” агентів. Підготовка “свого” проникаючого агента — справа дорога і складна, він готується роками зі студентської лави.

Схема організації розвідки великих комерційних корпорацій подана на рис. 4 [46].

Не виключається, що розвідувальні великих корпорацій можуть використовувати послуги незалежних розвідувальних агентств. Є багато таких фірм, серед яких найбільш відомі “Джорж Уокнехт”, “Континентл телефон енд сеїплай компани”, “Спайз інкорпорейтед” та ін. Ці незалежні агентства нараховують в окремих випадках тисячі агентів, їх послугами користаються сотні і тисячі корпорацій [46].

**Організація розвідки в середніх фірмах.** Зрозуміло, середні компанії не можуть дозволити собі утримання могутньої і широкої мережі економічної розвідки, оскільки не володіють відповідними фінансовими ресурсами. Разом з тим у них достатньо засобів, щоб утримувати хоча і невелику, але спеціалізовану службу розвідки [60].

- ➔ Принципові особливості організації розвідки полягають у наступному:
1. Організація розвідувальної роботи ведеться вузьким колом людей (у межах кількох чоловік).
  2. До розвідувальної роботи на конфіденційній основі залучаються кваліфіковані фахівці фірми.

3. Більшою мірою використовуються послуги незалежних розвідувальних агентств і фахівців.

Незалежно від того, хто конкретно організує розвідувальну роботу, загальне керівництво здійснює одна з перших осіб адміністрації фірми – перший президент, генеральний директор чи перші їх заступники, які наділені широким колом розпорядницьких функцій, що особливо необхідно для оперативного вирішення питань у розвідувальній роботі.

Середнє підприємство може дозволити собі утримувати спеціальний розвідвідділ чи групу, про яку знає дуже вузьке коло осіб. Відділ може бути самостійним чи групою якого-небудь підрозділу фірми. Він може називатися “*відділ дослідження зовнішнього середовища*”. Цей відділ організує економічну розвідку за такими основними напрямками:

- обробка легальної економічної інформації про конкурентів службовцями фірми;

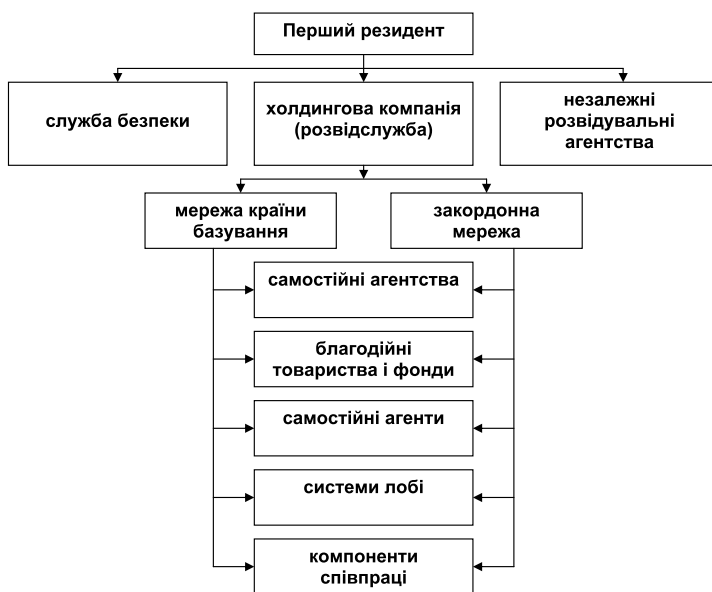


Рис. 4. Схема організації розвідки крупних підприємств

- вербування “місцевих” і “внутрішніх” агентів у конкурентів;
- встановлення контактів з незалежними агентствами й агентами;
- організація лобі на місцевому рівні.

Усі відзначені напрямки роботи вимагають бюджетного забезпечення, крім витрат на утримання організаторів розвідки, тобто спеціальних працівників. Завдання останніх зводиться не стільки до добування інформації, скільки до організації такого добування, причому здебільшого в прихованій формі. Ці витрати визначаються обсягом і цінністю інформації, що переробляється [46].

Насамперед необхідно обробити доступний, але іноді об’ємний матеріал про конкурентів, що міститься у відкритій інформації: газетні, тіле- і радіоматеріали, статистична звітність, проспекти, постачальники, покупці і т.ін. Завдання полягає в тому, щоб у всіх відділах і службах знайти фахівців, що могли б відбирати й обробляти відповідну інформацію про конкурентів. Цим працівникам необхідно забезпечити доступ до інформаційних матеріалів, дати можливість відвідувати виставки, бібліотеки, огляди тощо. Дана робота може бути організована на конфіденційній основі. Вона може частково ставитися в службові обов’язки, а частково повинна заохочуватися відповідними надбавками до заробітної плати, преміями, пільгами і т.ін. Фінансист повинен стежити за фінансовою стійкістю, платоспроможністю конкурентів, покупців, постачальників. Служба головного інженера, технолога — за НДДКР, патентами, ліцензіями, організацією виробництва; працівникам кадрових служб найлегше стежити за персональними переміщеннями в зовнішньому середовищі.

Робота з вербування місцевих і внутрішніх агентів не може бути передоручена комусь, крім безпосередніх працівників відділу — це очевидно. Контакти з незалежними розвідувальними агентствами й агентами також повинні вестися цими ж особами. У той же час до роботи з забезпечення лобізму можуть залучатися фахівці фірми, що за сферою своєї роботи можуть мати контакти з місцевою адміністрацією. Для цих цілей також можуть використовуватися окремі благодійні акції, що організовуються фірмою [46].

**Особливості організації розвідки малими підприємствами.** Малі підприємства також повинні вести комерційну розвідку того середовища, у якому вони функціонують. Оскільки малі підприємства працюють на вільних, хоча і локальних ринках, у них на відміну від великих корпорацій і середніх фірм є безліч конкурентів. Організація служби економічної розвідки щодо них стає недоцільною з погляду ефективності.

- ➔ Організатором збору цієї інформації виступає менеджер малого підприємства. Інформацію він може одержати :
- а) у консультантів спеціальних консалтингових фірм, що на основі огляду відкритої інформації можуть дати відповідний висновок про стан того чи іншого підрозділу ринкової інфраструктури;
  - б) у працівників підрозділів ринкової інфраструктури, що можуть працювати консультантами в малому підприємстві на умовах сумісництва і за відповідні гонорари представляти необхідну інформацію, давати поради;
  - в) у незалежних розвідувальних агентств і агентів;
  - г) нарешті, якщо мале підприємство має спонсором велику фірму, воно може одержувати деяку інформацію від її служби.

Таким чином, особливості організації економічної розвідки на підприємствах різних типів зводяться до зміни співвідношення між зовнішніми і внутрішніми джерелами одержуваної інформації. В міру збільшення розмірів підприємства відносно скорочується частка інформації, агентів, що купується в незалежних розвідувальних агентствах, консалтингових фірмах і консультантів й зростає значення спеціальних розвідувальних підрозділів корпорацій.

### **3.3. Методи шпигунства (методи збирання інформації)**

#### **3.3.1. Легальні методи збирання інформації**

Особливістю легальних методів збору інформації є те, що з величезної маси матеріалу потрібно витягти буквально краплини необхідних відомостей. Наприклад, у газетному нарисі про конфлікт на фірмі ви знаходите деякі відомості про менеджера, який вас цікавить, його спосіб життя чи відомості про технологію, що може бути використане в конкурентній боротьбі [46].

Збір інформації з легальних каналів повинен розгортатися за багатьма напрямками. У середніх і великих фірмах до цієї роботи за напрямками (фінанси, виробництво, НДДКР, менеджмент, маркетинг, кадри й ін.) залучаються окремі працівники. Їм забезпечується доступ до необхідних легальних джерел інформації. За рахунок фірми купуються книги, довідники, виписуються журнали, газети, включаються в мережу "Інтернет" і т.ін. Якщо немає окремих джерел на підприємстві, службовцям, що займаються збором легальної інформації, дозволяється в службовий час

працювати в бібліотеках за межами підприємства, відвідувати виставки, презентації, якщо необхідно, вони можуть спеціально відряджатися в інші міста і країни. Щоб виключити зловживання в цій роботі, кожне спеціальне відвідування чи відрядження повинне закінчуватися інформаційною довідкою щодо тих чи інших об'єктів.

### **Використання експертів**

Одним з досить ефективних методів збору легальної інформації є залучення до цієї роботи агентів-експертів (вони можуть бути працівниками державних органів, посередницьких організацій, консалтингових фірм). Ця категорія фахівців, як правило, добре знає ситуацію в галузі і регіоні, непогано орієнтується в інформаційних потоках. Особливе місце в цій категорії займають науковці і викладачі вищих спеціальних навчальних закладів, що мають розвинуті навички аналізу й узагальнення матеріалу.

### **Використання офіційних представництв за кордоном**

В сучасних умовах для цілей економічної розвідки широко використовуються офіційні представництва за кордоном: від посольств, консульств до торгових та інших представництв. Звичайною практикою в цих установах є підготовка економічних оглядів на основі легальних джерел інформації. Завдання подібного роду ставляться в службові обов'язки працівників цих установ. Зразок організації такої легальної економічної розвідки демонструє Японія, що створила доволі—таки ефективну систему збору науково-технічної і комерційної інформації про своїх закордонних конкурентів [46].



За визнанням фахівців, у Японії немає спеціальних розвідувальних органів, подібних ЦРУ, “Інтеллідженс сервіс”, ГРУ і т.ін. До речі, такий центр суперечив би конституції Японії, прийнятій у свій час з подачі американців. Організаційну роботу зі збору економічної інформації в Японії веде ДЖЕТРО (JETRO) — Організація японської зовнішньої торгівлі. У 1954 р. над ДЖЕТРО установило контроль Міністерство Міжнародної торгівлі, а в 1958 р. був прийнятий спеціальний закон. На підставі цього закону ДЖЕТРО функціонує як орган, що за завданням Міністерства міжнародної торгівлі займається збором комерційної інформації, необхідної для розвитку зовнішньої торгівлі. ДЖЕТРО має 78 філій у 57 країнах і 84 відділення в Японії. В закордонних філіях трудяться 300 японців і стільки ж місцевих громадян, що збирають інформацію відносно економіки, торгової промисловості, технологій, нових товарів, кон'юнктури ринку і т.ін. [91].

Той, хто в такий спосіб хоче організувати легальний збір інформації, може поставити перед подібною службою вирішення таких задач:

- 1) Підтримання контактів між державними органами, приватною промисловістю, дослідницькими організаціями і науковими колами (рішення проблем збору й охорони інформації).
- 2) Представлення членам цієї організації необхідної інформації про закордонних конкурентів.
- 3) Представлення інформації про закордонних конкурентів не членам організації на комерційній основі.
- 4) Відмова від збору інформації нелегальними методами.

Зібраний у такий спосіб матеріал накопичується в архіві бази даних. Тут він систематизується за об'єктами розвідки й окремими напрямками.

Серед об'єктів розвідки, як уже підкреслювалося, у першу чергу цікавлять конкуренти, постачальники, споживачі, керівники органів державного і місцевого управління, профспілкових організацій, політичних партій і рухів. Тому спочатку в базі даних виділяються ці об'єкти. Потім у базах даних про конкурентів, постачальників і споживачів виділяються внутрішні бази даних, що характеризують фінанси, виробництво (технології, продукт, НДДКР), менеджмент, маркетинг і персонал (див. рис. 5).

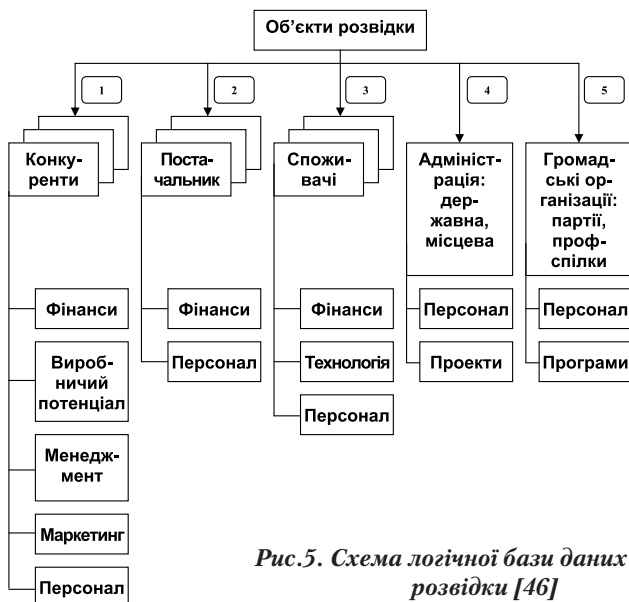


Рис.5. Схема логічної бази даних економічної розвідки [46]

Систематизований у такий спосіб матеріал підлягає подальшій аналітичній обробці. Звичайно, і схема систематизації бази даних економічної розвідки прив'язується до конкретної ситуації.

На закінчення необхідно звернути увага ще на один штрих, що стосується легальних методів збору інформації: ці дані вимагають особливо ретельного аналізу і повторного огляду, тому що в них може виявитися і дезінформація конкурента, що спеціально запускається у засоби масової інформації для приховання дійсного стану, щоб одержати кредит, замовлення, уникнути офіційного визнання банкрутства [46].

### **3.3.2. Напівлегальні методи збору інформації**

Як уже зазначалося, ці методи збору інформації найчастіше стосуються моральної норми міжособистісних взаємин, етики менеджменту і підприємництва. Тому їх не прийнято представляти сторонньому погляду. Арсенал напівлегальних методів збору інформації досить широкий. Серед них можна виділити такі, як бесіди з фахівцями конкурента в неофіційній обстановці, помилкові переговори про купівлю продукції конкурента, помилкові конкурси, зманювання з роботи провідних спеціалістів конкурента, одержання інформації від спільних постачальників, споживачів, через фонди і благодійні організації, через органи контролю [46].

#### **Бесіди з фахівцями**

Найпростіший і безневинний спосіб одержати цікавлячу інформацію — це поговорити з фахівцем конкурента в неофіційній обстановці (на прийомі, за сніданком, вечерею, на відпочинку тощо). Головне — створити невимушену обстановку, без видимої цікавості викликати співрозмовника на розмову щодо проблеми, яка цікавить, дати йому можливість висловитися і вміти його вислухати.

Основне завдання — знайти працівника з персоналу конкурента, що ще не навчився мовчати. Як звертає увагу В.Суворов, люди більше страждають від того, що наявні в них думки, ідеї ніхто не слухає. Тому, якщо ви готові і вмієте слухати, шанс одержати інформацію цим способом істотно підвищується. Спочатку бесіди, зрозуміло, можна імітувати своє прагнення *“висловитися з наболілого питання”*, але потім треба різко звільнити поле дії особі, яка вас цікавить [88].

### **Неправдиві конкурси і наймання**

Наступний напівлегальний спосіб одержати інформацію — неправдиві переговори з конкурентом про купівлю його продукції, патенту, ліцензії, ноу-хау з наступним відмовленням. Під час переговорів цілком природним виглядає цікавість до особливостей продукта, технології, винаходу і т.ін. У такий спосіб сто років тому японці “купували” в англійців кораблі, поки останні не зрозуміли, в чому справа і підкинули першим дезінформацію, у результаті чого побудований японцями зразок корабля перевернувся догори кілем при спуску [31].

Великі можливості одержання інформації про конкурента дають помилкові конкурси й оголошення про наймання. Спочатку виявляються фахівці — носії інформації, що цікавить розвідку, у фірмі конкурента. Потім вивчаються всі його особисті дані: професійний рівень кваліфікації, здібності і обдарування, захоплення, моральне обличчя, родинний стан, коло друзів, спосіб життя і т.ін. Усі ці дані оцінюються з погляду можливості одержання інформації протягом неправдивих переговорів [22, 31].

Фахівці конкурента ретельно вивчаються, виділяються їх “болючі місця”, на основі яких готується індивідуальний план неправдивого конкурсу чи переговорів про наймання. Наступний етап — встановлення контакту з об’єктом розвідки.

Оголошення про конкурс дає більш широкі можливості подання необхідної інформації. Якщо адресат не відгукнувся на оголошення про конкурс, звістка про конкурс доводиться через родичів, друзів, адвокатів, лікарів, що лікують, перукарів, офіціантів і т.ін., тобто через тих, з ким він спілкується.

Значною мірою сказане відноситься і до несправжніх наймів, Фахівець, прагнучи одержати вигідну посаду, не робить внутрішнього опору видачі інформації. Однак це зовсім не означає, що всі питання можна ставити прямо. Напроти, це повинно бути завуальовані, непрямі питання, що підштовхують до необхідної відповіді [46].

Коли отримані тести, матеріали співбесід, наступним етапом є розшифровка отриманих відомостей.

### **Запрошення консультантів**

Важливим джерелом напівлегальної інформації є фахівці, що працюють у державних органах влади і контролю (статистичних органах, органах санітарно-епідемічного контролю, пожежної охорони і т.д., місцевих і центральних органах влади).

Ще більші можливості одержувати конфіденційну інформацію напівлегальним шляхом можна через запрошення на роботу консультантів, які перебувають у стосунках з фахівцями посередницьких фірм, що обслуговують і вашого конкурента (постачальників, дистриб'юторів, брокерів, службовців банківських, страхових і транспортних компаній і т.ін.). Сюди ж відносяться і спеціальні консалтингові фірми, працівники науково-дослідних установ, викладачі навчальних закладів [46].

### **Використання фондів і товариств**

Великі можливості для напівлегального збору інформації мають різного роду фонди і товариства. Вони можуть розгортати збір даних у територіальному розрізі, вести персональну роботу. Наприклад, у сорокових роках такі відомі американські компанії, як “Дженерал електрик”, “Вестингауз” та інші, підтримували фінансово американську місію “Нові племена”, що вела роботу з християнізації племен, яких не торкнулась цивілізація, у 16 країнах Латинської Америки. Представники місії, як правило, розгортали свою роботу серед тих племен, що проживали на територіях з перспективними покладами корисних копалин [46].

Місії і фонди, залучаючи до своєї діяльності окремих осіб, мають можливість вигідно використовувати їхній інформаційний потенціал [31]. Найчастіше до такого співробітництва залучаються колишні рядові службовці корпорацій, що опинились поза справами з виходом на пенсію. Якщо вищий управлінський персонал, як носій цінної інформації, навіть після виходу на пенсію залишається в корпорації в якості “радників”, почесних президентів, почесних голів, почесних членів спостережних та інших рад зі збереженням високих окладів, то про рядових службовців, що обслуговували інформаційні потоки корпорацій, як правило, забувають [46].

### **Зманювання провідних спеціалістів**

Особливо варто зупинитися на такому напівлегальному методі збору інформації, як зманювання провідних спеціалістів конкурента.



У 60-ті рр. Г. Форд II посварився з президентом власної фірми Лі Якокою. Причиною сварки послугували перспективи розвитку політики автомобілебудування: поставляти на ринки “крейсери доріг” чи “малолітражки”? Ситуація повторилася як і на початку тридцятих років, коли батько Г. Форда II — Г. Форд I — віддав пальму першості переходу на плідні технології “Дженерал моторз”. Мабуть син хотів піти по стопах батька і знову подивитися, що вийде з переходом на виробництво

“малолітражок” у свого конкурента, з чим принципово був незгодний Лі Якокка. В результаті сварки Лі Якокка виявився в кріслі президента, а потім і голови правління “Крайслер Корпорейшн”. Звичайно ж, з переходом президента секретри фірми “Форд Моторз”. перестали бути секретами для правління “Крайслер Корпорейшн”. Цей перехід обернувся Фордові втратою значної частки американського ринку легкових автомобілів (частка Форда скоротилася з 30 до 25% — приблизно півмільйона автомобілів). У 1968 р. “Форд Моторз” переманила у “Дженерал Мотора” одного з її президентів, що опікував заводи “Шеврове” — С. Кнудсена разом із секретами “Дженерал Моторз” [46].

### **Використання жіночої краси**

Не менш важливу роль у напівлегальних і нелегальних способах одержання необхідної інформації споконвічно відіграла жіноча краса. Суть проблеми полягає у використанні особливостей біологічної природи людини, коли гра на почуттях дає можливість “розв’язати язик” людині й одержати необхідну інформацію. Прикладів тут незліченна безліч і літературних, і історичних.

Жінки значною мірою є природженими мисливицями за чужими секретами. Мата Харі була знаменитою розвідницею, видаючи себе за індійську танцівницю. Зоя Рибкіна, відома як письменниця Воскресенська, виконала не один десяток найскладніших розвідувальних завдань [66].

З таким самим успіхом жіночі здібності в розвідці експлуатуються “сильною статтю”. В.Шелленберг описує успішну розвідку югославським військовим через любовні зв’язки з представницями “слабкої статі” у вищих колах гітлерівської Німеччини перед другою світовою війною [98].

### **Використання наукових зв’язків**

Ще одним каналом збору інформації є наукові контакти. Конференції, симпозіуми, семінари і т.ін., що проводяться на міжнародному рівні, з успіхом можуть бути використані для одержання потрібної інформації.

Ще більше можливостей для одержання науково-технічної інформації існує при встановленні через фонди стипендій, грантів.

## **3.3.3. Нелегальні методи збору інформації**

Як уже підкреслювалося, нелегальні методи збору розвідувальної інформації стосуються таємних відомостей, що охороняються власником, а нерідко і законом.

Численні нелегальні методи збору інформації можуть бути класифіковані в такий спосіб:

1. Викрадання власності конкурента.
2. Викрадання документів, що містять інформацію, яка цікавить заінтересовану сторону.
3. Копіювання документів, що містять інформацію, яка цікавить заінтересовану сторону.
4. Засилання проникаючих агентів на об'єкт конкурента.
5. Впровадження агентів у структурах конкурента.
6. Прослуховування розмов конкурента.
7. Проникнення в комп'ютерну систему конкурента.

### **Викрадання власності конкурента**

Особливо часто прийоми викрадання використовуються під час підготовки, проведення і згорання виставок, ярмарків, демонстрацій та інших рекламних заходів. Крім того, викрадання мають на меті отримання об'єкта для дослідження, вони можуть використовуватися і для зриву рекламних заходів. Історії відомо багато подібних випадків (викрадення шовкопряда, порцеляни, технологій виплавки сталі; зрив демонстрацій кулемета “Максим” і т.ін.). Викрадена продукція потім досліджується в спеціальних таємних лабораторіях, що ще називаються “лабораторіями вівісекції”.[46]

### **Викрадання і копіювання документів**

Розкрадання документів, якщо воно навіть і не закінчилося провалом агента, служить сигналом для фірми і вона застосує захисні заходи. Більш вдалим у цьому відношенні є копіювання документів конкурента. *По-перше*, уміло проведене копіювання документів не залишає слідів і для їх власника залишається невідомим. Це, мабуть, найголовніший фактор на користь даного прийому. *По-друге*, сучасна комп'ютерна, фото- і відеотехніка дозволяють робити цю роботу швидко, якісно і надійно. [46]

### **Засилання і впровадження агентів у структури конкурента**

*Задача таємного збору інформації*, — відзначав А.Даллес, — складається головним чином з того, щоб обійшовши всі перешкоди наблизитися до визначеного об'єкта [40]. Наступна задача — збір і добір інформації, що також здійснюються таємними методами. Подальша задача і, мабуть, не менш відповідальна — передача інформації користувачу. Нарешті, остан-

ня — обробка інформації, вирішується простіше, за допомогою залучення фахівців у спеціальних відділах і лабораторіях.

При нелегальних методах збору інформації перші три задачі вирішуються агентами. Головна проблема підбору агентів зводиться до наступного: вони повинні уміти вирішувати всі три задачі, пов'язані з доступом до об'єкта, збору і добору інформації та її передачі. Цим вимогам різні типи агентів відповідають не рівною мірою.

Відзначені перешкоди переборюються двома методами:

- 1) комбінуванням агентів для проведення однієї операції чи рішення однотипних задач;
- 2) впровадженням агента на об'єкт розвідки.

При епізодичному проникненні на об'єкт конкурента можна комбінувати на рішенні однієї задачі декількох агентів, фахівців у різних галузях: проникнення, добору інформації, її доставки. При епізодичному проникненні розвідник на об'єкті знаходиться нелегально і першим кроком до такого стану є подолання охорони на вході і виході.

У цьому випадку використовуються різні прийоми: відключення сигналізації, підробка перепусток, відволікання охорони, вхід з чорного ходу і т.ін. Досвідченому розвіднику найчастіше допомагають інтуїція і випадок. Років тридцять тому робітники одного з тракторних заводів поспорили з охоронцями, що в них на очах виженуть трактор за ворота без документів. Недовго роздумуючи, узяли з конвеєра трактор, причепили до нього візок, що стояв зі сміттям, виїхали за ворота, поставили трактор і сказали охороні, щоб ті відправили його на місце (вочевидь, робітники знали, що в такий спосіб сміття вивозили постійно). [46]



Лектор з комерційної розвідки поспорив з президентом фірми, що в нього на очах увійде в ретельно охоронюваний офіс. Під'їхавши в супроводі президента і поліцейського (оскільки йшов експеримент) і переконавшись, що вхід дійсно ретельно охороняється, розвідник побачив, що з чорного входу йде розвантаження автомобіля. Підійшовши до нього, узяв ящик і ввійшов з ним у будинок. Пройшов по ньому. Вийшовши у вестибюль, щоб без підозр залишити об'єкт, попросив чергового викликати йому таксі, а коли той відлучився, взяв у нього зі столу телефонний довідник, яким підтвердив свою присутність на об'єкті президенту і поліцейському, що очікували [31].

При рішенні задач довгострокового проникнення доцільне вербування фахівця на об'єкті і підключення до нього зв'язкового ззовні.

Велику цінність має таке проникнення, коли агенту вдається потрапити на об'єкт легальним шляхом і влаштуватися там на роботу. Не важ-

ливо, що цей агент не буде ключовою фігурою на об'єкті, важливо щоб він мав доступ до каналів інформації. Наприклад, Д.Грінглас в атомній лабораторії Лос-Аламоса (США), де розроблялася атомна бомба, був лише креслярем.

“Впровадження” агента є тривалим і дорогим процесом, тому що агента треба “вирощувати”; його треба відбирати зі студентської лави, його треба “утримувати”, його треба підтримувати, допомогти зробити кар'єру (чим вище буде його службова сходинка в ієрархії конкурента, тим більш цінні відомості він буде поставляти). З цього погляду значну економію дає “вербування” [46].

### **Методики вербування агентів**

Цінність завербованого агента на підприємстві конкурента визначається не тільки тією інформацією, що він поставляє, а й самим фактом його присутності на об'єкті конкурента, самою можливістю постачань інформації.

Процес вербування агента умовно можна підрозділити на ряд етапів:

- визначення необхідного об'єкта вербування;
- пошук майбутнього агента;
- процес вербування
  - а)** на добровільній основі;
  - б)** під тиском.

В. Суворов, наприклад, виділяє декілька правил вербування [88], *перше з яких пов'язано з пошуком необхідного об'єкта вербування*. Вербування президента корпорації і його заступників, їхніх радників, головних конструкторів і фахівців пов'язане з дуже високими витратами. Іноді ця категорія співробітничує “під тиском”, з остраху позбавитися досягнутого статусу.

*Наступне правило говорить, що набагато дешевше обійдуться такі носії корпоративної інформації, що не мають високого службового статусу і райдужних перспектив*. Такими кандидатами можуть бути працівники ремонтних служб, зв'язківці, працівники канцелярій, секретарі, референти, помічники провідних спеціалістів, президентів і їх заступників, креслярі, програмісти й оператори ЕОМ, дружини і коханки відповідальних працівників. Не треба забувати, що ця категорія людей знає про об'єкт, який вас цікавить, не менше ніж їх начальники.

*Важливе правило вербування зводиться до того, що контакт з об'єктом вербування варто встановлювати в невимушеній обстановці*.

*Четверте правило чи закон вербування, згідно з В. Суворовим, говорить, що в кожній людині в голові є блискучі ідеї, і кожна людина страждає*

*в житті більше від того, що їй ніхто не слухає.* Головне в мистецтві вербування — уміння уважно слухати співрозмовника. Навчитися слухати не перебиваючи, — це гарантія успіху.

*П'яте правило, чи закон вербування — це закон полуниці.* Якщо твій співрозмовник любить полуницю, не пригощай його тістечком.

Мистецтво вербування складається в умінні застосовувати всі ці п'ять правил.

Якщо у військово-політичній розвідці добровільне вербування може здійснюватися без підкупу, коли агент готовий працювати на вас з ідейних міркувань, то в економічній розвідці в основі добровільного вербування лежить підкуп.

Коли вербування на добровільній основі не спрацьовує, тобто об'єкт не виявляє готовності до співробітництва, до нього, як правило, застосовують політику “тиску”.

### **Лабораторії “вівісекції”**

Викрадені чи придбані продукти, устаткування, їх деталі, як правило, використовуються для “конструювання навпаки”. Великий матеріал для цього поставляють таємні лабораторії, що називаються лабораторіями “вівісекції”. Такі лабораторії мають усі більш-менш великі корпорації, де досліджується продукція конкурента за всіма параметрами: якості, продуктивності, надійності, технологічності виробництва й обслуговування. Продукція конкурента порівнюється з власною не тільки в цілому, а й за окремими деталями.

➔ Організація лабораторій “вівісекції” повинна будуватися на таких принципах:

- 1) Продукція конкурента аналізується за всіма параметрами;
- 2) власна продукція аналізується за тими самими параметрами;
- 3) порівнюється власна продукція і продукція конкурента, виявляються переваги тієї та іншої;
- 4) виключаються особисті емоції;
- 5) виключається патріотизм і відданість компанії в оцінці продукції конкурента;
- 6) продукція конкурента на основі удосконалення пристосовується до власного виробництва;
- 7) інформація про вади власної продукції секретна;
- 8) існування лабораторій “вівісекції” не афішується.

Приклад такої лабораторії “вівісекції” описаний у романі А. Хейлі “Колеса”. [46]

### **Використання технічних засобів**

Сучасний розвиток науки і техніки дозволяє одержувати інформацію без проникнення на об’єкт звичайними методами. Аудіо- і відеотехніка досягла мікроскопічних розмірів і може виявитися в найнесподіваніших місцях. Датчики монтуються в ручки для писання, окуляри, запальнички, капелюхи, гудзики, прикраси, зуби, підбори і т.ін. Окрім того, розвиток комп’ютерної техніки та всеохоплюючий її характер потенційно дає можливість проникнути у комп’ютерну мережу, наприклад конкурента, з приміщення, що розташоване далеко за межами його об’єктів; лазерна техніка забезпечує можливість зчитування ззовні розмов всередині будинку; переміщення та радіозв’язок записуються супутником, що пролітає в космосі, і т.ін.

Детальніше ці методи та засоби будуть розглянуті в наступних розділах. Також розглянемо шляхи мінімізації витікання інформації при використанні технічних засобів.

## **3.4. Канали витікання інформації**

Для того, щоб максимально захистити секрети підприємства від шпигунів, необхідно насамперед визначити, яка саме інформація може стати об’єктом комерційного та промислового шпигунства, хто або що є її носієм, яким чином до неї можна отримати доступ, а також хто може бути зацікавлений в отриманні такої інформації. Кожне підприємство мусить самостійно визначати всі ці перераховані параметри відносно своєї діяльності та положення на ринку.

Передусім необхідно визначити, розголошення якої інформації може завдати шкоди підприємству, а також визначити носіїв цієї інформації. Найчастіше часто об’єктами шпигунства стають:

- 1) розробка нових виробів, ідеї;
- 2) науково-дослідні роботи, нові технології;
- 3) інформація про розробників;
- 4) створення нових підприємств, злиття;
- 5) ноу-хау;
- 6) ресурси;
- 7) умови контрактів;

- 8) постачальники, клієнти;
- 9) рекламні програми;
- 10) інвестиції;
- 11) плани;
- 12) способи захисту інформації.

Після визначення ступеня секретності інформації необхідно визначити, де зібрані відомості щодо конкретного об'єкту та яким чином вони можуть бути отримані. На цьому етапі виявляються джерела отримання інформації та визначаються методи шпигунства, за допомогою яких ця інформація може бути отримана.[93]

Необхідно зазначити, що першочерговим каналом як виникнення, так витікання інформації є людина, тому необхідно визначити осіб — потенційних викрадачів секретів:

- 1) конкуренти;
- 2) клієнти;
- 3) постачальники;
- 4) рекламні агенти;
- 5) працівники державних органів контролю;
- 6) журналісти;
- 7) професійні шпигуни;
- 8) незадоволені працівники та особисті вороги керівників.

Найбільш вірогідним каналом витікання інформації є людина, тому основна увага повинна приділятися психологічній профілактичній роботі зі співробітниками підприємства, прищепленні відданості підприємству.

Отже, основними каналами витікання інформації можуть бути:

- 1) працівники підприємства, міграція спеціалістів;
- 2) публікації в засобах масової інформації, звіти про НДДКР, доповіді і виступи співробітників підприємства на симпозіумах, семінарах тощо;
- 3) спільна робота з іншими підприємствами, контрагентами ринкових відносин, а також контакти з потенційними замовниками та покупцями, постачальниками, інвесторами;
- 4) торгові виставки, рекламні матеріали;
- 5) комп'ютерна техніка та інші технічні засоби.

**Оцінити шкоду від викрадення конфіденційної інформації** дуже важко, оскільки економічна злочинність багатопланова і практично завжди копіювання товару, корупція, рекет або шахрайство передбачають попереднє викрадення інформації. Фахівці багатьох країн намагались систематизувати інформацію про нанесені таким чином збитки, але точ-

них статистичних даних отримати не вдалось. У даному розділі наведені деякі цифри, що характеризують обсяги нанесеної економічним шпигунством шкоди та затрат, які деякі підприємства несуть як в процесі його здійснення, так і в процесі боротьби з ним.[93]

Викрадення комерційних та промислових секретів у США наносить шкоди значно більше 100 млрд доларів рік, і якщо не буде вжито заходів, ця сума буде й надалі постійно зростати.

Дрібні підприємства Нью-Йорка через злочинні посягання терплять збитки в розмірі 1 млрд доларів на рік. Шкода, що наноситься американському бізнесу від викрадення торгових секретів, складає близько 4 млрд доларів на рік, незважаючи на те, що приватні компанії в США витрачають на забезпечення конфіденційності своєї інформації понад 12 млрд доларів на рік, а приватна поліція нараховує понад 1 млн чоловік, що вдвічі перевищує кількість державних поліцейських. [93]

При цьому щорічна шкода від комп'ютерних злочинів у США складає 100 млрд доларів, а в Західній Європі — 35 млрд доларів. У середньому шкода, нанесена кожним комп'ютерним злочинцем, становить 450 тис. доларів США. [93]

В Японії витрати на комерційну розвідку складають в середньому 1,5% обороту великих концернів, а витрати на захист комерційних секретів — близько 20% річного прибутку підприємств.

У Франції на економічне шпигунство витрачається понад 1 млрд. доларів США, а займаються ним більше 50 тис. чоловік.

У Німеччині функціонує понад 3 тис. фірм, що займаються виготовленням засобів захисту підприємств від економічного шпигунства на суму приблизно 4 млрд доларів США на рік, а щорічне зростання цієї галузі промисловості складає 7–8%. У цій країні нараховується понад 280 тис. приватних детективів та охоронців (при штаті офіційної поліції — 250 тис. чоловік). [93]

Економічна оцінка втрати комерційної таємниці повинна базуватися на розмірах прибутку, який отримує підприємство від впровадження або використання нових технологій, продуктів, товарів та послуг. Для впровадження будь-яких інновацій, що складають комерційну таємницю, розробляються конкретні бізнес-плани з урахуванням витрат на її захист. До таких затрат відносяться разові закупівлі технічних засобів захисту об'єктів, систем сигналізації та їх монтаж, а також поточні витрати: витрати на утримання спеціалістів з експлуатації систем сигналізації і працівників, які постійно займаються питаннями забезпечення захисту комерційних секретів, а також на утримання приміщень служби безпе-

ки, друкування спеціальних бланків, перепусток, карток для відвідувачів тощо.

Закордонні джерела визначають витрати на захист комерційної таємниці підприємства в розмірі до 20% його прибутку. [93]

Додаткові витрати можуть виникати при зверненні до суду для захисту своїх комерційних інтересів при порушенні комерційної таємниці.

Закордонні джерела рекомендують завчасно підрахувати ефективність звернення до суду. Так, послуги адвоката по захисту комерційної таємниці в США коштують 75 тис. доларів, зняття копій з документів для подання до суду — до 2 тис. доларів. Виникнуть додаткові витрати на консультантів, експертів, а також дорожні витрати. Однак спеціалісти США вважають, що найбільшою шкодою є втрата часу менеджерів на участь в судових розглядах [93].

### **3.5. Дані про ділових партнерів та конкурентів**

Найбільшу небезпеку для підприємств становлять зовнішні загрози, потенційними носіями яких найчастіше є ділові партнери та конкуренти. Тому питанню відслідковування загроз, що йдуть від них, варто надавати великої уваги. Для цього необхідно постійно збирати інформацію про конкурентів та ділових партнерів.[93]

Завданням осіб, що займаються збиранням та аналізом інформації, є виявлення джерел зовнішньої загрози безпеці, щоб максимально знизити невизначеність стратегічного ризику. Така інформація повинна розкривати наміри потенційних та дійсних партнерів щодо підприємства; характеризувати сильні та слабкі сторони конкурентів; попереджати про можливе виникнення загроз та кризових ситуацій; полегшувати контроль за дотриманням партнерами досягнутих раніше домовленостей; сприяти виявленню несанкціонованих каналів витікання конфіденційної інформації про підприємство; допомагати в процесі прийняття рішень та вироблення власної політики підприємства щодо окремих суб'єктів господарювання.

Практика свідчить, що інформація щодо можливих партнерів та конкурентів, яка надходить у розпорядження керівництва підприємства, повинна містити, як мінімум, такі відомості [93]:

- Повну назву, юридичну адресу, номери телефонів, факсів.
- Дату та номер реєстрації, в якому місті, юридичній фірмі це було зафіксовано.
- Імена керівників, їх службове сходження, адреси.

- Інформацію про участь в судових та інших процесах, заставах майна, цитати з газет та журналів та їх оцінка.
  - Інформацію про практику виконання платежів: які суми, в які терміни та з якими затримками були виплачені.
  - Назви банків, з якими працює підприємство, адреси та номери рахунків.
  - Порівняльну характеристику фінансового стану підприємства за останні роки.
  - Прибутковість вкладень, розмір інвестицій тощо.
  - Основні показники з останнього балансового звіту, звіту про фінансові результати.
  - Назви дочірніх підприємств, філіалів та відділень.
  - Характеристику діяльності: товари і послуги, експорт-імпорт, умови угод.
  - Перерахунок партнерів даного підприємства.
  - Ймовірні зв'язки в кримінальному оточенні.
- ⊙ *Збирання, аналіз і оброблення подібної інформації є найбільш відповідальною складовою системи забезпечення безпеки підприємства. Крім того, практично вся зібрана інформація потрібна також для маркетингу, оскільки на його основі виробляється політика підприємства.[93]*

Складання подібних досьє на всіх головних конкурентів допоможе у відпрацюванні найбільш ефективної стратегії фірми. “Анкету ділового партнера” (додаток 1) повинна заповнювати особа, яка відповідає за роботу з даним партнером, “Анкету конкурента” (додаток 1) повинні заповнювати особи, що розробляють стратегію фірми на ринку, спеціальні агенти. Такі досьє необхідно складати лише на ті підприємства, що є конкурентами для вашого підприємства або можуть ними стати.[93]

Інформація про ділових партнерів направлена в основному на те, щоб змусити партнера робити те, що необхідно вашому підприємству. Створювати такі досьє слід на важливих та потенційних партнерів.

### 3.6. Технічні засоби збирання інформації

#### 3.6.1. Технічні засоби і збирання розвідувальних даних

У практиці розвідувальної роботи давно використовується зовнішнє спостереження за конкурентом без проникнення на його об'єкти. Усі новітні технічні засоби, у першу чергу, використовувалися в розвідслужбах. В. Шелленберг відзначає, що під час другої світової війни, щоб прийняти швидкісну радіограму від агента за допомогою мініатюрного (на ті часи) радіопередавача за тисячу кілометрів у Берліні необхідно було змонтувати устаткування, що займало три кімнати [98]. Нині мікросхеми дають можливість зменшити аудіо- і відеопристрої до таких меж, що дозволяють ховати їх у дрібних предметах побуту людини, що значно полегшує процес проникнення і збору інформації без постійної присутності агента [25]. А. Даллес з приводу цього зауважив, що радари й електронні прилади будуть займати місце розвідниці типу Мата Харі. Він виділяв такі способи використання технічних засобів для спостереження за об'єктом розвідки [40]:

1. Радіолокація.
2. Фотографування.
3. Прослуховування переговорів.
4. Хімічний аналіз екологічного середовища об'єкта (грунту, повітря, води).

Тепер сюди можна додати телевізійні спостереження, комп'ютерну розвідку, біологічний аналіз. Інформація, одержувана за допомогою технічних засобів безпосередньо з об'єкта розвідки, обробляється набагато легше. Головні труднощі можуть полягати в розшифровці інформації, зібраної за допомогою технічних засобів за межами об'єкта.

Відомо, що кожен об'єкт економічного аналізу являє собою систему, в яку надходять ресурси, що переробляються і з якої виходить продукція: товари і послуги. Але крім них є ще виробничі відходи, викиди тощо, є ще комунікаційні зв'язки об'єкта з зовнішнім середовищем.

Використання технічних засобів дає цілий ряд переваг [46]:

- *по-перше*, розкритий “жучок” на відміну від розкритого агента менше скаже про того, хто його поставив;
- *по-друге*, сьогодні використання технічних засобів може виявитися дешевшим з огляду на те, що карна і цивільна відповідальність за економічне шпигунство посилюється, а разом з нею зростає вартість інформації, отриманої агентами;

- *по-третє*, використання технічних засобів дає можливість одержувати безперервний потік інформації, що є дуже цінним в розвідувальній роботі.

### 3.6.2. Аудіо- і радіотехніка в розвідувальній роботі

З винаходом радіо використання звукозаписних і передавальних пристроїв одержало могутній імпульс у розвідці. Сьогодні мініатюрні передавачі можуть бути вмонтовані в пишучий олівець, окуляри, запальничку, кулю від дрібнокаліберної гвинтівки і т.ін. Електронні “жучки” вставляються в телефонні апарати, підкидаються в приміщення, монтуються в предмети побуту осіб, які цікавлять розвідку, тощо і постійно передають звукову інформацію.

Акустичний контроль приміщення можливий за допомогою:

- мікрофона, з виводом сигналу по кабелю;
- диктофона;
- стетоскопа;
- радіомікрофона;
- телефонної лінії;
- лазерного зняття інформації із віконного скла.

Спеціальні мікрофони мають дуже маленькі розміри. Інформація із мікрофона передається по кабелю у сусідню кімнату, де виконується її запис. Вузьконаправлений мікрофон дає змогу прослуховувати на відстані до кілометра.

Професійні цифрові диктофони, незважаючи на маленькі розміри, дозволяють безперервно записувати до 20 год.. Якщо використати функцію акустопуску (запис здійснюється лише тоді, коли хтось говорить), то залишений диктофон може записувати інформацію дуже довго. Деякі диктофони монтують у побутові речі (наприклад у ручку).

Стетоскоп — прилад, що дає можливість прослуховувати крізь товсті стіни (товщиною до метра).

Телефонна лінія використовується не тільки для прослуховування телефонних розмов, а й для прослуховування офісу (при цьому трубка лежить на телефонному апараті). Для цього використовується мікрофонний ефект, високочастотне нав'язування, системи “теле-монітор”, “телефонне вухо” та інші. Деякі системи дозволяють прослуховувати будь-яке приміщення, через котре проходить телефонний кабель, навіть з іншої держави.

За допомогою спеціального лазера можливе прослуховування офісу через зачинене вікно з відстані до кілометра.

Радіомікрофон — основний пристрій для негласного отримання інформації. Залишений один раз у офісі “жучок” буде роками передавати акустичну інформацію по радіоканалу. Розміри цих “жучків” залежать від розміру блоку живлення. Якщо “жучок” живиться від стороннього джерела (наприклад від телефонної лінії), то він зовсім непомітний. Вага таких пристроїв коливається від декількох грамів до кількох сотень грамів, потужність передавального пристрою — від десятих часток до кількох сотень мВт, що забезпечують передачу інформації від декількох годин до декількох років на відстані від десяти метрів до восьми тисяч метрів (наприклад НКГ-1452 може передавати інформацію на відстань 2–8 км).

Акустичні закладки (пристрої для перехоплення акустичної інформації) — “жучки” — класифікуються за видом виконання, місцем встановлення, джерелом живлення, способом передачі інформації та її кодування, способом керування і т.ін.. Перехоплена ними інформація може передаватись по радіо або оптичному каналу, по електромережі змінного струму, по телефонних та інших з’єднувальних лініях, а також по металоконструкціях будівель, трубах систем опалення і водопостачання тощо. Найбільш широко використовуються закладки, що передають інформацію по радіоканалу (радіозакладки).

В залежності від середовища розповсюдження коливань, що переходять на радіозакладками, їх поділяють на акустичні радіозакладки (перехоплення акустичних сигналів через повітряний канал) та радіостетоскопи. Акустичні радіозакладки (радіомікрофони) здатні вловлювати неголосну розмову на відстані 5–10 метрів. Радіостетоскопи здатні вловлювати звукові коливання через бетонні стіни товщиною 0,3–0,7 м, а також через двері та віконні рами.

Акустичні радіозакладки мають оригінальні форми. Наприклад у формі настільного калькулятора вагою 350 г. випускається радіомікрофон РК-620 з дальністю дії 100–200 м і необмеженим часом, тому що передавач і калькулятор працюють одночасно.

Цікава модель радіомікрофона РК-585, виконана у формі авторучки, вага якої з батарейкою складає 25 г, а дальність передачі 80–300 м у прозовж 6 год., чи STG-4130 вагою 60 г і виконана у формі пачки цигарок. Не менш цікавою є модель радіомікрофона, виконана у формі трійника для побутової апаратури, оскільки живиться від електричної мережі час передачі на 100–200 м необмежено. Модель АД-45–3 виконана у формі телефонної розетки, живиться від телефонної мережі, час роботи не обмежено, передача до 150 метрів. Модель РК-535 виконана у формі склянки для віскі, а РК 565-S — у формі попільниці, РК-580 має вигляд підсвіч-

ника, РК-575 — настільної запальнички, РК-560 виглядає як стандартна електролампа.

Також є підслуховуючі пристрої, що ховаються в одязі людини (наприклад РК-157-S чутливістю до 20 м), а також під наручним годинником (РК-1025-S), у шкіряному ремені (РК-850-S).

Для прослуховування в транспортних засобах використовуються моделі РК-465-S, РК-470, РК-475-S, при цьому шум від двигуна та їзди практично усувається.

Тепер для збільшення тривалості роботи “жучків” з автономним живленням, а також для вирішення проблем скритності (зменшення часу “холостої” роботи передавача знижує імовірність його виявлення) розробляються моделі з дистанційним включенням (110 F, РК-550 — розетковий, НВ-РМ-430К — в середині настільного електронного годинника), а також що автоматично включаються при виникненні звуку — музики, мови і включаються при його зникненні (STG- 4001).

Якщо проникнення на об’єкт обмежено, “жучки” монтуються в кулі, стріли. Так, модель РК-995 монтується в стрілу і безшумним пістолетом прицільно вистрілюється на відстань до 25 м. Модель STG 301 монтується в стрілу арбалета і передає інформацію на відстань до 100 м [16].



У свій час преса описувала випадок економічної розвідки проти японської компанії “Нагоя-Вінер”. Ця компанія була на грані банкрутства, але майстерно приховувала даний факт в офіційній звітності і кваліфіковано зберігала цю таємницю від своїх партнерів. Банки, відчуваючи подвійну гру з боку “Нагоя-Вінер”, звернулися до послуг спеціального розвідувального агентства. Стеження за об’єктом не приносило відчутного успіху доти, поки в головного бухгалтера не розболівся зуб. Досвідчений дантист підлікував йому зуб, поставив пломбу, в яку був вмонтований радіомікрофон і який протягом декількох днів передавав все, що говорив головний бухгалтер компанії “Нагоя-Вінер”. Секрет фірми розкрився: банки відмовили їй у кредиті і вона збанкрутувала [46].

Недоліком радіозакладок є можливість виявлення їх випромінювань спеціальним приймачем контролю. З метою усунення цього недоліку розроблені закладні прилади, що передають інформацію по оптичному каналу в інфрачервоному діапазоні (РК 770-S). Дальність передачі для них складає декілька сотень метрів. Наприклад, інфрачервоний передавач STG-4403 забезпечує передачу інформації на відстань до 500 м.

Також значно зменшились і радіоприймальні пристрої. Їхня вага коливається від 150–250 г до 8–15 кг, а габарити вимірюються від десятків

міліметрів до десятків сантиметрів, тобто вони можуть бути заховані в кишені, кейсі, автомобілі. Найкращим варіантом вважається такий радіоприймальний пристрій, що укомплектований записуючим механізмом, наприклад мініатюрним магнітофоном [46].

Зараз, радіомікрофони з позиції “жучків” починають переміщатися в позицію “клопів”, що ще більше розширює технічні можливості їх застосування.

Дуже важливим джерелом одержання інформації є телефонна мережа: телефонний апарат, телефонна лінія зв'язку. Телефонний апарат перетворюється в мікрофон навіть тоді, коли трубка не знята, і через нього прослуховуються всі розмови за допомогою спеціального пристрою, підключеного до мережі.

Одержання інформації з телефонної мережі хоча і більш доступне, але залишається все-таки трудомісткою справою. Однак доцільність прослуховування визначається не рівнем витрат, а цінністю можливої інформації. Пристрої для прослуховування можна вбудовувати в телефонний апарат (РК-110, НВ-ПТ, РК-130 “Рисове зерно”), підключати до лінії від телефонного апарата (АД-31, АД-48, АД-45–4) і, нарешті, до кабелю.

Найчастіше використовуються телефонні радіотранслятори, що підключаються до телефонної лінії і передають інформацію з радіоканалу. Джерелом живлення для таких пристроїв зазвичай слугує напруга телефонної мережі. Включаються вони і виключаються разом із включенням телефонного апарата в мережу. Ці радіотранслятори малогабаритні, тому що на відміну від радіомікрофонів їм не потрібні мікрофони і джерела живлення.

Телефонна лінія використовується і для прослуховування розмов у приміщеннях, де встановлений телефон. До телефонної лінії підключається апаратура типу ИМ103, ST-01ELSY, БОКС-Т та інші. Деякі з цих пристроїв мають дуже доступну ціну [16].

Крім телефонних апаратів для прослуховування приміщень часто використовуються “стетоскопи”. Датчик-мікрофон, комбінується з радіопередавачем спільно чи роздільно і веде радіопередачу на відстань від декількох десятків до кількох сотень метрів. Перевагою використання стетоскопа є те, що він, як правило, встановлюється на зовнішній стороні стіни — зовні будинку, в іншій кімнаті, на горищі, тому менша імовірність його виявлення, розміри датчиків і передавачів вимірюються міліметрами і десятками міліметрів (моделі АД-50, SKS, РК-1005, РК-775 (інфрачервоний передавач), РК-845-S, РК-845-SS, AP-8, STG-4025, STG-4027, НВ-СТ 05 та ін).

Особливо великі можливості прослуховування розмов, і не тільки телефонних, відкриває лазерна техніка. Невидимий промінь, спрямований на вікно чи стіну, як патефонна голка знімає вібрацію, викликану голосом людини. Так у кінофільмі “Бригада” показаний такий прийом прослуховування.

Подібна апаратура також малогабаритна, вміщується в кейсі, але коштує дуже дорого. В Росії з’явилися перші дослідні зразки, наприклад ЛСТ-ЛА2 з дальністю до 100 м. У США подібний пристрій НР-150 забезпечує дальність дії в 10 разів більшу. Але ще на порядок вища їх ціна [16].

Цим же цілям служить і радіоперехоплення переговорів, що ведуться з використанням ефіру. В державній розвідці необмежені можливості прослуховування переговорів дають супутники-шпигуни, що, пролітаючи на величезній висоті, фіксують всі електронні сигнали в провідному й ефірному зв’язку. Ці сигнали потім розшифровуються в потужних електронно-обчислювальних центрах.

Останнім часом широке розповсюдження одержали радіомаяки. Є товари багатофункціонального призначення (наприклад комп’ютери). Якщо вони замовлені об’єктом, що цікавить розвідку, в нього монтується радіомаяк, який включається тоді, коли над цією країною пролітає супутник-шпигун. Ця методика нагадує супутникову систему пристрою проти викрадення автомобіля, коли в нього монтується радіомаяк, що посилає сигнали на супутник, який фіксує його місцезнаходження.

- ◎ *Тепер у комп’ютерні блоки вбудовуються уже не просто маяки, а цілі ретранслятори, що накопичують і ретранслюють за стіни підприємства інформацію, оброблювану комп’ютером.*



Як повідомляли “Московські новини” у 1992 р. подібна закладка була виявлена в ЕОМ “Вакс” американської фірми “ТЕК”. Перевірка 200 комп’ютерів цього типу, закуплених у свій час Мінавіапромом СРСР, показала, що в 8 з них було 20 закладок. Виявилося це випадково, коли на одному з підмосковних підприємств вийшов з ладу комп’ютер “Вакс”. За задумом розвідників із ЦРУ за поломкою комп’ютера повинен був піти виклик “фахівця”, який би і списав інформацію, що міститься в блоці. А після цього, через якийсь час у закладці повинна була спрацювати програма на самознищення комп’ютера. Підприємство врятували несанкціоновані дії (не за інструкцією) персоналу, коли обслуговуючий персонал чи через нестачу валюти, чи через власну допитливість вирішив самостійно розібратися з комп’ютером, за який у свій час було сплачено 3 млн доларів. Виявлена шпигунська

закладка послугувала сигналом до загальної перевірки комп'ютерів цього типу, закуплених у США [21].

### 3.6.3. Відеотехніка в розвідці

Відеотехніка в розвідці почала використовуватися не пізніше, ніж аудіотехніка. Підзорні труби і біноклі з'явилися набагато раніше радіопередавальних і радіоприймальних пристроїв. Крім них до цієї групи технічних засобів відноситься фотографічна й телевізійна техніка.

“Ми, наприклад, — пише В. Шелленберг, — могли зменшити при фотографуванні цілу газетну сторінку до розмірів голівки звичайної шпильки. Після збільшення текст на фотографії читається зовсім вільно. При фотографуванні за допомогою таких камер можна було цілі томи документів умістити на плівці розміром трохи більше сантиметра. Багато разів, коли мені доводилося їздити по різних країнах без права дипломатичної недоторканності, я ховав такі плівки в отворі порцелянового зуба”. [98]

Широке використання в розвідувальній роботі фото- і телевізійної техніки забезпечила їх мініатюризація і висока здатність. Фотоапарат можна вмонтувати в запальничку, портсигар, навіть окуляри. А здатність відеотехніки сьогодні така, що із супутника, який пролітає, можна ідентифікувати фігуру людини, а з літака — розшифрувати назву газети, що він тримає в руках.

Для цілей розвідки використовуються мініатюрні відеокамери і відеомагнітофони. Розміри відеокамер визначаються декількома сантиметрами, а вага — 15–30 грамами. Наприклад VPC-715 (PAL) має габарити 42x84x12 мм, вагу 30 г, а відеомагнітофон OVS-9–148x130x62 мм і вагу 670 г [16].

Відеокамери і відеомагнітофони можуть використовуватися для спостереження усередині приміщень і зовні. Вони можуть встановлюватися нерухомо і фіксувати об'єкти, що попадають у їх “поле зору”, а можуть використовуватися з пристроями дистанційного керування. В останньому випадку можливості спостереження з їхньою допомогою підвищуються.

Для застосування пристроїв відеоспостереження в умовах недостатньої освітленості використовуються інфрачервоні освітлювачі, що можуть бути або самостійними пристроями або вмонтованими у відеокамери і відеомагнітофони. Їхнє застосування ще більш розширює можливості відеоспостереження.



У свій час преса повідомляла про те, як відомому американському бізнесмену Гемблу, співвласнику знаменитої “Проктер енд Гембл” з нагоди було подароване опудало крокодила. Подарунок був так прекрасно виконаний, що хазяїн прикрасив ним свій кабінет. Дружина Гембла звернула увагу на те, що крокодил якось дивно “дивиться” на неї. Але це спочатку було залишено без уваги. Через кілька тижнів під наполегливим впливом жінки провели “вівісекцію” крокодила, і виявилось, що замість очей йому були вмонтовані мініатюрні телекамери, що протягом декількох тижнів передавали поряд із секретами подружнього життя ще й зображення секретних документів з особистого кабінету Гембла [46].

З низько пролітаючих літальних апаратів можуть фотографуватися технологічні процеси, устаткування і продукція, вироблена на підприємствах. Причому це не обов'язково можуть бути легкі літаки чи вертольоти. Найчастіше для подібних цілей використовуються великі радіокеровані моделі літальних апаратів, здатні транспортувати мініатюрну відеотехніку [46].

### 3.6.4. Комп'ютерна розвідка

Одним із найбільш плідних об'єктів одержання інформації є комп'ютер. Особливістю сучасної економіки є комп'ютеризація всіх сторін її функціонування.

У багатьох країнах створені комп'ютерні системи, що обслуговують оборону, статистичні, податкові органи, медицину, науку і т.ін. Деякі з них об'єднані в міжнародному масштабі, такі як “Інтернет” та ін. У цих системах циркулює найцінніша інформація. Сьогодні по міжнародних комп'ютерних системах проводяться телеконференції, переговори, обмін науково-технічною інформацією, досє по кримінальних суб'єктах тощо. Кожна з перерахованих складових частин становить значний інтерес для розвідки взагалі й економічної зокрема. Крім того, навіть якщо цінна інформація і не надходить у систему, то система служить каналом, по якому представляється можливість проникнути в комп'ютер і скопіювати інформацію, що зберігається в ньому [30, 77].

Розвиток комп'ютеризації і розширення можливості викрадення інформації. Високий рівень розвитку комп'ютерних систем не тільки полегшує умови життєдіяльності людини, а й створює нові, практично необмежені, можливості шпигунства. Очевидно, що це протиріччя розвитку, і цим протиріччям з успіхом користуються.

Як відзначають Ю. Батурін і Л. Жодзішский, рівень розробки проблем комп'ютерної злочинності і правове відображення його ще настільки

низькі, що, за оцінками фахівців, тільки один з десяти комп'ютерних злочинів виявляється методами цілеспрямованого контролю, а решта — випадково. Не треба бути фахівцем, щоб зробити висновок: які широкі можливості представляє комп'ютерне шпигунство з огляду на забезпечення доступу до найціннішої інформації [21].

### **Умови, що сприяють проникненню в комп'ютерні мережі.**

1. Комп'ютерне шпигунство важко кваліфікувати як злочин. Якщо розкрадання товару чи навіть документа легко або відносно легко кваліфікувати, то розкрадання інформації, що знаходиться в комп'ютері, не спричиняє видимого матеріального збитку. Припустимо, знята копія з програми чи бази даних. Якщо доступ до комп'ютера погано контролюється, власник його навіть не помітить вчиненого. Отже, факт витоку інформації найчастіше залишається прихованим від потерпілого.
2. Процес розкрадання інформації, не враховуючи підготовчої роботи, може займати дуже мало часу: секунди чи навіть невеликі частки секунд, тоді як звичайне розкрадання з проникненням чи вербуванням агента займає незрівнянно більше часу.
3. Складність визначення розміру збитку, заподіяного розкраданням інформації, що міститься в комп'ютері. Викрадач інформації може ввести в програму додаткові команди, які ховають факт розкрадання, чи "віруси", "бомби", що руйнують програми і бази даних.
4. При кваліфікації комп'ютерних злочинів важко відокремити намір від необережності. Програми нерідко містять помилки, що виявляються не відразу, вони певний час знаходяться в "сплячому" стані і виявляються при деякій комбінації умов використання, що не можуть бути передбачені заздалегідь. Ці помилки можуть призводити до витікання інформації, подачі інших команд по розподілу доходів і т.ін., що слугує прекрасним прикриттям для шпигунства.
5. Розслідування комп'ютерних злочинів найчастіше буває не менш дорогою справою, ніж заподіяний збиток. Нерідко власники комп'ютерів намагаються уникнути збільшення своїх втрат, тоді як можливість покриття цього збитку залишається дуже проблематичною.
6. Сам факт розкрадання програмного забезпечення і бази даних, що містяться в комп'ютерах, нерідко приховується обслуговуючим персоналом, тому що він кваліфікує їх професійно неспроможність.

Усе відзначене істотно полегшує комп'ютерне шпигунство, робить його більш ефективним [46].

**Методи проникнення в комп'ютерні мережі і комп'ютери.** На тлі сприятливого середовища комп'ютерної злочинності сформувалися і свої методи проникнення в комп'ютерні мережі та комп'ютери [31].

В умовах недосконалості відповідальності за комп'ютерні злочини таке несанкціоноване входження в мережі і бази даних, копіювання програм та іншої інформації найчастіше розглядається майже як дрібне хуліганство, чим і користується економічна розвідка.

Ось простий приклад з “Комерсанта” №33 за 1992 рік.



Програмісти із Санкт-Петербурзької організації “Севзапмонтажавтоматика”, роздобувши телефон “Спринт-Сеть” російської філії міжнародної корпорації “Sprint International”, що володіють розгалуженою світовою мережею комунікаційних послуг, склали оригінальну програму підбору паролів за допомогою якої довідалися коди входу в російський сегмент комунікаційної мережі. Знову підбравши паролі, вони проникли в конфіденційні бази даних американських і канадських клієнтів корпорації “Sprint International”. Розслідування показало, що базами даних хакери користувалися протягом п'яти годин комп'ютерного часу. Керівники “Севзапмонтажавтоматика” відмовилися від співучасті в проникненні, хоча, на думку фахівців викрадена база даних могла бути використана для розробки власних замовлень. Сплативши відносно невелику суму — 30 тис. руб. за використання мережевого часу “Спринт-Сеть”, “Севзапмонтажавтоматик” уник якої-небудь іншої відповідальності [84].

Хитромудрі системи безпеки усе-таки переборні, іноді навіть мало-кваліфікованими хакерами. У 1994–95 рр. ВМС США провели перевірку безпеки 757 інформаційних систем і мереж. До них допустили, у навчальному порядку, хакерів. Вони домоглися повного контролю над 266 системами (тобто 36%), ще увійшли в 96 систем. Отже, кожна друга система була зламана. Лише кожне третє проникнення (всього 117) було виявлено. З 117 виявлених проникнень обслуговуючий персонал заявив тільки в декількох випадках [71].

Кваліфіковані фахівці проникають у комп'ютерні мережі з чітко визначеними цілями. Нещодавно правоохоронні органи Росії, Великобританії, Німеччини, Ізраїлю і Нідерландів знешкодили велику міжнародну групу комп'ютерних зломлювачів, які проникли в систему “Сіті-бенк”, яка має філії в 96 країнах світу. На основі сорока підроблених документів, посланих через зламану систему захисту комп'ютерної

мережі, вони зняли з рахунків різних клієнтів понад 10 млн доларів США [46].

Несанкціоноване проникнення в комп'ютерну систему може здійснюватися шляхом видачі себе за законного користувача, якщо система не має засобів автентичної ідентифікації (за голосом, сітківкою очей, відбитками пальців і т.ін.). Ідентифікуючі шифри, коди тощо здобуваються шляхом підкупу обслуговуючого персоналу, у погано охоронюваних місцях зберігання, при прослуховуванні телефонних ліній і т.ін.

Проникнути в комп'ютерну мережу допомагає недбалість програміста, коли допускаються спрощення при угрупованні даних, порушується логічна послідовність і т.ін., тобто все те, що має місце при складанні великих програм. Іноді в таких величезних програмах спеціально залишаються “прогалини” для того, щоб у майбутньому програми можна було розвинути. Через подібні порушення логічних послідовностей і прогалини можна проникнути в програму, одержати необхідну інформацію і вставити в прогалину чи логічну паузу, одну чи кілька команд на постачання інформації, продукту, чи вибух системи для приховання слідів, як це було передбачено в програмах комп'ютерів “Вакс” [46].

Вставка в прогалині програм інших команд називається “троянським конем”, “логічною бомбою”. Різниця між ними полягає в тому, що в першому випадку нові команди в програмі починають працювати відразу (наприклад віддавати інформацію, перенаправляти потоки продуктів, доходів і т.ін.), а в другому — після проходження визначеного відрізка часу чи при настанні визначеної комбінації умов [46].

Особливе місце в економічному шпигунстві займає збір інформації про персонал конкуруючої фірми.



Колишнього кандидата в президенти США Г. Харта вдалося усунути, коли на основі аналізу покупок по кредитній картці встановили, що придбана жіноча білизна за розмірами відповідає не дружині, а коханці [46].

Комп'ютерна інформація також може зніматися без проникнення в комп'ютерну мережу або базу конкретного комп'ютера радіоприймальними пристроями на відстані в кілька десятків метрів, шляхом запису електронних сигналів з наступною їх розшифровкою.

### Питання для самоконтролю

1. Економічне шпигунство як фактор в конкурентній боротьбі.
2. Взаємозв'язки різноманітних видів розвідок.
3. Ефективність розвідувальної роботи.
4. Можливі канали витікання інформації підприємства.
5. Об'єкти економічного шпигунства.
6. Потенційні викрадачі комерційних секретів.
7. Економічна оцінка можливих наслідків втрати економічної інформації.
8. Класифікація методів економічного шпигунства.
9. Перелік мінімальних відомостей про ділових партнерів у конкурентів.
10. Анкета ділового партнера. Склад, призначення.
11. Анкета конкурента. Склад, призначення, застосування.
12. Комп'ютерне шпигунство.
13. Використання аудіо- і радіотехніки в розвідувальній роботі.
14. Цілі використання відеотехніки.
15. Використання комп'ютерної техніки.
16. Розвиток комп'ютеризації і розширення можливостей викрадення інформації.
17. Умови, що сприяють проникненню в комп'ютерну мережу.
18. Методи проникнення в комп'ютерні мережі і комп'ютери.

## **Розділ 4. СИСТЕМА ЗАХИСТУ ПІДПРИЄМСТВА**

Вивченню даної проблеми приділяли увагу багато авторів, які розглядали питання класифікації заходів захисту, способів захисту, проблеми захисту комерційної таємниці, економічної безпеки та безпеки підприємництва. Найбільш чітко та цікаво для сприйняття питання економічного захисту підприємства викладені А.А. Чернявським [93] та В.Е. Духовим [46], бачення яких в основному наведено нижче.

### **4.1. Загальні положення і класифікація заходів захисту**

Під безпекою підприємства розуміється стан його стійкої діяльності, при якому реалізуються його програми, забезпечуються прибуток і захист від зовнішніх і внутрішніх дестабілізуючих чинників.

Безпека підприємства повинна забезпечуватися за такими напрямками [93]:

- економічна безпека, включаючи комерційну;
- науково-технічна безпека;
- фізична безпека;
- соціальна безпека.

➔ Дестабілізуючі чинники — це реальні або потенційні дії, які заподіють або можуть заподіяти шкоду діяльності підприємства або зробити її неможливою. [93]

До зовнішніх дестабілізуючих чинників відносяться:

- зміни законодавства, введення нормативних державних актів, які припиняють, гальмують підприємницьку діяльність або роблять її неможливою;
- дія криміногенних структур;
- недобросовісна конкуренція.

До внутрішніх дестабілізуючих чинників відносяться:

- промислове і комерційне шпигунство;
- соціальні потрясіння;
- незадовільна організація управління підприємством.

Система заходів забезпечення безпеки підприємства включає сукупність державно-правових, адміністративних, режимних заходів, організацію попереджувально-профілактичної роботи з персоналом, фізичну охорону об'єктів і працівників підприємства, впровадження технічних засобів захисту від промислового і комерційного шпигунства.

Заходи по забезпеченню безпеки підприємства можна підрозділити на дві групи [93]:

1. Заходи загального забезпечення безпечної діяльності і функціонування підприємства, покликані попереджати і утруднювати можливість негативної дії на діяльність підприємства будь-якого з дестабілізуючих чинників.
2. Заходи, направлені безпосередньо на боротьбу з ворожою діяльністю конкурентів; їх призначення — виявляти, локалізувати і не допускати конкретних ворожих дій конкурентів.

Група заходів загального забезпечення безпечної діяльності і функціонування підприємства включає:

- а) державно-правові заходи;
- б) адміністративні заходи;
- в) заходи, здійснювані службою безпеки підприємства.

**Державно-правові заходи** покликані забезпечити безпеку підприємства в правовому відношенні на державному рівні.

- ⊙ *На практиці державно-правові заходи можуть бути реалізовані за допомогою організації вивчення державних і нормативних актів по захисту підприємства державними органами. З цією метою на підприємстві створюється юридично-правова служба, яка відстежує інформацію в галузі забезпечення захисту підприємств. [93]*

У першу чергу вивчаються законодавчі і нормативні акти — закони, постанови Верховної Ради, укази Президента; потім аналізуються підзаконні акти міністерств і відомств щодо захисту й забезпечення безпеки підприємств. Вивчаються проблеми захисту підприємств від зовнішніх дестабілізуючих чинників. Аналізуються матеріали засобів масової інформації про виникнення потенційних загроз підприємництву внаслідок відсутності законодавчих актів або недоліків законодавчої бази;

вивчається криміногенна ситуація в районах функціонування підприємства і його контрагентів, постачальників та інших суб'єктів економічних відносин. [93]

Керівниками підприємства можуть бути встановлені ділові контакти з депутатами Верховної Ради і представниками державної адміністрації на державному і регіональних рівнях для доведення до їх відома проблем, пов'язаних із захистом підприємств, а також для обговорення питань про внесення необхідних поправок в чинні законодавчі і нормативні акти з питань захисту підприємництва.

**Адміністративні заходи** призначені для забезпечення безпеки підприємства і всіх його співробітників, а також для здійснення контролю виконання встановлених норм і правил, сприяння керівникам різних структур в підтримці встановленого режиму безпеки на об'єктах підприємства. Вони можуть бути реалізовані за допомогою організаційно-правового впливу на діяльність керівників об'єктів і інших структур підприємства в галузі забезпечення захисту цих об'єктів і структур. [93]

**Заходи, здійснювані службою безпеки підприємства** включають в себе [93]:

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

**Режимні заходи** покликані не допустити нанесення збитку підприємству з боку конкурентів. Для цього на об'єктах вводяться різні режими безпеки; розробляються інструкції і положення, які регламентують поведінку працівників і забезпечують захист комерційних інтересів підприємства. Такими документами можуть бути:

- положення щодо забезпечення безпеки об'єктів;
- інструкція, що регламентує перебування працівників на своїх робочих місцях, їх пересування територією, а також контакти між собою;
- інструкція, що регламентує контакти з представниками інших підприємств;
- інструкція по роботі з конфіденційною інформацією.

Контроль виконання режимних заходів забезпечується шляхом проведення планових перевірок і експериментів за оцінкою ефективності функціонування системи безпеки в цілях виявлення недоліків, вдосконалення методів захисту підприємництва.

На підприємстві необхідно організувати *фізичну охорону* території і будівель шляхом їх огороження, встановлення сигналізації, захисту дверей, воріт, вікон, встановлення зовнішніх і внутрішніх постів, захисту окремих приміщень за допомогою встановлення металевих дверей, ґрат, охоронної сигналізації тощо. Необхідно також забезпечити фізичний захист персоналу і керівників підприємства різними методами залежно від криміногенної обстановки.

*Технічні засоби захисту* покликані обмежити можливості отримання інформації про об'єкт структурами економічної розвідки, організованої злочинності і окремими особами. Особливу увагу слід надавати захисту комп'ютерної інформації. Крім організаційно-режимних заходів дана система повинна передбачати своєчасне виявлення встановленої шпигунської техніки шляхом систематичного проведення силами компетентних фахівців інструментальних перевірок приміщень на об'єктах, де можливе отримання конкурентами інформації, що їх цікавить. Слід розробляти і застосовувати додаткові заходи технічного захисту від шпигунства під час проведення переговорів.

*Попереджувально-профілактичні роботи* з персоналом є запорукою успіху загальної системи захисту підприємництва. Вони включають вивчення морально-психологічного клімату на підприємстві, виховання у працівників морально-психологічних якостей, що забезпечують дотримання ними вимог безпеки, відчуття відданості фірмі, здійснення профілактики негативних процесів.

## 4.2. Проблеми захисту підприємницької діяльності та організація захисту в розвинутих країнах

Оскільки комерційне шпигунство становить серйозну загрозу для об'єктів підприємництва, існує невідкладна необхідність забезпечення їх безпеки.

Останніми роками за кордоном простежується стійка тенденція до об'єднання служб безпеки приватних фірм для більш ефективного захисту від комерційного шпигунства і недобросовісної конкуренції.



Наприклад, в цілях боротьби з просочуванням науково-технічної інформації з філіалів американських корпорацій за кордоном була створена єдина спеціальна служба ASIS — Американське співтовариство по промисловій безпеці, що об'єднало керівників служб безпеки найбільших транснаціональних компаній американського походження.

З метою об'єднання зусиль по боротьбі з розповсюдженням підробок відомі французькі фірми, що є до того ж конкурентами ("П'єр Карден", "Шанель", "Крістіан Діор", "Ніна Річчі", "Гуччі"), зробили аналогічні кроки, бо прийшли до висновку, що їх розрізнені спроби подавити підпільних конкурентів позитивного результату не дадуть [93].

Існують й інші міжнародні об'єднання приватних фірм, що займаються захистом підприємств і підприємців від комерційного шпигунства. Найбільш відомі з них "Міжнародна служба безпеки і розслідувань", що об'єднала приватні служби Західної Європи, і "Всесвітня організація детективів".

З початку 90-х рр. у США стала діяти широкомасштабна система колективної безпеки американського бізнесу. З того часу державний департамент і понад 500 корпорацій США регулярно обмінюються інформацією з питань тероризму та інших злочинних дій з метою захисту інтересів американських підприємств і громадян в інших країнах. [93]

➔ Керівники служб безпеки японських фірм мають лінії прямого зв'язку з поліцейськими органами. До кожного підприємства або компанії прикріплений дільничний патрульний поліцейський, який контактує зі службами безпеки.

Діяльність служб безпеки у Великобританії координується спеціальним органом — Британською асоціацією по забезпеченню безпеки в економічній галузі (BSIA), щорічний бюджет якої складає 1 млн. фунтів стерлінгів.

У розвинутих країнах існують різні погляди на функції недержавних підрозділів безпеки. У ФРН діяльність приватних служб охорони підприємств в основному спрямована на попередження правопорушень на виробництві (до 90%). Їх робота складається насамперед з попередження або зведення до мінімуму випадків нанесення будь-якої шкоди виробництву. Друга їх функція — здійснення попереднього затримання правопорушника на місці злочину, а також проведення розслідування з метою виявлення порушень внутрішнього розпорядку та інших протиправних дій, здійснюваних на підприємстві.

Попереджувальна діяльність цієї служби охорони ні в кого не викликає сумнівів, але діяльність, пов'язана із розслідуванням, піддається критиці, оскільки вважається, що вона перетинається з функціями поліції. На великих, а також середніх підприємствах Німеччини у випадку підозри можливості скоєння злочину співробітнику служби охорони

часто доручається здійснення дій, направлених на попередження злочину. При цьому служба охорони підприємства не має права застосовувати заборонені законом прийоми (прослуховування, порушення виробничої таємниці) та здійснювати процесуальні дії, що є прерогативою поліції (допит тощо).

Також проблемним є питання, що стосується обов'язку повідомляти про злочини, скоєні на підприємствах їх співробітниками. Зазвичай заяви надходять на тих співробітників, які “заважають” і яких прагнуть позбутися.

За результатами досліджень німецького Інституту ім. М. Планка, приблизно про 16,8% злочинів стає відомо на підприємстві. Готовність співробітників повідомляти про скоєні правопорушення вища на невеликих підприємствах, ніж на крупних, які мають більше можливостей для проведення розслідування злочинів. Караються скоювані порушення, як правило, “заводською юстицією”. Тому можна сказати, що головна задача служб охорони підприємства — створення умов для діяльності заводських судів, які в якості санкцій застосовують штрафи, попередження. Від порушників нерідко вимагають врегулювати конфлікт мирним шляхом [93].

У ФРН неодноразово висловлювалася думка про те, що служба охорони підприємств повинна скласти з себе повноваження щодо розслідування і передати їх поліції. Показово, що жоден інший інститут приватної служби безпеки не піддається такій жорсткій критиці з боку громадськості Німеччини, як служба охорони на підприємствах. [93]

Американські дослідники виділяють три функціональні області діяльності недержавних підрозділів безпеки [93]:

- захист інформації;
- захист персоналу;
- фізичний захист.

Служби промислової і комерційної безпеки США в числі інших функцій контролюють також характер і обсяг торговельно-економічних і науково-технічних обмінів фірм США і третіх країн з іноземними партнерами; встановлюють неофіційні відносини з керівниками місцевих фірм, особливо з представниками їх експортних відділів; підтримують контакти з місцевими митними органами, а також спецслужбами; поширюють в місцевих ділових колах, у тому числі через торгові палати й інші союзи і об'єднання підприємців, списки Консультативної ради із забезпечення безпеки за кордоном, матеріали її сесій і засідань окремих підкомітетів, рекомендації адміністрації США щодо обмеження поставок в ті або інші

країни новітньої технології і техніки; протидіють іноземним спецслужбам в їх зусиллях по добуванню науково-технічної і економічної інформації.

В КНР недержавні служби безпеки наділені функціями, що дають право [93]:

- організувати фізичну і технічну охорону промислових і торгових підприємств, місць зберігання матеріальних цінностей;
- здійснювати охорону окремих громадян і їх особистого майна;
- проводити консультації з питань захисту від злочинних посягань;
- забезпечувати безпеку виставок, ярмарків та інших заходів;
- забезпечувати протипожежну безпеку об'єктів;
- придбавати, встановлювати, експлуатувати необхідні для охорони об'єктів технічні засоби.

Фахівці відзначають, що останнім часом коло завдань, які вирішуються приватними службами безпеки, значно розширилося. Разом з чисто поліцейськими функціями — такими, як захист життя і власності громадян, попередження і розкриття злочинів, контроль за станом транспортних засобів — у компетенцію приватних розшукових агентств входить також забезпечення пропускну режиму; попередження пожеж і просочування секретної комерційної інформації; виявлення осіб, що займаються промисловим і комерційним шпигунством; вивчення фінансового становища конкуруючих фірм; перевірка службовців фірм і компаній (даних про їх освіту, минулу роботу, судимості і банкрутства, особливо відносно осіб, що претендують на посади, пов'язані з матеріальною відповідальністю); добування чисто комерційної інформації; розслідування правопорушень, пов'язаних з виходом з ладу устаткування, порушенням технологічного процесу, псуванням машин, крадіжкою інструментів і устаткування на підприємствах; розшук осіб за дорученням клієнтів. Виконання такого кола завдань під силу лише професійним працівникам. От чому в США і Великобританії багато службовців приватних розшукових і охоронних агентств — колишні співробітники поліції, а часто — державних розвідувальних служб. Так, в агентстві “Секюрітор” у Великобританії працюють колишні співробітники служби безпеки — розвідники вищої кваліфікації [93].

У США координація діяльності приватних служб безпеки і поліції здійснюється в таких формах:

- спільне проведення окремих заходів;
- обмін деякою оперативною інформацією;
- спільного використання оперативних сил і засобів;
- підготовка кадрів.

Останніми роками спецслужби США передали приватним, в основному промисловим, службам безпеки значну кількість спецтехніки — телефонні декодери, радіопередавальні станції і системи, установки електронного контролю за об'єктом спостереження.

В США обговорюється питання про створення спеціального органу, який координував би роботу поліції і приватних агентств служби безпеки і визначав сфери їх дій. Передбачається, що роботу такого органу можна побудувати за зразком Міжнародної асоціації промислової безпеки (МАПБ), яка є недержавною координуючою організацією. В її діяльності, окрім співробітників приватних служб безпеки, беруть участь і професійні поліцейські. Ця організація користується великим авторитетом також у державних правоохоронних органів [93].

### **4.3. Завдання забезпечення захисту підприємництва в Україні**

В Україні назріла необхідність створення системи безпеки недержавних об'єктів економіки.

Метою її створення є формування високопрофесійної розгалуженої структури, здатної забезпечити скоординоване ефективне функціонування спеціального блоку забезпечення безпеки економічної системи країни в її недержавній сфері, і виведення її на рівень, що відповідає потребам економіки.

Завдання системи забезпечення захисту підприємництва [93]:

- участь в реалізації державних програм у сфері забезпечення безпеки функціонування економіки;
- створення і забезпечення функціонування спеціалізованого інформаційного фонду комерційних організацій з питань безпеки їх діяльності;
- розробка і впровадження ефективного механізму захисту капіталів і матеріальних засобів підприємств;
- сприяння в регулюванні діяльності недержавних структур, що працюють в галузі безпеки, з питань, що зачіпають інтереси окремих комерційних підприємств і держави в цілому;
- надання допомоги в діяльності державних структур щодо проблем інформаційної безпеки;
- всебічний захист інтересів вітчизняних підприємців в їх взаємостосунках із іноземними фірмами;

- розв'язання проблем безпеки в промислово-фінансових групах;
- розв'язання проблем міжоб'єктного обміну конфіденційною інформацією;
- сприяння у вдосконаленні нормативно-правової бази безпеки підприємництва;
- участь в інспекції комерційних структур з питань безпеки;
- розв'язання складних, неординарних і суперечливих проблем, пов'язаних із забезпеченням безпеки діяльності економічної системи країни, а також груп підприємств і окремих об'єктів;
- виконання спеціальних науково-технічних робіт з питань захисту підприємництва;
- захист інтересів підприємців в законодавчих, виконавчих і судових органах влади з питань захисту підприємництва від економічного шпигунства [93].

Механізм функціонування міжоб'єктної системи безпеки підприємництва повинен передбачати також наявність системи взаємодії зі всіма державними структурами, що мають відношення до вирішення більш широкої проблеми — безпеки держави.

Діяльність міжоб'єктної системи безпеки доцільно налагодити на основі реалізації ряду програм, які повинні охоплювати такі напрями забезпечення безпеки [93]:

- науково-дослідні роботи по організації безпеки підприємництва;
- нормативно-правовий напрям;
- захист міжоб'єктної і внутрішньооб'єктної інформації;
- створення інформаційного фонду по безпеці об'єктів;
- вдосконалення податкової політики держави по відношенню до комерційних структур;
- захист капіталів банків від несумлінних позичальників, кредиторів і конкурентів;
- розвиток системи захисту іноземного капіталу й іноземних інвестицій в економіці держави;
- вдосконалення системи фізичного захисту комерційних структур;
- підготовку кадрів для служб безпеки об'єктів підприємництва.

#### 4.4. Служба економічної безпеки підприємства

Як підкреслював А. Даллес, розвідка завжди вирішує дві задачі: збір інформації про супротивника й охорону власних секретів [40]. Тому фірми, що працюють у ринкових умовах, питанню захисту власних секретів приділяють серйозну увагу. Як повідомляли “Вісті”, західні фірми на ці цілі витрачають до 15% своїх доходів. Західні бізнесмени, знайомлячись наприкінці 80-х рр. з радянськими підприємствами, були дуже здивовані відсутністю в них служб безпеки.

Службу, зайняту охороною власних секретів фірми, зазвичай прийнято називати службою безпеки. В логічному аспекті — служба безпеки — зворотний бік розвідки. Однак, це зовсім не означає, що дані служби варто поєднувати. Навпаки, з огляду на різний характер їх роботи, вони повинні бути відособлені. Це впливає з того, що об'єкти розвідки знаходяться в зовнішньому середовищі підприємства, тоді як об'єкти безпеки — у внутрішньому. Є розходження в методиці організації роботи. Тому, не виключаючи співробітництва між ними в обміні методикою й інформацією, їхню роботу треба спеціалізувати.

Законодавства багатьох держав СНД дозволяють організацію таких служб на підприємствах, у банках і т.ін. Протириччя полягають у тім, що ці служби не мають достатнього правового статусу. Сюди нерідко беруть “хлопців” зі сталевими м'язами, але які не мають відповідної правової підготовки, права на носіння і застосування зброї, не наділених правами працівника правоохоронних органів у частині затримання злочинців. Рішення цих проблем треба шукати на законодавчому рівні, перетворюючи служби безпеки організацій у позаштатні відділи органів правопорядку. Це дозволило б наділити їх мінімальними правами стосовно носіння і застосування зброї, затримання злочинців і, найголовніше, поставити під контроль правоохоронних органів [22].

##### **Методологічні підходи до організації економічної безпеки фірми**

Безпека організації визначається безліччю “загроз” у процесі її взаємодії з зовнішнім середовищем і розвитком внутрішнього середовища [85].

**Загрози зовнішнього середовища:** постачальник може зірвати договір, а покупець відмовитися від замовлення, недоброчесний конкурент може зробити диверсію, майно й інформація можуть бути викрадені, співробітник також може бути викрадений разом з інформацією.

**Загрози внутрішнього середовища:** недотримання технологічних режимів (вибухи, пожежі, інфекції та ін., зараження середовища); недотримання режиму роботи організації і режиму комунікацій (витік інформації).

Суть захисту зводиться до нейтралізації і запобігання загрозам, а якщо таке трапилось, то до відшкодування збитку. Спочатку визначаються об'єкти захисту. У якості таких можна виділити [46]:

1. Інтереси організації (вони визначені її місією, стратегією і цілями). Ці інтереси виявляються у відносинах з держорганами, партнерами, посередниками, громадськістю і засобами масової інформації.
2. Наступним об'єктом є власність організації, що служить одним з визначальних засобів досягнення цілей і реалізації інтересів. Формою власності є всі економічні ресурси, що належать підприємству, за винятком персоналу: будинки, споруди, устаткування, готова продукція тощо.
3. Також важливою формою власності, що служить одним із найбільш бажаних об'єктів викрадення у сучасних умовах, є інформація.
4. Однією з форм власності, охорона якої має принципове значення, є технології (які мають правовий статус і не мають його патенти, ліцензії, ноу-хау і т.ін. — як, наприклад, технологія “кока-коли”).
5. Важливим об'єктом захисту є економічні, кооперативні та інші зв'язки з партнерами. Вони вимагають захисту від зазіхань конкурентів, що завжди прагнуть їх порушити. Також необхідно виключити з цих зв'язків недобросовісних партнерів. У цьому напрямку служба безпеки працює разом з розвідкою.
6. Продукція і послуги, що поставляються організацією споживачам.
7. Транспортні засоби і вантажі, що транспортуються.
8. Персонал, що є носієм інформації.

Відзначені об'єкти захисту охороняються різними способами, серед яких можна виділити, як основні, наступні [60]:

1. **Юридичний захист.** Він покликаний охороняти законні права фірми і її співробітників у взаєминах з державою, юридичними і фізичними особами в карному і цивільному правових полях.
2. **Економічний захист** передбачає врахування економічних інтересів фірми у взаєминах з державою, фізичними і юридичними особами при оформленні відносин постачання, реалізації, інвестицій і платежів.

3. **Фізичний захист** передбачає припинення дій фізичних осіб, спрямованих на грабіж і розкрадання власності й персоналу, спроб нанесення збитку руйнуванням власності, технологій, комунікацій тощо.
4. **Інформаційний захист** передбачає визначення секретної інформації й організацію комунікацій, що запобігають її витіканню.
5. **Технологічний захист** передбачає забезпечення унікальності продукту чи послуги фірми.
6. **Організаційний захист** передбачає відпрацьовування процедур і режимів, що виключають нанесення збитку фірмі шляхом розкрадань власності, технологій, інформації тощо.
7. **Соціально-психологічний захист** передбачає виховну роботу в колективі по створенню атмосфери патріотизму, відданості інтересам фірми.

### Організація служби економічної безпеки фірми

Склад і структура служби безпеки організації визначаються двома факторами [46]:

- 1) потенційним складом і структурою загроз;
- 2) фінансовими можливостями організації.

Перед тим, як створювати службу безпеки організації, необхідно сформулювати модель загроз організації. У цій моделі повинні бути визначені загрози, варіанти захисту і відповідальні за організацію захисту. Вище ми виділили можливі джерела загроз з боку зовнішнього і внутрішнього середовища. Їх комбінація, наприклад, для банку і для кондитерської фабрики можуть бути різними (табл. 1).

Таблиця 1

### Фрагмент приблизної моделі загроз комерційному банку [46]

№ п/п	Джерело загрози	Характер загрози	Можливий захист	Відповідальний за захист
1.	Зовнішнє середовище (злочинці)	Пограбування каси, сховищ	Технічними засобами, охороною	Служба безпеки
2.	Зовнішнє середовище	Одержання грошей за фальшивими Авізо	Технічними засобами, фінансовим контролем	Відділ розрахунків, служба безпеки

3.	Зовнішнє середовище (клієнти)	Одержання кредиту без забезпечення	Контроль позичальника	Фінансова служба
4.	Внутрішнє середовище (персонал)	Привласнення коштів службовцями	Контроль комп'ютерних програм і операцій	Контрольна служба, служба безпеки
5.	Внутрішнє середовище (технології, персонал)	Пожежа	Дотримання режиму. Проти-пожежний захист. Страхування	Служба безпеки, комендант, юридична служба
6.	Зовнішнє середовище (злочинець)	Проникнення в комп'ютерну систему, розкрадання інформації, введення "вірусів"	Зміна програм	Служба безпеки. Програмісти
7.	Зовнішнє середовище (злочинці)	Розкрадання коштів і цінних паперів	Технічні засоби. Охорона	Служба безпеки
8.	Зовнішнє середовище (злочинці)	Викрадення Президента чи керуючого банком	Особиста охорона	Служба безпеки

Ця модель носить навчальний характер. Її можна розширювати, поглиблювати, конкретизувати. Задача її зводиться до визначення потреби і розмірів служби безпеки. Зрозуміло, чим більший об'єкт, тим більше загроз, і тим складніша організація служби безпеки. Другий висновок, який випливає з моделі загроз будь-якої організації, служба безпеки організує свою роботу в тісній взаємодії зі службами внутрішнього контролю, юридичним відділом, відділами забезпечення (програмісти, економісти, фінансисти, господарські служби тощо). Можна в модель загроз включити всі загрози відповідно до приведених вище форм захисту [46].

Звідси визначаються підходи до організації служби безпеки. У маленькій фірмі це може бути одна людина, що, спираючись на фахівців різних профілів, організовує захист фірми. З ростом фірми збільшується і персонал по захисту. У найбільших — ця служба нараховує сотні і тисячі фахівців.

Якщо це середнє підприємство, що нараховує декілька сотень працівників, то воно вже може дозволити собі утримання відділу з 7–15 чоловік. І перша проблема, яку необхідно вирішити, – це структура відділу. З огляду на те, що по окремих напрямках крім служби безпеки до захисту залучаються функціональні підрозділи фірми, загальне керівництво із забезпечення безпеки покладається на одну з перших осіб управління інституціонального рівня – першого президента чи його найближчого заступника.

Безпосередньо у відділі функціональні обов'язки розподіляються за об'єктами захисту: будівлі, територія, майно, продукт, транспортні засоби, інформація, зв'язок, персонал тощо. Крім того, можна спеціалізувати працівників і за способами захисту. Те, що їх діяльність може перетинатися, – це навіть добре. Будь-яка система працює стійкіше, якщо має дублююче забезпечення. Робота організується таким чином, щоб економічні, правові і технологічні методи захисту доповнювали один одного, а не заважали.

Наступна важлива проблема – це підбір кадрів. Дана робота трохи відрізняється від загальноприйнятих підходів у менеджменті. Насамперед відповідно до структури підрозділу безпеки визначається кількість співробітників і кваліфікаційні вимоги. У невеликих підрозділах це може бути фахівець у 1–2 галузях; наприклад, особиста охорона і технічні засоби захисту; реклама й інформація, технологія та засоби захисту тощо. Якщо дозволяють можливості, то краще підбирати по одному фахівцю чи навіть формувати групи за напрямками роботи [46].

І. Лямін вважає, що в основі пошуку необхідних фахівців повинна лежати особиста рекомендація. Ні в якому разі, якщо ви не хочете одержати “двійника”, не користуйтеся рекламою. Людей, необхідних для охоронної роботи, доцільно шукати серед колишніх працівників служб безпеки і правоохоронних органів держави (доцільно оперативників), для забезпечення технічної, технологічної, правової, економічної і психологічної безпеки доцільно підбирати практичних працівників і наукових співробітників дослідницьких установ [60].

Вимоги, які пред'являються до кандидатур [22, 101].

- *професійний рівень* (з'ясовується в ході бесід, тестування, перевірок);
- *надійність* (шляхом з'ясування думки людей, що близько знають кандидата на його попередній роботі, в місці проживання, навчання тощо);

- *психологічна стійкість*, відсутність хронічних захворювань (перевірка здоров'я);
- *відсутність близьких родичів, знайомих, що працюють у конкуруючих підприємствах і фірмах.*

Якщо кандидат за зазначеними параметрами відповідає вашим вимогам, необхідно правильно оформити трудові відносини. З цим колом осіб їх доцільно оформляти контрактом, у додатках до якого повинні бути чітко визначені професійні обов'язки. Тут також доцільно відобразити вимоги про лояльність і санкції за порушення цих вимог. Зрозуміло, контрактна форма трудових відносин повинна передбачатися Статутом. Тут також повинні обумовлюватися й умови припинення контракту обома сторонами.

Відділ служби безпеки веде роботу самостійно, координуючи її зі службою розвідки. Цими напрямками координації роботи можуть бути:

1. Перевірка фінансової стійкості, платоспроможності й ефективності функціонування партнера.
2. Перевірка добропорядності й інших якостей найнятих на роботу фахівців.
3. З'ясування технологічних можливостей партнерів.
4. Нейтралізація розвідувальної роботи конкурента та інших загроз, виявлених розвідкою.

➔ Декілька важливих висновків [46 ]:

**по-перше**, вартість збережених за допомогою служби безпеки секретів повинна оцінюватися і зіставлятися з ринковими цінами цих секретів. Служба безпеки доцільна доти, поки витрати на охорону даного секрету нижче ринкових цін його купівлі;

**по-друге**, службу безпеки й основні її напрямки повинні очолювати фахівці, що добре знають рівень і ціну таємності найважливіших досягнень галузі;

**по-третє**, межі таємності не повинні перевищувати необхідного рівня, тобто не повинні заважати організації виробничих процесів і рекламній діяльності;

**по-четверте**, служба економічної безпеки повинна постійно стежити за своєчасним розсекречуванням інформації, що втрачає здатність приносити додатковий дохід.

## 4.5. Способи захисту від економічного шпигунства

Способи захисту від промислового шпигунства такі ж різноманітні, як і саме шпигунство. Зупинимося на найпоширеніших з них.

Основою всієї програми захисту від промислового шпигунства, її вихідною точкою можна вважати визначення ступеня секретності інформації та її облік. Але тут виникає нова проблема: такі написи, як “конфіденційно”, “таємно”, “внутрішні матеріали фірми”, тільки привернуть увагу шпигуна. Тому краще використовувати зашифровані позначення, відомі тільки співробітникам фірми, що працюють з секретними матеріалами. Так, фірмові конверти для пересилки секретної інформації можуть мати краї незвичного кольору.

Очевидно також, що шпигуна, який потрапив у приміщення вашої фірми, перш за все зацікавлять документи, підписані вищим керівництвом. Тому кожному представнику адміністративної верхівки фірми можна порадити вибрати певний номер, який він міг би використовувати у внутрішньому листуванні замість підпису (при цьому початкові номери числового ряду використовувати не слід). Керівникам можна порекомендувати дозволяти своїм підлеглим користуватися тільки фірмовими блокнотами з пронумерованими сторінками, які потім слід вилучати і замінювати новими.

Слід також щодня знищувати вміст сміттєвих кошиків. Час від часу слід проводити раптові перевірки наявності фірмових блокнотів, стежити за знищенням можливих джерел інформації і т.ін. Все це навчить працівників уважно ставитись до довірених їм матеріалів. Слід зазначити, що нехтування вказаними правилами може повернутись великими матеріальними втратами.

Не варто також засекречувати всю інформацію, оскільки це може привести співробітників, що працюють з нею, до втрати пильності.

### Способи захисту від економічного шпигунства

Метод шпигунства	Способи захисту
<b>1. Вивчення і аналіз відомостей, що публікуються</b>	<ul style="list-style-type: none"> <li>• Обмеження публікації інформації, яка може бути використана конкурентом;</li> <li>• керівнику або його заступнику слід особисто перевіряти всю інформацію, підготовлену до публікації;</li> <li>• з провідними фахівцями фірми повинні бути укладені інсайдерські договори (див. додаток 2).</li> </ul>

<p><b>2. Вивчення і аналіз продукції, що випускається</b></p>	<ul style="list-style-type: none"> <li>• Пристрої пошкодження виробу при спробі його розбирання;</li> <li>• підписання договору з покупцем про те, що він не застосовуватиме сам і не передаватиме кому-небудь іншому отримане від вас ноу-хау.</li> </ul>
<p><b>3. Вивідання даних у керівництва, фахівців і працівників фірми-конкурента</b></p>	<ul style="list-style-type: none"> <li>• Час від часу нагадувати працівникам про пильність: поширювати серед них брошури, читати лекції, попереджати про неприємності, які можуть відбутися з фірмою у разі просочування інформації, підірвавши таким чином їх особистий добробут.</li> <li>• Із співробітником, якому доведеться працювати з секретною інформацією, слід провести бесіду, в ході якої необхідно:             <ol style="list-style-type: none"> <li>а) ознайомити його з методами промислового шпигунства;</li> <li>б) вказати способи захисту від нього;</li> <li>в) відзначити, яка частина інформації може особливо зацікавити конкурента;</li> <li>г) перерахувати співробітників фірми, з якими можна обговорювати цю інформацію;</li> <li>д) розшифрувати таємні позначення, прийняті в даній фірмі для визначення ступеня секретності інформації;</li> <li>е) нагадати про серйозність наслідків для фірми у разі просочування інформації.</li> </ol> </li> <li>• Встановити працівникам підприємства відсотки від прибутку;</li> <li>• укладення інсайдерського договору (див. додаток 2);</li> </ul>
<p><b>4. Проникнення у фірму конкурента з метою отримання інформації</b></p>	<ul style="list-style-type: none"> <li>• добре організована пропускна система;</li> <li>• особливі перепустки-значки різного кольору або зразка у відвідувачів та працівників;</li> <li>• супроводжувати відвідувачів має фахівець по безпеці;</li> <li>• підписати з відвідувачем “Угоду про конфіденційність” (див. додаток 2);</li> <li>• при прийомі на роботу підписання інсайдерського договору;</li> <li>• перевіряти лояльність працівників.</li> </ul>

<b>5. Технічне шпигунство</b>	<ul style="list-style-type: none"><li>• Використовуються технічні засоби (проти фотографування гамма-промені, для стирання магнітофонних записів над входом створюються змінні магнітні поля);</li><li>• особливо важливі наради можна проводити не в офісі, а, наприклад, на природі (ніхто не повинен наперед знати про обране місце);</li><li>• поставити на вікнах і уздовж стін в приміщеннях, де розташовані ЕОМ, залізні ґрати, це спотворює інформацію, якщо її прочитують з ЕОМ за допомогою супутника;</li><li>• керівники і крупні менеджери підприємств повинні звертати увагу на подарунки, що їм підносяться (може бути встановлений записуючий пристрій);</li><li>• до облаштування приміщень, які необхідно захистити від технічного шпигунства, слід запросити фахівця;</li><li>• бізнесменам, що знаходяться у відрядженні, в процесі переговорів можна порадити обмінюватися записками, які, зрозуміло, слід негайно знищувати.</li></ul>
<b>6. Підкуп співробітників фірми</b>	<ul style="list-style-type: none"><li>• Сприятлива атмосфера в колективі;</li><li>• укладення інсайдерського договору (див. додаток 2);</li><li>• одержання працівником відсотка з прибутку, тісно пов'язуючи свій особистий добробут з процвітанням фірми.</li></ul>
<b>7. Переманювання фахівців</b>	<ul style="list-style-type: none"><li>• Сприятлива атмосфера в колективі;</li><li>• укладення інсайдерського договору (див. додаток 2);</li><li>• одержання працівником відсотка з прибутку, тісно пов'язуючи свій особистий добробут з процвітанням фірми;</li><li>• якщо ваш працівник вже завербований конкурентами, можна спробувати зробити з нього подвійного агента і таким чином дезінформувати конкурента.</li></ul>

<b>8. Спостереження за перевезеннями підприємством сировини, товарів, побічних продуктів виробництва</b>	<ul style="list-style-type: none"> <li>• Фіктивні перевезення;</li> <li>• перевезення вантажів у закритих контейнерах.</li> </ul>
<b>9. Викрадення документів, зразків продукції, креслень</b>	<ul style="list-style-type: none"> <li>• Охоронці, замки, сейфи, паркани й т.ін.;</li> <li>• технічні засоби охорони та стеження;</li> <li>• добре організована пропускна система;</li> <li>• особливі перепустки-значки різного кольору або зразка у відвідувачів та працівників;</li> <li>• супроводжувати відвідувачів має фахівець по безпеці;</li> <li>• підписати з відвідувачем “Угоду про конфіденційність” (див. додаток 2).</li> </ul>

## **4.6. Комплексна система заходів захисту підприємництва**

### **4.6.1. Основні завдання щодо захисту підприємництва**

Безпека підприємства (підприємництва) означає захищеність його від зовнішніх і внутрішніх дестабілізуючих чинників, що дозволяє надійно зберегти і ефективно використати його матеріальний, фінансовий і кадровий потенціал.

Безпеку недержавного об'єкта економіки покликані забезпечувати посадовці об'єкта, його персонал, спеціальний підрозділ безпеки, державні правоохоронні органи й інші структури, що запобігають своєю діяльністю будь-яким порушенням нормального функціонування підприємства.

Під системою заходів забезпечення безпеки підприємства мається на увазі комплекс організаційно-управлінських, правових, спеціальних, соціально-психологічних, режимних, технічних, профілактичних і пропагандистських заходів, направлених на якісний захист суб'єкта підприємництва від зовнішніх і внутрішніх загроз.

#### **Завдання комплексної системи заходів забезпечення безпеки [93]:**

- захист законних прав та інтересів підприємства і його співробітників;
- своєчасне виявлення можливих спрямувань до об'єкта захисту і його співробітників;

- вивчення партнерів, клієнтів і конкурентів;
- виявлення, попередження і припинення можливої протиправної та іншої негативної діяльності співробітників об'єкта захисту на шкоду його безпеки;
- забезпечення збереження матеріальних цінностей і відомостей, що становлять комерційну таємницю підприємства;
- добування інформації для вироблення оптимальних управлінських рішень з питань стратегії і тактики економічної діяльності;
- фізична і технічна охорона будівель, споруд, території і транспортних засобів;
- формування в засобах масової інформації, у партнерів і клієнтури сприятливої думки про підприємство, що сприятиме реалізації його планів економічної діяльності;
- відшкодування матеріального і морального збитку, нанесеного в результаті неправомірних дій організацій і окремих осіб відносно об'єкта захисту;
- контроль за ефективністю функціонування системи безпеки підприємства.

Побудова системи заходів безпеки здійснюється на основі дотримання таких **принципів**:

- законності;
- поваги прав і свобод громадян;
- координації і взаємодії з правоохоронними органами;
- самостійності і відповідальності за забезпечення безпеки підприємства;
- розумної достатності;
- відповідності зовнішнім і внутрішнім загрозам безпеки підприємства;
- передової матеріально-технічної оснащеності;
- прогресивного стимулювання суб'єктів системи захисту;
- компетентності;
- конфіденційності;
- комплексного використання сил і засобів.

**Надійність і ефективність функціонування системи** оцінюються, виходячи з таких фактів: відсутності або своєчасного виявлення спроб несанкціонованого проникнення на об'єкт захисту зі злочинною метою; недопущення фактів витоку, розголошення відомостей, що становлять комерційну таємницю; втрати важливих документів, виробів; попередження протиправних і негативних проявів з боку персоналу об'єкта; збе-

реження матеріальних цінностей, фінансів; припинення насильницьких посягань на життя і здоров'я співробітників об'єкта; попередження надзвичайних подій [93].

Головним критерієм ефективності і якості системи заходів безпеки об'єкта захисту є стабільність його фінансового і економічного розвитку відповідно до намічених планів і завдань.

#### **4.6.2. Системи заходів забезпечення безпеки**

На основі сформульованих вище завдань системи заходів забезпечення безпеки об'єкта, принципів її побудови і функціонування комплексна система заходів безпеки включає такі основні й допоміжні підсистеми.

##### **Основні підсистеми:**

- внутрішня безпека;
- безпека будівель;
- фізична безпека;
- технічна безпека;
- безпека зв'язку;
- комп'ютерна безпека;
- захист комерційної інформації;
- психолого-соціологічна;
- протипожежна безпека;
- безпека перевезень;
- економічна розвідка;
- інформаційно-аналітична;
- радіаційно-хімічна безпека;
- пропагандистське забезпечення;
- експертна перевірка механізму системи безпеки.

##### **Допоміжні підсистеми:**

- дії в критичних ситуаціях;
- нормативні акти служби безпеки (СБ);
- нормативні акти персоналу об'єкта;
- режим зустрічей і переговорів з потенційними замовниками і партнерами;
- взаємодія з правоохоронними органами;
- навчання персоналу об'єкта;
- навчання працівників служби безпеки.

### 4.6.3. Організація захисту об'єктів підприємництва

<b>Організація охорони будівель і споруд</b>	<ul style="list-style-type: none"> <li>• Необхідно визначити місця можливого проникнення сторонніх осіб;</li> <li>• приміщення, де зберігається секретна документація, потрібно відділити від інших приміщень, встановити в них сигналізацію, шафи, що закриваються, і сейфи;</li> <li>• звернути увагу на зони прибуття транспорту, обмежити доступ водіїв до складів;</li> <li>• обмежити доступ до найважливіших ділянок і приміщень (охорона, таблички “Стороннім вхід заборонено”);</li> <li>• перепустки з фотографіями різного кольору (за рівнем доступу).</li> </ul>
<b>Контроль використання фотокопіювальної апаратури</b>	<ul style="list-style-type: none"> <li>• Повністю централізувати процес розмноження документів;</li> <li>• надати конкретному працівникові особисту відповідальність за копіювання;</li> <li>• зайві і браковані копії документів слід знищувати;</li> <li>• ведення журналу обліку копіювання документів.</li> </ul>
<b>Встановлення контролю за відвідувачами</b>	<ul style="list-style-type: none"> <li>• Встановити зони, куди доступ відвідувачів заборонений;</li> <li>• впускати на територію підприємства та випускати лише через одні двері;</li> <li>• супроводжувати;</li> <li>• вести журнал обліку відвідувачів (записувати їх прізвище, ім'я, місце роботи; причини відвідин; осіб, що приймають відвідувача; дату відвідин; час приходу і відходу відвідувача);</li> <li>• якщо відвідувач допущений на секретну ділянку, то перед цим він повинен підписати зобов'язання про нерозголошення секретних відомостей.</li> </ul>
<b>Організація захисту інформації при її обробленні на ЕОМ</b>	<ul style="list-style-type: none"> <li>• Фізична охорона;</li> <li>• обмеження доступу до апаратури і носіїв даних;</li> <li>• обладнання приміщень замками, охороною сигналізацією;</li> <li>• засоби контролю вклучення живлення і завантаження програмного забезпечення;</li> <li>• використання парольного захисту при вході в систему;</li> </ul>

	<ul style="list-style-type: none"> <li>• екранування апаратури і приміщень, експлуатація спеціальної захищеної апаратури;</li> <li>• застосуванням маскуючих генераторів шумів і перешкод;</li> <li>• додаткова перевірка апаратури на наявність компрометуючих випромінювань;</li> <li>• використання процедури аутентифікації (цифровий підпис) абонентів і повідомлень, шифрування і спеціальних протоколів зв'язку;</li> <li>• використанням імуностійких програм і засобів виявлення фактів модифікації програмного забезпечення.</li> </ul>
<p><b>Організація діловодства і контролю за секретними документами</b></p>	<ul style="list-style-type: none"> <li>• Вся інформація підприємства, що має конфіденційний характер, повинна бути задокументована;</li> <li>• всі документи, що містять секретну комерційну інформацію, повинні бути промаркіровані грифами кольорового кодування для позначення секретності документа;</li> <li>• на документі повинно обумовлюватись право користування закритою інформацією, а також порядок і терміни користування;</li> <li>• для обмеження фотокопіювання — використання кольорових етикеток;</li> <li>• система контролю за циркуляцією конфіденційних документів (складання списку осіб, що отримують ці документи; нумерація копій документів; фіксація часу отримання і здачі документів або їх копій);</li> <li>• організація спеціального діловодства з конфіденційними документами, включаючи їх розмноження, розсилку, прийом і облік, групування в справи, зберігання, порядок знищення і перевірки наявності;</li> <li>• порядок допуску та доступу працівників до конфіденційних документів;</li> <li>• журнал обліку документів.</li> </ul>
<p><b>Криптографічний захист інформації</b></p>	<p>Система зміни письма з метою зробити текст незрозумілим для інших — можна використовувати для шифрування невеликих за обсягом відомостей: описи винаходів, технологічних процесів, реквізитів клієнтів, формул тощо.</p>

#### 4.6.4 Програма захисту комерційної таємниці підприємства

На основі опису методів захисту підприємництва, викладених вище, достатньо повно відпрацьовані системи захисту комерційної таємниці підприємств і підприємців.

Програма захисту комерційної таємниці підприємства повинна враховувати всі види комерційної і технічної інформації, що підлягає захисту, потенційні канали витікання інформації, можливі втрати від промислового і комерційного шпигунства. [93]

Програма комплексного захисту комерційної таємниці складається з етапів:

1-й етап	Аналіз і класифікація відомостей, що містять комерційну таємницю.
2-й етап	Складання переліку відомостей, що містять комерційну таємницю підприємства.
3-й етап	Аналіз можливих каналів втрати комерційної таємниці.
4-й етап	Розробка правових документів, що закріплюють права підприємства на комерційну таємницю.
5-й етап	Організація захисту об'єктів підприємства.
6-й етап	Організація захисту інформації при обробленні на ЕОМ.
7-й етап	Організація діловодства і контролю за конфіденційними документами.
8-й етап	Регулювання взаємовідносин про власність на комерційну таємницю.
9-й етап	Економічна оцінка потенційної втрати комерційної таємниці підприємства.
10-й етап	Перевірка дієвості системи захисту комерційної таємниці підприємства.

#### 4.7. Технічні засоби захисту бізнесу

Модель загроз інформаційної безпеки бізнесу породжує не тільки модель її захисту а й попит на технічні засоби. Якщо є технічні засоби одержання інформації, то є такі ж засоби її захисту, обмеження чи доступу до неї.

Процес пошуку пристроїв зняття інформації спецслужбою передбачає такі етапи:

1. Вивчення оперативної обстановки біля об'єкта:
  - а) визначення найбільш імовірних місць розташування закладних пристроїв, ретрансляторів, пультів контролю;
  - б) фіксація підозрілих людей, машин.
2. Перевірка радіоєфіру за межами приміщення:
  - а) розташування пункту контролю радіоєфіру;
  - б) складання карти зайнятості радіоєфіру;
  - в) визначення та відокремлення частот радіостанцій;
  - г) проведення статистичного аналізу підозрілих частот.
3. Перевірка радіоєфіру у приміщенні:
  - а) перенесення пункту контролю радіоєфіру у приміщення;
  - б) складання нової карти зайнятості радіоєфіру. Карта зайнятості радіоєфіру складається при ввімкнутій та вимкненій електриці, при ввімкнутих та вимкнених електроприладах, при опущеній та піднятій телефонній трубці;
  - в) порівняння та аналіз всіх карток зайнятості радіоєфіру.
4. Візуальне обстеження всіх меблів та інших предметів. За необхідності меблі розбираються.
5. Перевірка стін приміщення радіолокатором.
6. Перевірка електротехніки:
  - а) перевірка індикатором поля та частотоміром;
  - б) при виявленні паразитних випромінювань вмикають джерело акустичного звуку і перевіряють ці випромінювання на наявність модуляції;
  - в) при необхідності виконується розбирання апаратури.
7. Перевірка ліній (телефонної, електричної):
  - а) у розрив лінії вмикається резистор;
  - б) за допомогою обладнання аналізується наявність сигналу на резисторі;
  - в) аналіз виконується на частотах до 30 МГц.

Для захисту інформації можливе встановлення спеціального обладнання.

1. Для захисту телефонних ліній використовуються:
  - аналізатори телефонних ліній;
  - прилади активного захисту;
  - скремблери;
  - фільтри;
  - випалювачі засобів зйому;
  - універсальні прилади.

2. Для захисту від радіозакладок використовуються джерела радіошуму.
3. Для захисту від диктофонів використовуються:
  - детектори диктофонів;
  - прилади, що дистанційно стирають запис з касетних диктофонів.
4. Для захисту від лазерного перехвату інформації з віконного скла використовується вібратор скла.
5. Для захисту від передачі інформації через лінію електромережі використовуються:
  - фільтри;
  - джерела шуму з діапазоном частот 50кГц — 300кГц.

До додаткових заходів відносяться:

- демонтаж всіх недіючих електричних кабелів;
- встановлення у мережі водопостачання та тепlopостачання діелектричних муфт;
- контроль оперативної обстановки біля офісу (охорона, встановлення камер).

### **Захист від “жучків”**

Як уже зазначалося, одним із найзручніших зручних способів одержання інформації є радіомікрофони, тобто “жучки” чи “клопи”. Оскільки вони передають інформацію на відстань чи навіть ведуть запис без передачі, у будь-якому випадку має місце радіовипромінювання, виділення тепла і локальні зміни температури. Якщо розвідка удосконалює апаратуру в напрямку зменшення небажаних побічних явищ, зробити їх непомітними, знайти прикриття, то технічна контррозвідка зайнята пошуком слідів технічних пристроїв.

- ➔ Оскільки “жучок” поміщається в який-небудь матеріал навколишнього середовища — стіну, підлогу, стелю, предмети побуту тощо, він може бути виявлений декількома способами:
- 1) просвічуванням за допомогою рентгенівської апаратури;
  - 2) радіолокацією;
  - 3) контролем магнітного поля;
  - 4) контролем теплових випромінювань.

Спеціальні приймачі для пошуку радіопередавачів зазвичай називають сканерами. Багато моделей їх виробляється в США, Німеччині, Япо-

нії, інших країнах і вже продаються на ринках країн СНД за цінами від кількох сотень до десятків тисяч доларів. Відомі Японські сканери IC-R-1; IC-R-100; IC-R-7100; IS-R-9000; AR-3000A та ін. Їх робочі діапазони коливаються від 0,03 до 2036 МГц; чутливість — від 0,2 до 6 МкВ, кількість каналів — від 100 до 1000, а вага — від одного до 20 кілограмів [16].

Дуже ефективним засобом є приймачі-сканери, що можуть автоматично реєструвати пристрої, що підслуховують, протягом 24 годин доби на стрічковому графобудівнику. Для прикладу можна назвати комплекс OSC-500 (OSCOR) компактних габаритів (розміщається в кейсі) чи СРМ-700 (“Акула”), що дозволяє не тільки виявляти “жучки”, а й телефонні закладки та коштує приблизно \$3400, а також багатофункціональні пошукові прилади ST-031 “Піранья” та ST-032.

Для цих же цілей часто використовуються аналізатори спектра. Вони не менш зручні в застосуванні і мають трохи меншу чутливість у порівнянні зі сканерами. Аналізатори спектра виробляються не тільки за кордоном, а й в країнах СНД: Білорусії, Росії, Україні. Відомі аналізатори спектра ZWOB 2, ZWOB 4, СМ-4–21, SR2000 та ін. [16].

Рентгенівська апаратура для пошуку вмонтованих “жучків” побудована на фіксації іншої щільності матеріалів “жучка” у порівнянні з щільністю середовища, в яке він вмонтований. Правда, радянські фахівці, коли будували будинок для посольства США в Москві, ухитрилися навіть у сталеві балки перекриттів умонтувати “жучки”, що за щільністю матеріалу не відрізнялися від щільності балок. Рентгенівська апаратура громіздка і зазвичай використовується рідко, та й лише спеціальними державними контррозвідальними службами [46].

Великі можливості для виявлення “жучків” закладені в тепловізійній техніці. Вже сьогодні тепловізори здатні виявляти зміни порядку 1 мкВт. Вони вже застосовуються в медицині й ветеринарії для визначення осередків захворювань по зміні температури тіла та в інших галузях біології. Використання цих приладів у контррозвідці поки ще не одержало широкого поширення, але є всі передумови їхньої появи в найближчому майбутньому. В даний час відомим і доступним є тепловізор SP Thermo View M3, призначений для виявлення камер, мікрофонів, радіопередавачів.

Мікромагнітофони, що не передають, а тільки фіксують інформацію, відшукуються по полю, що створює електродвигун чи генератор струму стирання. В Росії виробляється подібний детектор PTRD-12, який виявляє звукозаписну апаратуру на відстані 40–60 см, при цьому переборюється навіть “шумове” прикриття закладки. Прилад здатний зафіксувати

сигнал від електродвигуна магнітофона на фоні зовнішніх перешкод, які у тисячі разів переважають сигнал об'єкта пошуку [46].

Для захисту конфіденційних розмов можуть застосовуватись прилади для знешкодження диктофонів типу Шумотрон-5 (барсетка) та Шумотрон-3 (кейс). З появою на ринку цифрових диктофонів, які не підлягають впливу електромагнітних випромінювань, єдиним способом захисту залишається акустичний шум. Прилад MNG-300 створює такий шум в усьому голосовому діапазоні.

Для захисту інформації, що знімається лазерними пристроями, спрямованими ззовні на вікна і стіни приміщень, використовується два прийоми, що вирішують ту саму задачу різними способами. Як відомо, розвідник, направивши промінь на стіну чи вікно, приймає його відображення з усіма коливаннями, що викликані усним мовленням чи працюючими в приміщенні аудіосистемами, телефонами тощо. Завдання захисту зводиться до того, щоб амплітуду коливань скла, бетонної стіни тощо зробити іншою, ніж викликає її людська мова чи відтворюючі її технічні системи. Ефект розбіжності амплітуди коливань викликається двома способами: механічним і електронним. Перший передбачає встановлення віконного скла з товщиною, що змінюється, по всьому полю у приміщеннях, що найбільшою мірою піддані ймовірному технічному (лазерному) впливу. Це не так красиво, коли на перший погляд скло здається бракованим, спотворює світлові промені. Але воно спотворює й амплітуду коливань мови. Тож потрібно вибрати між естетикою шибки чи безпекою приміщення [46].

Якщо ви не бажаєте мати кривих шибок у власному кабінеті, тоді застосовуються електронні модулятори коливань (наприклад TRN-2000).

Оскільки на ринку з'явилися мобільні телефони "Spy GSM phone", які автоматично піднімають слухавку при дзвінку з визначеного номеру та при цьому не дають звукового сигналу і не змінюють зображення на дисплеї, практично будь-який телефон може бути перепрограмований або замінений ідентичною моделлю з встановленою відповідною функцією, після чого прослуховування розмов не становить проблеми, оскільки телефон майже завжди знаходиться поруч. При цьому контроль можна вести з будь-якого місця, де є покриття GSM. На сьогодні придбати такий телефон досить просто: таку функцію мають NOKIA 8850, 8310, 8250, 8210, 7250, 7210, 6610, 6500, 6100, 3390, 3350, 3330, 3315..., SIMENS M50, C55, S55 тощо. Для захисту від знімання інформації через мобільний телефон створені прилади "GSM сейф" (настільна підставка з дерева) та "GSM кейс" (шкіряний чохол для носіння на поясі). Також можуть ви-

користуватись пригнічувачі GSM телефонів типу SRC 300A, SRC 120, SRC-250, SRC-100, SRC-200 в місцях небажаної роботи мобільних телефонів.

### **Відеозахист**

Оскільки в розвідці використовуються фото- і відеозасоби для добування інформації, вони ж застосовуються і для її захисту. Правда, фотографічна техніка для захисту інформації використовується вкрай рідко. Перевага віддається відео- і телевізійним системам (надалі ми їх будемо називати відеотехніка).

- ➔ Відеотехніка використовується для вирішення таких задач:
- 1)** спостереження за проникаючими агентами;
  - 2)** внутрішнього спостереження за співробітниками і працівниками організації;
  - 3)** обмеження доступу до секретів організації.

Насамперед відеотехніка встановлюється там, де найбільш ймовірна поява злочинців, шпигунів тощо. Відео- і телекамери доцільно розміщувати таким чином, щоб вони забезпечували “перехресний” огляд об’єкта. Для внутрішнього спостереження за персоналом також вибираються місця, де найчастіше контактують з іншими особами носії секретної інформації (робочі місця, кімнати відпочинку, бари, кафетерії і т.ін.). Наприклад можуть бути встановлені відеокамери типу ZC-F11CH4, ZC-Y12PH4 або зовнішня швидкісна денна/нічна купольна камера XPOWER-M5.

Відеотехніку для спостереження за проникаючими агентами і власними співробітниками доцільно також встановлювати приховано, що підвищує ефективність її використання. Відкрито встановлюється відеотехніка зазвичай для “відлякування” грабіжників банків, ощадкас, магазинів тощо [46].

Для обмеження доступу до секретних об’єктів використовується променева техніка (рентгенівські, лазерні й інші промені). Наприклад, перетинання лазерного променя може викликати включення механізмів огороження чи локалізації проникаючого агента. Променеві огороження доцільно робити схованими, про них не повинен знати проникаючий агент.

Для реєстрації координат та маршрутів пересування може використовуватись пристрій Super Trackstick. Дана розробка працює в будь-якому місці на планеті Земля, використовуючи сигнали від 24 супутни-

ків на земній орбіті дозволяє вирахувати місцезнаходження з точністю до 2,5 м. Такий пристрій може використовуватись для контролю переміщення комерційного транспорту, особистої безпеки, для накопичення комерційних та наукових даних. Для захисту від подібних систем у випадку необхідності можуть бути використані такі пристрої: GPS-Jammer-002 — захист транспортних засобів (живлення від прикурювача автомобіля); GPS-Jammer-003 — захист об'єктів від систем спостереження (живлення від мережі 220 V), радіус роботи 10–25 м.

### **Захист телефонних ліній зв'язку**

Як один з найпоширеніших засобів зв'язку, телефон і сьогодні є одним із найцінніших об'єктів, за допомогою якого здійснюється комерційна розвідка. Тому захист телефонних апаратів і ліній зв'язку є однією із насущних проблем контррозвідки [16, 59, 68].

- ⊙ *Інформація, що циркулює по телефонній лінії зв'язку, як уже відзначалося, може бути викрадена з телефонного апарата чи з телефонної лінії зв'язку.*

Безпосередньо в телефонному апараті варто контролювати і захищати дзвінковий і мікрофонний ланцюги. Як відомо, акустичні коливання, викликані розмовами в приміщеннях, де є телефонні апарати, через маятник дзвоника впливають на якір електромагнітного реле, мікроколивання якого, у свою чергу, викликають мікроструми в котушках і які можуть бути записані при підключенні до абонентської лінії.

Для захисту телефонних апаратів як правило використовуються пристрої типу “Екран”, “Гранит-8”, “Корунд”, “Грань-300” і т.ін.. Найбільш ефективним методом захисту інформації при веденні в приміщенні конфіденційних переговорів є відключення телефонних апаратів від лінії. До типових пристроїв, що реалізують даний метод відноситься “Барьер-М1”.

Активним методом захисту від витікання інформації по електроакустичному каналу передбачається зашумлення телефонної лінії. Шумовий сигнал подається в лінію, коли трубка покладена, а при піднятті трубки телефонного апарата подача шумового сигналу припиняється. До таких засобів відносяться пристрої МП-1А (захист аналогових телефонних апаратів) та МП-1ЦП-1А (захист цифрових телефонних апаратів).

Велику можливість доступу до інформації, що циркулює по телефонній мережі, дає лінія телефонного зв'язку, оскільки вона може також ви-

користуватись як джерело живлення акустичних закладок, а також для передачі інформації, отриманої цими закладками.

Для захисту телефонних ліній використовуються як прості пристрої, що реалізують один з методів захисту, так і складні, що забезпечують комплексний захист ліній різними методами. На вітчизняному ринку є велика кількість різноманітних засобів захисту, серед яких “SP 17/T”, “КТЛ-3”, “КТЛ-400”, “Ком-3”, “Прокруст” (ПТЗ-003), “Прокруст-2000”, “Гром-ЗИ-6”, “Протон” та інші. Для виведення з ладу засобів несанкціонованого підключення до телефонної лінії використовуються пристрої типу “ПТЛ-1500”, “КС-1300”, “КС-1303”, “Кобра” та ін. Разом із засобами активного захисту використовуються пристрої, що дозволяють контролювати деякі параметри телефонних ліній та встановлювати факт несанкціонованого підключення до них. Наприклад, контролери телефонних ліній “КТЛ-2”, “КТЛ-31” ТА “КТЛ-400” за декілька хвилин дозволяють виявити закладки із живленням від телефонної лінії незалежно від способу, місця та часу їх підключення.

Дуже надійним способом є криптографічні методи захисту телефонних переговорів. В Англії, наприклад, дві найбільші телефонні фірми “Водейфоін” і “Селнет” створили розгалужені мережі цифрових мобільних телефонів (понад 1,2 млн абонентів), підключених до глобальної системи мобільних комунікацій (GSM), що охоплює 40 країн (15 млн абонентів). Кожен цифровий мобільний телефонний апарат, ціна якого в Англії складає, між іншим, 5 ф. ст., забезпечений власним “обертним” кодом, що зашифровує “своїм” кодом кожен окрему розмову [58].

Кодування розмови відбувається за допомогою мікро-ЕОМ, вмонтованої в слухавку. Вона мовний сигнал перетворює у цифровий, котрий передається по мережі. Кодування відбувається щоразу по-новому, тому важко розшифровується. Пристрої, що забезпечують захист, називаються скремблерами, які працюють одночасно в алгоритмі кодування і декодування. Тому скремблери не мають потреби в синхронізації.

Скремблери використовуються не тільки для цифрових, а й аналогових перетворень телефонних розмов. Мова в цьому випадку піддається частотній інверсії, частотній і тимчасовій перестановкам. Звуковий сигнал, займаючи ту ж саму частоту лінії зв'язку, стає нерозбірливим для несанкціонованого абонента. Технічний опис скремблера можна знайти в уже згаданому джерелі В. Адріанова й інших.

### **Захист комп'ютерних систем**

Найбільшу інформаційну цінність представляють комп'ютерні системи [16, 27, 30, 77].

- ➔ Захист комп'ютерних систем здійснюється за декількома напрямками. Найважливіші з них:
1. Організаційні заходи.
  2. Технічні заходи.
  3. Правові заходи.

Кожен з відзначених напрямків захисту комп'ютерних систем має складну внутрішню структуру. Серед організаційних заходів не можна не виділити такі напрямки:

- 1.1. Фізична охорона комп'ютерної системи.
- 1.2. Забезпечення обслуговування комп'ютерних систем.
- 1.3. Управління доступом до комп'ютерної системи.
- 1.4. Створення спеціального програмного забезпечення захисту інформації тощо.

Охорона комп'ютерних систем є першим кроком на шляху управління доступом до комп'ютерної системи. Коли в організаціях було мало комп'ютерів і вони зосереджувались в обчислювальних центрах, контролювалася присутність у центрі осіб, що обслуговують комп'ютери. Тепер персональні комп'ютери знаходяться на багатьох робочих місцях. Тому проблема фізичної охорони комп'ютерної системи стала складовою частиною охорони майна організації взагалі. А головний момент охорони перемістився в галузь управління обслуговуванням і доступом до комп'ютерної системи [46].

Як один з найважливіших моментів забезпечення безпеки обслуговування комп'ютерних систем, слід виокремити виключення випадків ведення особливо важливих робіт однією людиною. Крім того, доцільно сформулювати “взаємоперекриваюче” технічне обслуговування комп'ютерних систем, що також створює обстановку незацікавленості в прихованні фактів порушення режиму комп'ютерної системи.

Серед різних заходів щодо охорони комп'ютерних систем на перше місце висувається проблема управління доступом до системи. Модель доступу до комп'ютерної системи розробляється у формі матриці, де, з одного боку, позначаються об'єкти інформації, а з іншого — суб'єкти, що користуються нею (табл. 2.).

Таблиця 2

## Фрагмент матриці моделі доступу до інформації фірми[46]

Суб'єкти інформації	Об'єкт інформації				
	Особові справи персоналу	Баланс фірми	Торгова мережа	Витрати	Прибутки
Перший президент	Читання, Передача	Читання, Передача	Читання, Передача	Читання, Передача	Читання, Передача
Гол. бухгалтер		Читання, записи, передача	Читання	Читання, записи, передача	Читання, записи, передача
Маркетолог			Читання, записи, передача		
Начальник відділу кадрів	Читання, записи, передача				

У кожному випадку визначаються способи доступу до інформації: читання, запис, передача інформації іншим суб'єктам і т.ін. На підставі моделі доступу розробляються спеціальні технічні засоби забезпечення доступу до комп'ютерної системи [46].

Наступна задача, яка тут вирішується, — це ідентифікація й аутентифікація суб'єктів. Кожен користувач, щоб одержати доступ до системи, повинний ідентифікувати себе, тобто ввести власне ім'я. Комп'ютерна система, зі своєї сторони, повинна встановити: чи той це суб'єкт, за якого він себе видає?, тобто перевірити дійсність (автентичність). Найпростіший спосіб аутентифікації — пароль. У сучасних умовах найчастіше використовується контроль біометричних параметрів власника: сканування голосу, відбитків пальців, роги́вки ока, почерку і т.ін.

Необхідно звернути увагу на наступне: електронні картки користувачів (наприклад “Jouch Memory” чи “Software Security Inc” тощо) при усій своїй оригінальності можуть потрапити в руки третьої особи. У цьому відношенні більш безпечні біометричні системи забезпечення доступу. Щоб проникнути в систему, треба до комп'ютера доставити самого носія закодованих біометричних параметрів. Загальновідомо, що сітківка пальців, роги́вка ока, голос людини настільки унікальні, що не піддаються підробці,

а сучасні технічні засоби їхнього аналізу настільки досконалі, що виключають таку підробку [46].

Сам факт доступу до комп'ютерної системи і процес роботи з базою даних повинен протоколюватися. Кожне спілкування з комп'ютерною системою повинне підтверджуватися протоколом, у якому фіксуються наступні найважливіші параметри:

1. Хто працював (відповідно до допуску).
2. Характер роботи:
  - 2.1. Читання файлів і яких.
  - 2.2. Імпорт інформації в існуючу базу даних.
  - 2.3. Перетворення наявної інформації.
  - 2.4. Перетворення наявної інформації на основі імпортованих даних.
  - 2.5. Експорт інформації.

Ці дії суб'єкта повинні відповідати моделі доступу до інформації. Тому протокол спілкування суб'єкта з комп'ютером повинен бути адекватним і слугувати джерелом для обмеження дій користувача, якщо вони порушують встановлені для нього правила доступу [46].

Варто враховувати той факт, що багато хто утримається від несанкціонованих дій у комп'ютерній системі, знаючи що всі його вчинки протоколюються. Аналіз протоколів, що стосуються випадків порушення режиму доступу і використання комп'ютерної системи дає можливість встановити, чому вони стали можливі, оцінити розміри заподіяного збитку, виявити порушника і вжити заходів щодо недопущення подібного в майбутньому.

Однак не можна не підкреслити, що протоколювання роботи в комп'ютерній системі приведе до значного росту обсягу реєстрованої інформації. Це неминучі витрати щодо захисту інформації.

Проблема, що тут виникає полягає в такому швидкому наростанні обсягу протокольної інформації, що стає неможливим її ефективний аналіз. Це породжує обмеження, пов'язані з продуктивністю комп'ютерної системи. Проблеми, що виникають, вирішуються за допомогою [46]:

- 1) розширення продуктивності комп'ютерної системи;
- 2) застосування вибіркового протоколювання як щодо суб'єктів, так і щодо об'єктів інформації;
- 3) створення спеціальних програм, що аналізують протокольну інформацію.

Коли комп'ютерні системи окремих фірм включаються в електронні інформаційні системи (наприклад використання "модемів"), з'являється нова можливість витікання інформації через лінію зв'язку електронної

пошти. Для захисту інформації, що проходить електронною поштою від однієї комп'ютерної підсистеми до іншої, необхідно використовувати криптографічні методи.

Є велика кількість програм кодування і шифрування інформації, що можуть продаватися разом з операційними системами. Вони перетворюють інформацію, в основному, трьома шляхами:

- методом перестановки, коли символи інформації, що шифрується, в межах заданого блоку переставляються за визначеним правилом, заданим відповідним алгоритмом;
- шляхом аналітичного перетворення, коли інформація, що шифрується, перетворюється за визначеними аналітичними правилами;
- шляхом підстановки, коли символи інформації, що шифрується, замінюються символами іншого алфавіту відповідно до заданого алгоритму. Доступ до алгоритму, що забезпечує шифровку інформації, здійснюється за допомогою ключа, що знаходиться у осіб, які розпоряджаються даним видом інформації. Відомі програмні засоби криптографічного захисту, такі як DES, Return to safe, Diskreet, Programm Protect ver.3.0, ДСТ 28147–89 (Росія) та інші. [16]

Поряд із криптографічним захистом інформації, що циркулює по електронних лініях зв'язку комп'ютерних мереж, виникає необхідність захисту програмних продуктів від копіювання. Як відзначалося раніше, електронні лінії зв'язку комп'ютерних систем дозволяють не тільки “знімати” циркулюючу по них інформацію, а й проникати в комп'ютерні підсистеми і копіювати інформацію, що є в них.

Захист від копіювання здійснюється шляхом перетворення копійованої інформації в непрацездатну чи, знову ж, шляхом шифрування інформації не тільки при передачі по електронній пошті, а й при збереженні в комп'ютері. Для цього створюється спеціальна дискета, на якій зберігаються спеціальні програми, необхідні для копіювання файлів жорсткого диска.

Наприклад, програмний пакет АКТУСОР складається з цілого ряду файлів, що захищають інформацію, яка міститься на жорстких і гнучких дисках. Програмний пакет обмежує доступ і захищає від копіювання файли, які заносяться до відповідного списку, що не дозволяє їх копіювати, видаляти і змінювати. Відомі також програмний пакет “ПРОКОР”, комплекс “ТЕХТПРОТЕКШН” та інші [16].

У рамках загального захисту комп'ютерної інформації особливе місце займають антивірусні програми. Вони досить широко описані в спеціальній літературі.

Але є також шкідливі програми ще одного класу. Від них, як і від вірусів, слід особливо уважно очищувати свої комп'ютерні системи. Це так звані програмні закладки. Такі закладки здійснюють:

- копіювання інформації (паролів, кодів доступу, криптографічних ключів, конфіденційних електронних документів);
- зміну алгоритмів функціонування систем, програм (наприклад, внесення змін в програму обмеження доступу);
- нав'язування певних режимів роботи (наприклад зі збереженням додаткової копії документів).

Універсальним засобом захисту від впровадження програмних закладок є створення ізолюваного комп'ютера, для якого виконані перевірки на наявність закладок системи BIOS, операційної системи, всіх програм, що запускаються.

Виявлення впровадженого коду програмної закладки можливе за допомогою ознак:

- якісних та візуальних — виявлення відхилень в роботі комп'ютерної системи (зміна складу та довжини файлів; старі файли кудись зникають, а замість них з'являються нові; програми починають працювати дуже повільно або завершують роботу занадто швидко, або перестають завантажуватись);
- виявлених засобами тестування та діагностики (ознаки характерні як для закладок, так і для вірусів). Виявляються найчастіше антивірусними програмами.

Конкретний спосіб видалення впровадженої програмної закладки залежить від методу її впровадження в комп'ютерну систему. Цю роботу повинен виконувати відповідний фахівець, який заслуговує довіру.

### **Питання для самоконтролю**

1. Завдання забезпечення захисту підприємництва в Україні.
2. Основні завдання комплексної системи заходів забезпечення безпеки.
3. Принципи побудови системи заходів безпеки.
4. Система заходів захисту підприємництва.
5. Основні і допоміжні підсистеми системи заходів захисту підприємництва.
6. Організація захисту об'єктів підприємництва.
7. Організація діловодства і контролю за секретними документами.

8. Економічна оцінка наслідків втрати комерційної таємниці підприємства.
9. Проблеми захисту підприємницької діяльності.
10. Організація захисту підприємництва в розвинутих країнах.
11. Основні проблеми захисту інформації.
12. Основні засоби захисту від економічного шпигунства.
13. Програма захисту комерційної таємниці підприємства.
14. Засоби захисту фізичних об'єктів.
15. Засоби захисту від радіоелектронної розвідки.
16. Організація служби економічної безпеки підприємства.

# ДОДАТКИ

## ДОДАТОК 1

### АНКЕТА ДІЛОВОГО ПАРТНЕРА

#### I. Загальні відомості про ділового партнера

1. Назва і адреса фірми.
2. Які ділові відносини пов'язують нас з цією фірмою (клієнт, постачальник, спільна діяльність тощо).
3. Рік заснування.
4. Основні напрямки діяльності.
5. Репутація фірми в ділових колах.
6. Розмір статутного капіталу.
7. Форма власності.
8. Довгострокова мета фірми.
9. Короткострокова мета фірми.
10. Фінансовий стан фірми в даний момент.
11. Найменування банків, в яких фірма має рахунки, їх фактичний стан.
12. Виробничі можливості.
13. Умови співпраці, поставок, розрахунків, можливість отримання знижок.
14. Позитивні та негативні сторони співпраці з фірмою.
15. Прізвище, ім'я, по батькові, прізвисько (якщо є) керівників, контактних осіб.
16. Чи є вони співвласником фірми або працюють там за наймом (потрібне підкреслити).
17. Домашня адреса керівників, контактних осіб.
18. Телефони керівників, контактних осіб:
  - службовий;

- домашній;
  - мобільний.
19. Дата і місце народження.
  20. Зріст (приблизно), вага (приблизно). Особливості фізичного стану (приклади: в прекрасній фізичній формі, артрит, болі в спині і т. ін.).
  21. Національність керівників, контактних осіб. Чи є питання про національність для кожного хворобливим?
  22. Яким видом спорту займаються?
  23. Соціонічний тип керівників, контактних осіб. Які працівники вашої фірми є для них:
    - а) дуалами;
    - б) замовниками;
    - в) конфліктерами;
    - г) підзамовними;
    - д) підревізними.

## II. Сім'я керівника, контактної особи

24. Сімейний стан. Прізвище, ім'я, побатькові дружини (чоловіка).
25. Освіта дружини (чоловіка).
26. Коло інтересів дружини (чоловіка), громадська діяльність, членство в яких-небудь організаціях.
27. Діти: імена, дати і роки народження.
28. Освітній рівень дітей.
29. Інтереси, проблеми дітей.

## III. Попередня діяльність керівника, контактної особи фірми-партнера

30. Колишні місця роботи (починаючи з останнього):
  - фірма;
  - адреса;
  - дати (з ... по ...);
  - посада;
  - репутація;
  - чи збереглися контакти, які можуть бути корисні для нас (якщо так, то які).
31. Попередня діяльність у фірмі, де працює на цей час (починаючи з останнього часу):

- посада;
  - дати (з ... по ...);
  - заохочення.
32. Які символи соціального становища є в кабінеті керівника, контактної особи партнера?
33. Кумири, люди, до думки яких він прислухається.
34. Які ділові відносини має із співробітниками нашої фірми?
35. Чи є вони добрими? Чому?
36. Хто з наших співробітників знайомий з керівником, контактною особою:
- прізвище, ім'я, по батькові;
  - тип контакту;
  - характер відносин.
37. Яке уявлення склалося у керівника, контактної особи партнера про нашу фірму?
38. Що з цього:
- йому подобається;
  - не подобається.
39. Чим керівник, контактна особа стурбований більше: благополуччям фірми або власним добробутом.
40. Чи думає керівник, контактна особа про теперішній час, майбутнє, чи згадує минуле?

#### **IV. Особливі інтереси і стиль життя керівника, контактної особи фірми-партнера**

41. Громадська діяльність:
- громадська організація, в якій знаходиться;
- адреса організації;
  - активність в ній;
  - її значення для цієї людини;
- політична партія, членом якої є дана особа;
- адреса;
  - активність в ній;
  - її значення для цієї людини;
- політичні переконання;
- їх значення для партнера;
  - релігія;
  - її значення для даної особи.

42. Конфіденційні відомості, що не підлягають обговоренню з керівником, контактною особою (приклади: розлучення, трагічна смерть батьків і т.ін.)
43. Що (крім бізнесу) керівник, контактна особа приймає близько до серця?
44. Медичний висновок (стан здоров'я на цей час).
45. Захоплення керівника, контактної особи партнера (як він вважає за краще проводити вільний час). (Приклади: жіноче товариство, спорт, спілкування з друзями, театр, азартні ігри.)
46. Яку пресу читає?
47. Чи вживає алкоголь? Який? Скільки? Як реагує, коли спиртне споживають інші? Як виявляється стан сп'яніння у нього самого?
48. Чи палить? Якщо ні, чи заперечує, коли палять в його присутності?
49. Улюблені:
  - ресторан;
  - марки вина;
  - цигарки;
  - страви;
  - автомобілі.
50. Як реагує, коли за нього намагаються заплатити в ресторані?
51. Про що любить поговорити?
52. На кого прагне справити враження і яке?
53. Якими життєвими досягненнями пишається якнайбільше?
54. Які, на вашу думку, цілі керівника, контактної особи фірми-партнера:
  - довгострокові;
  - короткострокові.
55. Розголошення якої інформації керівник, контактна особа бажав би найменше? Чи володіємо ми цією інформацією? Її джерела. Існуючі у нас докази. Якщо таких немає, де їх можна дістати.

## V. Освіта керівника, контактної особи фірми-партнера

56. Середня:
  - місце навчання;
  - час (з ... по ...);
  - результати (характеристика, медаль, диплом з відзнакою та ін.).
57. Вища:
  - місце навчання;

- час (з ... по ...);
  - результати (характеристика, диплом з відзнакою та ін.).
58. Якщо не отримав вищої освіти, чи є це для нього хворобливим?
59. Наукові і друковані праці керівника, контактної особи партнера, винаходи, патенти, науковий ступінь, звання, тема дисертації (якщо є).

## **VI. Діловий партнер і Ви**

60. Чи вважає керівник, контактна особа фірми-партнера, що у нього є якісь зобов'язання відносно Вас, нашої фірми або нашого конкурента? Якщо так, то які?
61. Чи турбує керівника, контактну особу Ваша думка про нього?
62. В чому, на думку керівника, контактної особи партнера, найголовніші проблеми, що заважають Вашій з ним співпраці?
63. Які проблеми адміністративного управління є найбільш терміновими для фірми партнера?
64. Чи існують конфлікти між контактною особою і адміністрацією його фірми?
65. Чи є у нас можливість вирішити ці проблеми? Яким чином?
66. Чи має наш конкурент кращі відповіді на вищенаведені питання, ніж ми?
67. Інші цікаві відомості про фірму-партнера, керівника, контактну особу.

***Прізвище, ім'я, по батькові особи, що склала анкету.***

***Підпис*** \_\_\_\_\_

***Дата заповнення*** \_\_\_\_\_

## АНКЕТА КОНКУРЕНТА

### I. Загальні характеристики фірми-конкурента

1. Назва фірми-конкурента.
2. Адреса правління.
3. Адреси філіалів (якщо є), починаючи з найбільших:
  - 1) ...
  - 2) ...
4. Заявлений розмір статутного капіталу фірми-конкурента.
5. Активи фірми-конкурента (вказати приблизну вартість).
6. Форма власності фірми-конкурента.
7. Власники; найбільші акціонери; холдинг, контролюючий фірму; якщо фірма — філіал, то чий.
8. Рік заснування.
9. Кількість співробітників.

### II. Фінансовий стан фірми-конкурента

10. Якого числа закінчується рік (для зарубіжних фірм)?
11. Розмір прибутку за минулий рік.
12. Розмір доходу за минулий рік.
13. Рентабельність за минулий рік. Якщо рентабельність вища, ніж у нас, за рахунок чого це досягнуто?
14. Тенденції у фінансовій діяльності за останні декілька років.
15. Що-небудь незвичайне у фінансових справах (приклади: зміна виду діяльності, дуже великі відрахування консультативним фірмам та ін.).
16. Характеристика загального фінансового стану фірми.

### III. Ціноутворення фірми-конкурента

17. Рівень цін фірми-конкурента.
18. Політика цін фірми-конкурента.
19. Якщо ціни нижче, ніж у нас, за рахунок чого це досягається?
20. Як фірма реагує на цінову конкуренцію?

#### IV. Кадри фірми-конкурента

21. Який стиль управління прийнятий у фірмі-конкуренті?
22. Яка моральна атмосфера у фірмі-конкуренті?
23. Найбільш важливі для фірми-конкурента співробітники:
  - 1) прізвище, ім'я, побатькові, адреса, телефон, посада;
  - 2) прізвище, ім'я, побатькові, адреса, телефон, посада.
24. Кого з них ми могли б схилити на нашу сторону? Як?
25. Якою репутацією користується фірма як працедавець?

#### V. Становище фірми-конкурента на ринку

26. На які верстви населення розрахована продукція (послуги) фірми?
27. “Чи досягає мети” її реклама?
28. За які сегменти ринку з тих, в яких ми не працюємо, фірма веде боротьбу? Скільки відсотків сегменту вона контролює:
  - 1) ...
  - 2) ...
  - 3) ...
29. За які сегменти ринку (з тих, в яких ми працюємо) фірма веде боротьбу? Скільки відсотків сегменту контролюється:
  - 1) нами, ними;
  - 2) нами, ними;
  - 3) нами, ними.
30. Яку унікальну продукцію випускає фірма?
31. Як охороняються ці ноу-хау?
32. Якість обслуговування клієнтів:
  - сильні сторони;
  - слабкі сторони.
33. З ким з клієнтів у фірми склалися якнайкращі відносини?
34. Втрата яких клієнтів виявилася б для фірми-конкурента найважчою?
35. Хто з працівників фірми-конкурента має на клієнтів найбільший вплив?
36. Чи можемо ми схилити цих працівників фірми-конкурента на свою сторону? Якщо так, то яким чином?
37. Хто найважливіші постачальники фірми-конкурента?

38. Чи можемо ми схилити їх на свою сторону? Якщо так, то яким чином?

## VI. Плани фірми-конкурента

39. Чи прагне фірма-конкурент зберегти свої позиції на ринку або активно розвиватися?
40. У чому полягає довгострокова стратегія фірми-конкурента?
41. У чому полягає короткострокова стратегія фірми-конкурента?
42. Чи не збирається фірма-конкурент придбати яке-небудь підприємство або ж, з чуток, вона може бути сама ким-небудь придбана або поглинена? Як ми можемо уточнити ці відомості?  
Якщо інформація підтвердилася, чи є у фірмах, з якими фірма-конкурент вестиме загальну діяльність, співчуваючі нам працівники (назвати прізвища і посади)?
43. Чи є які-небудь відомості щодо підготовки фірмою-конкурентом нової продукції або нового виду обслуговування? Як ми можемо уточнити ці відомості?

## VII. Престиж фірми-конкурента в діловому світі

44. Охарактеризуйте загалом репутацію фірми-конкурента.
45. Як відзиваються про методи, вживані фірмою-конкурентом, у ділових відносинах?
46. Чи виникали у фірми-конкурента (або у її вищих керівників) які-небудь проблеми юридичного характеру або проблеми, що відображаються на репутації цієї фірми? Коли і які?
47. Чи виділяє фірма (або її материнська компанія) засоби яким-небудь добродійним, громадським або муніципальним організаціям? Якщо так, то яким, коли і скільки?
48. Особиста репутація вищих керівників фірми:  
1) прізвище, ім'я, по батькові, посада, репутація;  
2) прізвище, ім'я, по батькові, посада, репутація.
49. Якої думки про фірму дотримуються у Вашій галузі?
50. Якої думки про фірму дотримуються в наших торгових організаціях?

### **VIII. Джерела інформації про фірму-конкурента**

51. Якими джерелами інформації Ви користувалися, заповнюючи цю анкету?
52. Хто з наших недавно прийнятих на роботу співробітників раніше працював на фірму-конкурента або на її партнерів?
53. Хто з наших партнерів працює зараз або працював раніше з фірмою-конкурентом?
54. В яких друкарських виданнях фірма-конкурент розміщує свою рекламу?
55. В яких друкарських виданнях недавно з'являлася яка-небудь інформація про фірму-конкуренті (вказати номер, назву статті, дату публікації)?
56. З яких ще джерел ми могли б отримати інформацію про фірму-конкурента?

### **IX. Можливості боротьби з фірмою-конкурентом**

57. Чи маємо ми відомості про те, яку інформацію про нас має фірма-конкурент?
58. Які можливі джерела цієї інформації? Як ми могли б їх усунути? Як ми могли б за їх допомогою дезінформувати фірму-конкурента?
59. Кого з партнерів фірми-конкурента ми могли б схилити на свою сторону? Як?
60. Яким чином ми могли б збільшити свою частку на ринках, де працює фірма-конкурент?
61. Чи був випадок, коли ми (або хтось інший) взяли верх у конкурентній боротьбі з цією фірмою? Якщо так, то яким чином вдалося цього досягти?

### **X. Визначення стратегії боротьби з фірмою-конкурентом**

62. Який метод було б варто використовувати в конкурентній боротьбі з цією фірмою (відзначити потрібне):
  - а) корпоративний захват, купівлю;
  - б) цінову конкуренцію;
  - в) проведення більш активної рекламної кампанії;
  - г) компрометацію фірми-конкурента у пресі;

- д) спробу “піймати” фірму-конкурента в питаннях порушення законодавства;
  - е) спробу схилити на свою сторону ділових партнерів або працівників фірми. Яких?
  - є) інші методи.
63. Що потрібно зробити для того, щоб скористатися вибраним методом (-ами):
- а) ...
  - б) ...
  - в) ...
  - г) ...

*Прізвища, імена, по батькові посадових осіб, що заповнювали анкету.*

*Підписи* \_\_\_\_\_

*Дата заповнення* \_\_\_\_\_

**ДОДАТОК 2****Типові зразки організаційно-методичних документів  
системи правового захисту комерційної таємниці  
підприємства****НАКАЗ**

“КТ-конфіденційно”  
(обмежуючий гриф залежить  
від змісту наказу)

“ ” \_\_\_\_\_ 200\_\_р.

№ \_\_\_\_\_

**Про введення в дію Положення  
Про комерційну таємницю підприємства**

В період переходу до ринкової економіки питання забезпечення безпеки та комерційних інтересів підприємства набувають принципово нового значення та будуть вирішуватися в рамках нових правових і організаційних форм.

В цих умовах уся виробнича, господарська, зовнішньоекономічна та інша діяльність підприємства повинна бути спрямована на недопущення витоку інформації комерційного характеру.

Враховуючи викладене, з метою захисту економічних і господарських інтересів, виробничих досягнень, нових видів технологій та наукових досліджень, які потенційно можуть мати велике економічне значення, недопущення безоплатного їх використання конкуруючими фірмами, іншими сторонніми організаціями та установами

**НАКАЗУЮ:**

1. Ввести в дію Положення “Про комерційну таємницю та правила її збереження”.

Усім працівникам підприємства, які мають відношення до комерційної таємниці, послуг комерційного характеру, суворо керуватися цим Положенням. Керівникам структурних підрозділів забезпечити контроль за виконанням підлеглим персоналом вимог цього Положення.

2. Створити за рахунок діючого штату підрозділ економічної безпеки підприємства. Покласти на нього завдання щодо організації захисту комерційної таємниці.

Заступнику директора подати на затвердження Положення “Про підрозділ економічної безпеки” та його штатний склад.

3. Постійно діючій комісії з комерційної таємниці розглянути та виділити наукову, виробничу та господарську інформацію, нові технології, проведення науково-дослідних та виробничих робіт, зовнішньоекономічні аспекти діяльності, послуги тощо, які мають комерційну цінність або перспективу та які підлягають юридичному й режимному захисту.

4. Комісії у своїй діяльності керуватися вимогами ст. 65 Господарського кодексу, ст.ст. 29, 40, 142 КЗпП України, Колективним договором та Правилами внутрішнього трудового розпорядку.

5. Керівнику підрозділу зовнішньоекономічних зв'язків розробити пропозиції та внести в діючі договори з сторонніми організаціями вимоги, які гарантують дотримання права підприємства на комерційну інформацію, заходи захисту важливих відомостей комерційного характеру на період договірних відносин, а також після їх припинення; дії проти третіх осіб та організацій, які зачіпають інтереси сторін; умови перевірки та контролю діяльності партнерів підприємства.

6. Заступнику керівника підприємства підготувати та провести з колективом співробітників підприємства нараду з питань захисту комерційної таємниці в умовах ринкових відносин.

7. Юридичному відділу підготувати довідково-методичні матеріали з питань права про комерційну таємницю, забезпечити ними співробітників, які мають відношення до неї.

8. Підрозділу економічної безпеки разом з юридичним відділом підготувати та провести для співробітників підприємства, з залученням компетентних спеціалістів, лекції та бесіди з питань забезпечення збереження комерційної таємниці.

9. Керівникам підрозділів та служб підприємства надати підрозділу економічної безпеки списки співробітників підприємства, які мають відношення до роботи з інформацією, яка складає комерційну таємницю.

Відділу кадрів разом з підрозділом економічної безпеки оформити договірні зобов'язання з зазначеними особами про зберігання ними комерційної таємниці.

10. Контроль за виконанням наказу залишаю за собою.

***Керівник підприємства*** \_\_\_\_\_

**“КТ-конфіденційно”**  
(при необхідності)

## **Положення про комерційну таємницю підприємства та правила її збереження**

Введено в дію наказом  
№ \_\_\_\_\_ від \_\_\_\_\_ 200\_\_ р.

Перехід на ринкові взаємовідносини припускає нові принципи організації виробничо-господарської діяльності підприємства. Результати цієї діяльності можуть набувати цінність на ринку, а також слугувати предметом комерційної таємниці.

Метою цього Положення є закріплення на основі Господарського кодексу України, Закону “Про інформацію” та інших нормативних актів прав підприємства на комерційну таємницю, на створення системи заходів щодо забезпечення збереження конфіденційної комерційної інформації, захисту інтересів кожного співробітника та всього колективу підприємства від неконтрольованого використання результатів виробничої, господарської та іншої діяльності підприємства, створити умови підвищення зацікавленості підприємства в отриманні прибутку від підприємницької діяльності.

### **1. Загальні положення**

1.1. Комерційну таємницю підприємства складає інформація, яка не є державною таємницею, але пов’язана з науковою, виробничою, економічною, фінансовою, управлінською та іншою діяльністю підприємства, розголошення (передача, витік) якої може нанести шкоду його інтересам, спричинити економічні збитки та втрату вигоди.\*

**Примітка:** комерційною таємницею можуть бути документи, записки, звіти, протоколи, креслення, карти, матеріали, обладнання та інші джерела інформації, які належать підприємству, у вигляді неоформлених або неповних патентів, ноу-хау, результатів наукових досліджень, програмного продукту, а також калькуляції витрат виробництва, структура ціни, тендерні пропозиції, контракти, дані про постачальників

---

\* Пункт 1.1 слід сформулювати, виходячи з особливостей підприємства, видів його діяльності, а також положень ст. 162 Господарського кодексу України.

та клієнтів, відомості про конфіденційні ділові переговори, огляди ринку, маркетингові дослідження, інвестиції та інші відомості, які являють підприємницький інтерес.

1.2. Положення визначає основи захисту наукової, виробничої, господарської, підприємницької та іншої діяльності підприємства, збереження комерційної таємниці, спрямоване на недопущення можливої економічної шкоди як самому підприємству, так і його клієнтам, партнерам.

1.3. Вимоги та правила, які викладені в Положенні, обов'язкові для виконання усіма підрозділами підприємства та їх співробітниками.

1.4. Відомості, які складають комерційну таємницю та які отримані за результатами виробничої, господарської, підприємницької та іншої діяльності, — належать підприємству.

Ці відомості можуть належати декільком підприємствам, установам (юридичним особам). Право володіння, використання та відповідальність за їх розголошення закріплюються у Статуті, установчому та господарському договорі, технічному завданні тощо.

1.5. Право прийняття рішення про використання відомостей, які включають комерційну таємницю, належить керівникові підприємства, який може делегувати це право у письмовому вигляді конкретній особі з числа своїх заступників або керівникові одного з підрозділів.

1.6. На підприємстві щорічно готується “Перелік відомостей, що становлять комерційну таємницю” (надалі — “Перелік”), який розглядається та обговорюється на засіданні постійно діючої комісії з комерційної таємниці, після чого склад, обсяг та термін обмежень затверджується керівником підприємства. У разі потреби до “Переліку” можуть бути внесені зміни та доповнення. Ці відомості не підлягають оприлюдненню до закінчення терміну їх обмеження.

1.7. У випадках зацікавленості підприємства в закріпленні пріоритету отриманого наукового або виробничого досягнення інформація, яка призначена для оголошення, повинна містити в собі мінімум відомостей комерційного характеру, достатній для досягнення цілей публікації. В рекламних матеріалах наявність відомостей, які містять конфіденційну інформацію, повинна бути виключеною.

1.8. Використання для відкритого оголошення відомостей, які містять, конфіденційну інформацію та які отримані на договірній основі, або такі, що є результатом спільної наукової (виробничої) діяльності, можливе лише з дозволу партнерів.

## **2. Механізм визначення інформації, яка складає комерційну таємницю**

2.1. В процесі науково-дослідної, конструкторсько-проектної, господарської, підприємницької та іншої діяльності керівники структурних підрозділів (автор) здійснюють прогностичну оцінку можливості отримання результатів, які можуть мати новизну та складати в наступному предмет комерційної таємниці. Ці відомості у вигляді контрольної картки через підрозділ безпеки передаються в постійнодіючу комісію з комерційної таємниці.

2.2. Підрозділ безпеки веде контрольний облік наданої інформації в журналі “Попередній облік інформації, яка має комерційну перспективу”.

2.3. В ході створення конкурентоспроможної продукції, товарів, послуг, відпрацювання дослідних зразків вивчається патентно-ліцензійна ситуація на основі науково-технічної та патентної інформації, провадиться оцінка їх вартості, можливої економічної ефективності, наявності аналогів, відповідності світовому рівню, конкурентоспроможності, можливої вигідної реалізації на внутрішньому та зовнішньому ринках.

2.4. У позитивному випадку висновки по результатах оцінки викладаються у висновку, в якому відображається предмет комерційної таємниці, термін її дії, коло осіб, які мають право доступу до цієї інформації.

Цей висновок підписується керівником структурного підрозділу, після чого він з усіма матеріалами передається до підрозділу економічної безпеки, який веде їх суворий облік, і направляє в постійно діючу комісію.

## **3. Заходи щодо захисту комерційної таємниці**

3.1. Організація та проведення заходів щодо захисту комерційної таємниці провадяться підрозділом економічної безпеки, права та обов'язки якого визначені окремим положенням.

3.2. Усі письмові джерела інформації, які мають комерційну таємницю, повинні мати обмежувачий гриф (“КТ — суворо конфіденційно”, “конфіденційно” та інші) та підлягають зберіганню в підрозділі економічної безпеки, який здійснює нагляд за використанням інформації, що містить комерційну таємницю.

3.3. В текстах документів та їх реквізитах додатково можуть бути обумовлені права на інформацію, порядок користування нею, терміни обмеження на публікацію та інше.

3.4. По кожній інформації, яка є предметом комерційної таємниці, оформляється тематичне досье.

3.5. Видача досье та документів з відміткою “конфіденційно” дозволяється авторам цих документів або іншим особам за письмовою вказівкою володаря інформації та його безпосереднього керівника.

3.6. При виявленні несанкціонованого доступу до конфіденційної комерційної інформації керівник підрозділу (виконавець) зобов'язаний негайно повідомити підрозділ економічної безпеки.

3.7. При укладанні дво- або багатосторонніх договорів та угод з українськими підприємствами, організаціями й іноземними фірмами про проведення науково-дослідної, виробничо-господарської або іншої діяльності, а також про передачу технологічних рішень дослідних зразків і т. ін., обов'язковою умовою угоди повинно бути додержання конфіденційності.

Змістом такої умови може бути:

- а) зобов'язання сторін щодо попередження розголошення комерційної таємниці;
- б) документи, послуги та інші умови повинні розглядатися сторонами як суворо конфіденційні;
- в) заходи по недопущенню порушень правил користування цими документами та виробами;
- г) зобов'язання сторін, щодо заборони передачі інформації третім особам без попереднього узгодження між сторонами;
- д) зобов'язання сторін ознайомлювати з договором суворо обмежене коло своїх співробітників.

3.8. Передача інформації, яка має комерційну таємницю, стороннім організаціям можлива лише на підставі договору або контракту.

3.9. Від осіб, які допущені до ознайомлення з конфіденційною інформацією, береться письмове зобов'язання про нерозголошення комерційної таємниці та проводиться ознайомлення з мірою відповідальності за порушення цих зобов'язань. Заявку з обґрунтуванням необхідності оформлення зобов'язання подають голові підрозділу економічної безпеки керівники структурних підрозділів.

3.10. Оформлення заявок на патенти, винаходи здійснюється з урахуванням вимог збереження комерційної таємниці. При необхідності в цих матеріалах вказується на обмеження відкритої публікації опису винаходів.

3.11. Надання даних, які містять в собі комерційну таємницю, представникам органів державного управління та засобів масової інформації регулюється відповідними законами, іншими нормативно-правовими актами та здійснюється з санкції керівника підприємства.

3.12. Обмеження на розповсюдження комерційної інформації встановлюються керівником підприємства. За часом та місцем дії вони не повинні перевищувати розумної межі.

3.13. Працівник підприємства, якому відома комерційна таємниця, не має права використовувати її задля особистої користі або розголошувати її, а також без письмового дозволу адміністрації займатися прямо або опосередковано будь-якою діяльністю, яка, як конкурентна дія може нанести збиток підприємству, що є володарем цієї комерційної таємниці.

3.14. При звільненні працівник підприємства на протязі дії часу комерційної таємниці не має права її публікувати, розголошувати, передавати будь-кому без дозволу адміністрації підприємства. При звільненні з підприємства у нього береться зобов'язання-попередження.

#### **4. Відповідальність**

4.1. Відповідальність за організацію забезпечення зберігання комерційної таємниці, своєчасну розробку та здійснення заходів щодо її збереження несуть керівники підприємства, структурних підрозділів підприємства та особи, безпосередньо призначені на ці ділянки роботи.

4.2. У разі навмисного або несанкціонованого розголошення (передачі) відомостей, які складають комерційну таємницю, внаслідок чого підприємству була заподіяна матеріальна або інша шкода (втрачена вигода), співробітник притягується до відповідальності, передбаченої трудовим, адміністративним, цивільним або кримінальним законодавством (співробітник може бути звільнений з роботи по недовірі, через судові органи з нього стягнутий штраф на відшкодування заподіяної матеріальної шкоди тощо).

Якщо співробітник займається збиранням конфіденційної інформації комерційного характеру в інтересах конкуруючих або інших організацій, в тому числі іноземних, або фізичних осіб, він несе відповідальність згідно з чинним законодавством.

Притягнення до кримінальної відповідальності може мати місце з ініціативи або згоди власника комерційної таємниці.

Працівники підприємства зобов'язані суворо зберігати комерційну таємницю, яка стала їм відомою в процесі наукової, виробничої, господарської, підприємницької або іншої діяльності, що закріплюється при щорічному укладанні колективного договору. Кожен працівник зобов'язаний знати, що в умовах ринку, конкуренції збереження комерційної таємниці є елементом маркетингу та заповзятливості, способом максимізації при-

бутку підприємства, а її розголошення, безкоштовний обмін досвідом роботи може виявитися економічно небезпечним як для підприємства, так і для кожного його співробітника.

### **Підрозділ безпеки підприємства**

*З положенням про комерційну таємницю підприємства і правила її зберігання під розписку знайомляться всі співробітники підприємства, що мають відношення до відомостей і документів, які становлять комерційну таємницю, в частині, яка їх стосується.*

**НАКАЗ**

“ \_\_\_\_\_ 200\_\_ р.

№ \_\_\_\_\_

**Про визначення відомостей,  
які складають комерційну  
таємницю підприємства**

В умовах переходу до ринкової економіки, розширення зовнішньо-економічних зв'язків, збільшення кількості конфіденційної інформації комерційного характеру в процесі виробничої, господарської, наукової, підприємницької, фінансової та іншої діяльності підприємства назріла необхідність розробки та реалізації нових підходів до вирішення завдань щодо забезпечення збереження відомостей, які належать до комерційної таємниці підприємства. Ці відомості є власністю підприємства. Розголошення або несанкціонована передача цієї інформації може нанести підприємству матеріальної та моральної шкоди, погіршити його економічне та фінансове становище.

У зв'язку з цим, керуючись чинним законодавством України та з метою формування переліку відомостей, які складають комерційну таємницю підприємства,

**НАКАЗУЮ:**

1. Створити постійно діючу комісію з питань комерційної таємниці в складі:

*Голова комісії* \_\_\_\_\_ ;

*Заступник голови* \_\_\_\_\_ ;

*Секретар* \_\_\_\_\_ ;

*Члени комісії* \_\_\_\_\_ .

2. Комісії приступити до роботи \_\_\_\_\_ 200\_\_ р.

3. Покласти на комісію такі завдання:

3.1. Збирання пропозицій від структурних підрозділів підприємства щодо відомостей які можуть бути віднесені до комерційної таємниці підприємства та підлягають захисту від витоку цієї інформації.

3.2. Вивчення пропозицій, що надходять, їх оцінка, узагальнення, систематизація та розробка проекту “Переліку відомостей, які складають комерційну таємницю підприємства”.

4. Встановити, що право кваліфікувати інформацію як комерційну таємницю підприємства, надається керівникам структурних підрозділів

підприємства (філій, госпрозрахункових підприємств, цехів, відділів, лабораторій тощо), які з урахуванням “Методики визначення відомостей, які складають комерційну таємницю підприємства” (Додаток 1), мають провести оцінку наукових розробок, перспективних наукових напрямків, комерційних та інших планів, структури цін, тендерних пропозицій, внутрішньої інформації тощо та до \_\_\_\_\_ 200\_\_р. надати в комісію пропозиції за встановленою формою (Додаток 2) про внесення в “Перелік” відомостей, які доцільно віднести до категорії “комерційна таємниця”.

5. Голові постійно діючої комісії \_\_\_\_\_ :

5.1. Забезпечити контроль за своєчасним надходженням матеріалів від керівників структурних підрозділів та планомірність роботи комісії.

5.2. Проект “Переліку відомостей, які складають комерційну таємницю підприємства” обговорити на засіданні технічної ради та подати керівнику підприємства на затвердження до \_\_\_\_\_ 200\_\_р.

6. Покласти на керівників підрозділів, які беруть участь у виробленні пропозицій для “Переліку”, особисту відповідальність за збереження інформації, яка складає комерційну таємницю. Підготовленим для комісії документам, які містять комерційну таємницю, присвоювати гриф “комерційна таємниця” та передавати секретареві комісії, а йому забезпечити їх облік та зберігання.

7. Голові комісії у десятиденний строк ознайомити з наказом членів комісії та керівників структурних підрозділів (за списком), які беруть участь у підготовці відомостей для “Переліку”.

8. Контроль за виконанням цього наказу залишаю за собою

***Керівник підприємства*** \_\_\_\_\_

Додаток № 1 до наказу  
№ \_\_\_\_\_ від \_\_\_\_\_ 200\_р.

## **МЕТОДИКА** **визначення відомостей, які складають** **комерційну таємницю підприємства**

Визначення відомостей, які складають комерційну таємницю, є важливим елементом в системі заходів, які здійснюються підприємством щодо захисту своєї економічної безпеки. Правильне і своєчасне визначення таких відомостей суттєво підвищує ефективність цієї системи.

Поняття “комерційна таємниця” юридично закріплене в ст. 505 Цивільного кодексу України: “Комерційною таємницею є 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.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці”.

Виходячи з даного формулювання, а також з Закону “Про інформацію” відмінностями конфіденційної комерційної інформації від будь-якої іншої є те, що вона:

- є власністю підприємства, має матеріальну (комерційну) цінність, її витік може нанести матеріальну шкоду підприємству, у зв’язку з цим підприємство здійснює заходи щодо її захисту;
- не є державним секретом (хоча можливе переростання однієї категорії в іншу) і не захищена авторським та патентним правом — є товаром, має ціну, вартість;
- позначена обмежуючим грифом та підприємством здійснюються заходи щодо її захисту;
- не може відповідно до законодава України приховувати негативну сторону діяльності підприємства, здатну нанести шкоду суспільству.

З цих причин, як комерційну таємницю, доцільно захищати лише конкурентоспроможну інформацію (наукові ідеї, нові технології, дослідні

зразки виробів, продукції, тендерні пропозиції, послуги тощо), яка може принести прибуток. Об'єктом досліджень для визначення відомостей, як комерційної таємниці, повинна бути науково-дослідна, конструкторсько-технологічна, підприємницька, виробнича, організаційно-управлінська або інша діяльність підприємства.

Визначення відомостей, які складають комерційну таємницю підприємства, передбачає перш за все проведення аналізу всієї вказаної вище діяльності підприємства для визначення, наприклад, конкурентоспроможних НДР, виробничої продукції, нових технологій, послуг, які надаються, тощо. При проведенні аналізу важливо також врахувати перспективи розвитку підприємства. Цю роботу повинні здійснювати керівники структурних підрозділів (начальники відділів, цехів, лабораторій, груп і т.ін.) із залученням, при необхідності, інших компетентних співробітників підприємства.

За результатами аналізу слід визначити категорію відомостей, які можуть бути класифіковані як "комерційна таємниця" та розрахувати можливий розмір збитків, які може понести підприємство у разі витоку цих відомостей, якщо вони не будуть захищені. При визначенні збитку від витоку конкретних відомостей у вартісному вираженні можна користуватися методиками, які існують в економічних та фінансових структурах підприємства. Завершити проведення аналізу та оцінку розміру можливого збитку від витоку інформації слід проведенням маркетингових досліджень діяльності конкурентів на ринку ідей, технологій, реалізації готової продукції, різних видів послуг тощо.

Класифікація відомостей, які складають комерційну таємницю, значною мірою залежить від профілю та напрямку наукової, виробничої, зовнішньоекономічної, організаційної та іншої діяльності відділів, цехів, лабораторій та інших підрозділів підприємства, вміння оцінити результати цих видів діяльності.

Проблема визначення таких відомостей та ранжування їх за ступенем конфіденційності надто складна. Вона потребує аналізу великого обсягу різномірної інформації про спрямування та види діяльності підприємства, його структур, партнерів, а також конкурентів. У зв'язку з цим від об'єктивного, чіткого та, що дуже важливо, своєчасного визначення предмета захисту залежить збереженість важливої для підприємства конфіденційної інформації.

При визначенні відомостей, які складають комерційну таємницю підприємства, необхідно керуватися такими критеріями:

1. Науково-дослідні роботи та технології, нові види товарів і продукції, послуги повинні мати дійсну або потенційну цінність з комерційних міркувань. Вміщені в них відомості повинні мати не тільки загальні показники своєї виключної важливості, а й бути відносними показниками економічної важливості та конкурентоспроможності, а також мати споживчі властивості.

2. Не потребують додаткового захисту і не можуть бути віднесені до комерційної таємниці відомості, які є державними секретами, захищені патентним або авторським правом (примітка: відомості, які є державними секретами, можуть переростати в категорію комерційних секретів, якщо держава зніме з них гриф таємності).

3. До комерційної таємниці можуть бути віднесені результати досліджень (конструкторських робіт), які при впровадженні їх у виробництво підвищують конкурентоспроможність продукції, що випускається підприємством.

4. Відповідно до постанови Кабінету Міністрів України від 9 серпня 1993 року № 611 “Про перелік відомостей, які не є комерційною таємницею”, такими є:

- установчі документи, документи, які дозволяють займатися підприємницькою або господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки нарахування та сплати податків й інших обов’язкових платежів;
- відомості про чисельність та склад працюючих, їх заробітну плату в цілому та за професіями і посадами, а також наявність вільних робочих місць;
- документи про сплату податків та обов’язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізації продукції, яка шкодить здоров’ю, а також інші порушення законодавства України та розміри нанесених при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, товариствах, об’єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, які відповідно до чинного законодавства належать розголошенню.

Відповідно до зазначеної Постанови підприємства зобов'язані надавати ці відомості органам державної виконавчої влади, контролюючим та правоохоронним органам, іншим юридичним особам згідно з чинним законодавством за їх вимогою.

Слід мати на увазі, що небезпечним для підприємства є як несвоечасне, так і необґрунтоване засекречування комерційної інформації.

**Деякі рекомендації** по підготовці та складанню “Переліку відомостей, які складають комерційну таємницю”.

Перелік — це зведення конкретних відомостей комерційного характеру, які підлягають захисту, в нього можуть входити:

- науково-технічна і технологічна інформація про результат науково-дослідних та дослідно-конструкторських робіт;
- відомості про матеріальне (товарне) виробництво;
- інформація про нові технології;
- маркетингова інформація;
- ділова інформація: відомості про фінансову діяльність підприємства (стан розрахунків з партнерами та клієнтами, ціни, заборгованість, кредити,); плани та обсяги реалізації виробничої продукції; плани рекламної діяльності тощо.
- відомості про конкурентів, партнерів і т.ін.

Пропозиції про засекречення відомостей, які складають комерційну таємницю, повинні надаватися до постійно діючої комісії з комерційної таємниці.

В пропозиції висловлюється суть питання, вказується найменування відомостей, їх коротка характеристика, обґрунтування для включення до розряду “комерційна таємниця” відповідно світовому рівню, конкурентоспроможність, економічна користь, приблизний термін їх засекречення та життєздатності, а також перелік осіб, яким повинен бути дозволений доступ до даних відомостей. У пропозиції повинен бути визначений відповідний рівень конфіденційності відомостей, які підлягають захисту (наприклад, “КТ-суворо конфіденційно”, “КТ-конфіденційно” тощо). Далі ці відомості групуються за ознаками або видами наукової, виробничої, торговельної, фінансової та іншої діяльності і, наприкінці, комісія складає кінцевий варіант документа у вигляді “Переліку відомостей, які складають комерційну таємницю підприємства”. Цей перелік доповідається керівникові підприємства, затверджується ним та запроваджується в дію наказом по підприємству, після чого доводиться безпосереднім виконавцям у частині, що їх стосується.

Якщо в процесі господарської та іншої діяльності виникає необхідність виділити нові відомості, які підлягають захисту, керівник структур-

ного підрозділу подає до комісії матеріали в тому ж порядку, зазначеному в даній методиці.

У роботі постійно діючої комісії з комерційної таємниці повинні брати участь, крім провідних фахівців з основних напрямків науково-дослідної, виробничої, господарської та управлінської діяльності підприємства, також представники підрозділів безпеки, зовнішньоекономічного, патентно-ліцензійного відділів, відділу інформатики, бухгалтерії та ін.

“Перелік відомостей, які складають комерційну таємницю підприємства” є юридичним документом, який фіксує право підприємства на захист своїх комерційних секретів. Він дає право у встановленому законодавством України порядку (в тому числі через судові органи) вимагати відшкодування нанесених матеріальних збитків або упущеної вигоди в разі, якщо передбачені “Переліком” відомості, при порушенні встановленого на підприємстві порядку, були розголошені особою, якій вони були доручені, або втрачені чи передані конкурентам.

### **Підрозділ безпеки підприємства**

*Методика є обов’язковим документом, яким керуються всі співробітники підприємства, що залучаються до роботи по класифікації відомостей як комерційної таємниці.*

/гриф конфіденційності/  
Додаток № 2 до наказу  
№ \_\_\_\_\_ від \_\_\_\_\_ 200\_р

## СЛУЖБОВА ЗАПИСКА

Просимо розглянути та включити до “Переліку відомостей, які складають комерційну таємницю підприємства”:

1. Найменування відомостей \_\_\_\_\_  
(чітке формулювання відомостей)

2. Гриф конфіденційності, в яких джерелах (документах) містяться відомості, які складають комерційну таємницю: \_\_\_\_\_  
\_\_\_\_\_  
(конфіденційно, суворо конфіденційно)

3. Обґрунтування для включення \_\_\_\_\_  
\_\_\_\_\_  
(новизна, конкурентоспроможність, економічна вигода і т.д.)

4. Орієнтовна вартість відомостей, які складають комерційну таємницю (результати НДР, виробы, продукція, товари, послуги, постачання та ін.) \_\_\_\_\_  
\_\_\_\_\_

5. Орієнтовний термін відомостей, які складають комерційну таємницю \_\_\_\_\_  
\_\_\_\_\_

6. Перелік осіб, яким необхідно дозволити допуск до цих відомостей:  
\_\_\_\_\_  
\_\_\_\_\_

**Додаток:** матеріали на \_\_\_\_\_ сторінках, їх найменування (при необхідності)

Керівник підрозділу \_\_\_\_\_ “ \_\_\_\_\_ ” \_\_\_\_\_ 200\_р  
(прізвище)

*Службова записка складається на кожну конкретну відомість, віднесenu до категорії “комерційна таємниця”.*

“КТ-конфіденційно”

## **ПРИБЛИЗНА СТРУКТУРА ПЕРЕЛІКУ ВІДОМОСТЕЙ, ЩО СКЛАДАЮТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ**

Структура “Переліку” залежить від багатьох індивідуальних особливостей підприємства: спрямованості його господарської, наукової, зовнішньоекономічної, комерційної та іншої діяльності, обсягу виконуваних робіт, послуг, які надаються, наявністю конкуруючих підприємств тощо.

Можна рекомендувати для використання при складанні “Переліку” зразковий перелік відомостей, що складають комерційну таємницю підприємства, запропонований в роботі “Економічна безпека підприємства: захист комерційної таємниці” за редакцією В.М. Чаплигіна.

“Перелік” може мати таку структуру.

### **1. ВИРОБНИЦТВО**

1.1. Відомості про структуру виробництва, виробничі потужності, типи і розміщення устаткування, запаси сировини, матеріалів, комплектуючих і готової продукції.

### **2. УПРАВЛІННЯ**

2.1. Відомості про застосовувані оригінальні методи управління виробництвом.

2.2. Відомості про підготовку, прийняття і виконання окремих рішень керівництва підприємства з комерційних, організаційних, виробничих, науково-технічних та інших питань.

### **3. ПЛАНИ**

3.1. Відомості про плани або розширення (згортання) виробництва різних видів продукції і їхніх техніко-економічних обґрунтувань.

3.2. Ті ж відомості про плани закупівель, продажу та інвестиції.

### **4. НАРАДИ**

4.1. Відомості про факти проведення, цілі, предмети і результати нарад і засідань органів управління підприємства.

## **5. ФІНАНСИ**

- 5.1. Відомості про баланси підприємства.
- 5.2. Відомості, що містяться в бухгалтерських книгах управління.
- 5.3. Відомості про кругообіг коштів підприємства.
- 5.4. Відомості про фінансові операції підприємства.
- 5.5. Відомості про стан банківських рахунків підприємства, виробничі операції.
- 5.6. Відомості про рівень доходів підприємства.
- 5.7. Відомості про боргові зобов'язання підприємства.
- 5.8. Відомості про стан кредиту підприємства (пасиви й активи).

## **6. РИНОК**

- 6.1. Відомості про застосований підприємством оригінальний метод вивчення ринку.
- 6.2. Відомості про результати вивчення ринку, що містяться в оцінках стану і перспектив розвитку ринкової кон'юнктури.
- 6.3. Відомості про ринкову стратегію підприємства.
- 6.4. Відомості про застосований підприємством оригінальний метод здійснення продажів.
- 6.5. Відомості про ефективність комерційної діяльності підприємства.

## **7. ПАРТНЕРИ**

- 7.1. Систематизовані відомості про внутрішніх і зарубіжних замовників, підрядників, постачальників, споживачів, покупців, компаньйонів, спонсорів, посередників, клієнтів, а також про інші ділові відносини підприємства про його конкурентів, що не містяться у відкритих джерелах (довідниках, каталогах та ін.).

## **8. ПЕРЕГОВОРИ**

- 8.1. Відомості про підготовку і результати проведення переговорів діловими партнерами підприємства.

## **9. КОНТРАКТИ**

- 9.1. Відомості, умови конфіденційності яких установлені в договорах, контрактах, угодах та інших зобов'язаннях підприємства.

## **10. ЦІНИ**

10.1. Відомості про методи розрахунку, структури і рівні цін на продукцію та розміри знижок.

## **11. ТОРГИ, АУКЦІОНИ**

11.1. Відомості про підготовку до торгів або аукціону і їхні результати.

## **12. НАУКА І ТЕХНІКА**

12.1. Відомості про цілі, завдання, програми перспективних наукових досліджень.

12.2. Ключові ідеї науково-дослідних робіт.

12.3. Точні значення, конструктивні характеристики створюваних виробів і оптимальних параметрів розроблюваних технологічних процесів (розміри, обсяги, конфігурація, процентний зміст компонентів, температура, тиск, час і т.ін.)

12.4. Аналітичні і графічні залежності, що відображають знайдені закономірності і взаємозв'язки.

12.5. Дані про умови експериментів і устаткування, на якому вони здійснювалися.

12.6. Відомості про матеріали, з яких виготовлені окремі деталі.

12.7. Відомості про методи захисту від підробки товарних знаків.

## **13. ТЕХНОЛОГІЯ**

13.1. Відомості про особливості використаних і розроблюваних технологій та специфіка їхнього застосування.

## **14. БЕЗПЕКА**

14.1. Відомості про порядок і стан організації захисту комерційної таємниці.

14.2. Відомості про порядок і стан організації охорони, пропускний режим, системи сигналізації.

14.3. Відомості, що складають комерційну таємницю підприємств-партнерів і передані на довірчій основі.

**Підрозділ безпеки підприємства**

“КТ-конфіденційно”

**НАКАЗ**

№ \_\_\_\_\_ “ ” \_\_\_\_\_ 200\_р.

**Про затвердження Переліку відомостей,  
що складають комерційну таємницю підприємства****З метою запобігання витоку відомостей, що складають комерційну таємницю підприємства,****Наказую:**

1. Затвердити і ввести в дію підготовлений постійно діючою комісією з комерційної таємниці “Перелік відомостей, що складають комерційну таємницю підприємства”.

2. Усім співробітникам підприємства, що мають відношення до комерційних секретів, суворо керуватися зазначеним “Переліком”. Попередити, що особи, які допустили розголошення відомостей, передбачених даним “Переліком” (їхню передачу іншим особам, втрату документів, що містять комерційну таємницю), будуть притягнуті до відповідальності згідно з законодавством України.

3. Керівникам структурних підрозділів провести з підлеглими співробітниками роз’яснювальну роботу, спрямовану на запобігання витоку конфіденційної комерційної інформації, включеної в “Перелік”.

4. Зобов’язати керівників структурних підрозділів вчасно надавати до постійно діючої комісії з комерційної таємниці інформацію про необхідність віднесення нових відомостей до категорії “комерційна таємниця” або виключення з переліку тих відомостей, які втратили своє значення.

5. Керівнику підрозділу економічної безпеки \_\_\_\_\_ ознайомити з даним наказом і “Переліком” усіх співробітників підприємства, допущених до документів і відомостей, що становлять комерційну таємницю (у частині, що їх стосується).

6. Контроль за своєчасним доповненням або зміною “Переліку” і припиненням термінів дії окремих відомостей покласти на \_\_\_\_\_.

**Керівник підприємства.**

**ЗАТВЕРДЖУЮ**  
**КЕРІВНИК ПІДПРИЄМСТВА**  
“ \_\_\_\_\_ ” \_\_\_\_\_ 200\_р.

## **ПОЛОЖЕННЯ**

### **про підрозділ безпеки підприємства**

#### **1. Загальні положення**

1.1. Положення про підрозділ безпеки розроблене згідно з Господарським кодексом України, КЗпП України й іншими нормативно-правовими актами щодо захисту комерційної таємниці в Україні.

1.2. Підрозділ безпеки є структурним, на який покладається відповідальність за організацію і здійснення заходів щодо забезпечення збереження комерційної таємниці (захист передових ідей, нових технологій, підприємницької, комерційної, господарсько-управлінської інформації тощо), запобігання витоку відомостей, що складають комерційну таємницю.

1.3. Підрозділ безпеки безпосередньо підпорядковується керівникові підприємства, комплектується компетентними фахівцями в галузі захисту комерційної таємниці.

1.4. Заходи щодо запобігання витоку відомостей, що складають комерційну таємницю, підрозділ безпеки здійснює у взаємодії з кадровим апаратом, юридичною службою, іншими підрозділами.

1.5. З питань забезпечення збереження комерційної таємниці компетенція підрозділу безпеки поширюється на всі структурні підрозділи, що входять до складу підприємства.

#### **2. Основні цілі і завдання**

2.1. Підрозділ безпеки організує свою роботу, виходячи з наступних цілей забезпечення економічної безпеки підприємства:

- захист законних прав підприємства і його співробітників у взаєминах з державними органами, іноземними і внутрішніми партнерами та конкурентами;
- забезпечення збереження конфіденційної комерційної інформації підприємства, а також зразків виробів, устаткування й інформації, наданих у користування підприємству на договірній основі;
- досягнення внутрішньої і зовнішньої організаційної стабільності підприємства, надійності кооперативних і партнерських зв'язків,

- виключення ділових контактів з випадковими і несумлінними партнерами та посередниками;
- підвищення конкурентоспроможності наукових розробок, вироблених товарів і послуг, створення сприятливої ринкової кон'юнктури для їхньої реалізації в умовах конкуренції на внутрішньому і світовому ринку;
  - підтримка стабільних і вигідних для підприємства відносин всередині колективу і зовнішніх стосунків, зміцнення дисципліни праці і створення стимулів для сумлінної роботи співробітників;
  - максимально повне інформаційне забезпечення наукової, підприємницької, виробничої й іншої діяльності підприємства для своєчасного і належного реагування на виникаючі небезпеки і загрози.

2.2. Для досягнення зазначених цілей підрозділ безпеки, разом з дирекцією й іншими структурними підрозділами, бере участь у вирішенні наступних основних завдань:

- своєчасне виявлення загроз життєво важливим інтересам трудового колективу, причин і умов, які сприяють нанесенню підприємству матеріального і морального збитку, його нормальному функціонуванню і розвитку;
- формування надійних гарантій підтримки законності, взаємовигідності, сумлінності співробітництва підприємства, організаційної стабільності його зовнішніх і внутрішніх зв'язків, відпрацьовування механізмів оперативного реагування на загрози і негативні тенденції в розвитку;
- ефективно припинення зазіхань на законні інтереси підприємства, використовуючи юридичні, економічні й організаційні заходи впливу;
- максимально повне відшкодування збитків, що наносяться неправомірними діями фізичних і юридичних осіб.

### 3. Функції

3.1. Вивчає всі сторони науково-виробничої, зовнішньоекономічної, підприємницької й іншої діяльності підприємства для своєчасного виявлення, закриття можливих каналів витоку конфіденційної комерційної інформації, накопичує й аналізує дані про інтерес і поінформованість іноземних фірм, конкурентів про комерційну діяльність підприємства, здійснює цю роботу разом з постійно діючою комісією з питань комерційної таємниці із залученням провідних спеціалістів підприємства.

3.2. Розробляє і здійснює заходи щодо запобігання витоку конфіденційної комерційної інформації, контролює виконання вказівок і роз-

поряджень керівника підприємства з питань збереження комерційної таємниці.

3.3. Запобігає витоку комерційної таємниці при обліку, зберіганні, зверненні і фізичній охороні конфіденційної інформації, що перебуває в будь-якому вигляді і будь-якій формі.

3.4. Запобігає необґрунтованому допуску і доступу працівників підприємства, представників сторонніх організацій до відомостей, що складають комерційну таємницю і містяться в документах, дослідних зразках виробів, товарів і т.ін.

Організує і здійснює захист економічних інтересів трудового колективу, вживає заходів щодо запобігання матеріальних збитків підприємству як власнику конкурентоспроможної інформації, виробленої продукції, що перебуває в його винятковому володінні.

3.5. Запобігає витоку конфіденційної інформації в процесі здійснення зовнішньоекономічних і інших зв'язків з партнерами й конкурентами, а також при підготовці працівниками підприємства матеріалів для опублікування у відкритому друку.

3.6. Ініціативно чи за вказівкою керівника підприємства через експертну комісію (підрозділ по зв'язках із засобами масової інформації):

- оцінює і відбирає інформацію, що має комерційну перспективу і підлягає юридичному і режимному захисту;
- запобігає передчасній публікації у відкритому друці, рекламних матеріалах інформації про передові ідеї, нові технології, що можуть мати велике економічне значення;
- виключає безоплатне використання (передачу) сторонніми організаціями і особами об'єктів інтелектуальної власності.

3.7. Розробляє внутрішні правила і порядок кваліфікації інформації, як комерційної таємниці підприємства, і зняття з неї обмежень; за поданнями керівників підрозділів готує список посадових осіб, уповноважених кваліфікувати інформацію як комерційну таємницю і знімати ці обмеження; подає списки таких осіб на затвердження керівникові підприємства.

3.8. Розробляє річні і поточні плани роботи з вирішення завдань, що стоять перед підрозділом, по захисту конфіденційної комерційної інформації, яка виникає в процесі зовнішньоекономічної, виробничої і господарської діяльності підприємства при прийомі партнерів та конкурентів, іноземних фахівців і бізнесменів, укладанні комерційних та інших договорів і контрактів з інофірмами, при проведенні господарсько-управлінської діяльності, пов'язаної з комерційними інтересами підприємства (підго-

товка звітної документації про діяльність підприємства, при укладанні договорів, угод і т.ін.)

3.9. За участю керівників структурних підрозділів розробляє перелік посад співробітників, що підлягають допуску до відомостей, які складають комерційну таємницю.

3.10. Вживає заходів щодо запобігання витоку конфіденційної комерційної інформації:

- при здійсненні наукової, виробничої, зовнішньоекономічної і господарської діяльності та ділових зв'язків з інофірмами, партнерами й іншими установами і підприємствами України, СНД і далекого зарубіжжя;
- при експлуатації ЕОМ і інших технічних засобів, призначених для передачі, прийому й обробки секретної і конфіденційної інформації, а також при використанні незахищених каналів зв'язку;
- при проведенні нарад, конференцій, ділових зустрічей, виставок, захисту дисертацій, у процесі яких використовується важлива комерційна інформація.

3.11. Спільно з працівниками підприємства, відповідальними за прийом іноземних партнерів і ділових людей, розробляє програми прийому таких осіб, погоджує конкретні проблеми і питання, що мають обговорюватися, характер і обсяг комерційної інформації, з яким ці особи мають бути ознайомлені і котра їм буде передана; забезпечує облік і своєчасність звітності про бесіди з партнерами, конкурентами.

3.12. Із співробітниками підприємства, що виїжджають у закордонні відрядження, проводить бесіди з питань безпеки під час перебування за кордоном, а після повернення з-за кордону — про можливий інтерес іноземців до конфіденційної комерційної інформації, якою володіє підприємство, веде облік і аналіз матеріалів про такого роду спрямування та поінформованість.

3.13. При укладанні договорів і угод з іноземними партнерами, сторонами установами в Україні контролює: наявність умов, що гарантують дотримання прав підприємства на комерційні секрети; надійність заходів захисту конфіденційної комерційної інформації, вимог конфіденційності на період договірних відносин; дії проти третіх осіб і організацій, що стосуються інтересів сторін, за вказівкою керівника звертається до суду чи господарського суду з питань відшкодування нанесеного збитку і т.ін.

3.14. Організує і веде діловодство документів, що містять комерційну таємницю; контролює забезпечення порядку їх використання, розмно-

ження, обліку, збереження, наявності і передачі (у т.ч. за межі України) у процесі повсякденної роботи з ними.

3.15. Веде виховну та профілактичну роботу зі співробітниками підприємства, що мають доступ до конфіденційної інформації, спрямовану на підвищення професійної етики збереження таємниці; проводить підготовку співробітників, що беруть участь у міжнародних зовнішньоекономічних зв'язках, здійсненні комерційних операцій на внутрішньому ринку; організує вивчення співробітниками нових правових норм і правил захисту комерційних інтересів в умовах ринкових відносин.

3.16. Розробляє нові організаційні форми захисту науково-технічних, технологічних та інших відомостей, що мають комерційну цінність, а також інструктивні, організаційно-методичні документи щодо правового забезпечення збереження комерційної таємниці (накази, розпорядження, положення, рекомендації тощо).

3.17. Разом з відділом кадрів (менеджером з персоналу) бере участь в оформленні договірних зобов'язань (трудової угоди, договору, контракту) з особами, що матимуть доступ до інформації, яка становить комерційну таємницю.

3.18. Вживає заходів щодо запобігання розголошення і витоку відомостей, позначених грифом секретності при веденні діловодства; вивчає й аналізує відкрите службове листування підприємства з метою виявлення в ньому відомостей, що не підлягають розголошенню.

3.19. Забезпечує встановлений порядок відвідування підприємства представниками сторонніх організацій, а також іноземцями; контролює виконання співробітниками позавідомчої охорони і працівниками підприємства правил внутрішнього розпорядку.

3.20. При виконанні зазначених у дійсному Положенні завдань і функцій підтримує ділові контакти з правоохоронними органами України.

#### **4. Права**

Для виконання покладених завдань і функцій підрозділ безпеки має право:

4.1. Вимагати від усіх співробітників підприємства виконання нормативних документів з питань збереження комерційної таємниці.

4.2. Залучати провідних спеціалістів підприємства до участі у вирішенні завдань щодо запобігання витоку конфіденційної інформації (консультації, аналітична робота, вироблення пропозицій щодо захисту інформації тощо).

4.3. Здійснювати перевірки стану і організації роботи щодо захисту конфіденційної інформації в усіх підрозділах підприємства.

4.4. Проводити службові розслідування за фактами розголошення відомостей, що складають комерційну таємницю, втрати документів або виробів, що містять таку інформацію, зловживання правом на комерційну таємницю: некваліфікованого поводження з нею користувачів конфіденційної інформації, порушення договірних зобов'язань про комерційну таємницю тощо; вимагати від співробітників підприємства надання письмових пояснень у зв'язку з допущеними порушеннями.

4.5. Давати рекомендації й обов'язкові для виконання вказівки керівникам підрозділів підприємства з питань захисту конфіденційної інформації.

4.6. Вносити подання керівникові підприємства про призупинення комерційних операцій при виявленні грубих порушень вимог щодо захисту від розголошення комерційних секретів, а також про залучення до кримінальної чи дисциплінарної відповідальності осіб, винних у порушенні порядку захисту комерційної таємниці.

4.7. Брати участь в укладанні угод, контрактів, договорів, предметами яких є відомості і документація комерційного характеру, що підлягають юридичному захисту.

4.8. Представляти інтереси підприємства в правоохоронних органах або суді при надходженні в ці органи від співробітників скарг і заяв про порушення адміністрацією трудового договору, пов'язаних із захистом конфіденційної інформації.

4.9. Вносити керівництву підприємства пропозиції про заохочення співробітників, що активно беруть участь у виробленні і забезпеченні спеціальних заходів захисту від розголошення комерційної таємниці.

Введено в дію наказом  
№ \_\_\_\_\_ від \_\_\_\_\_

**ПОЛОЖЕННЯ**  
**про дозвільну систему доступу співробітників підприємства**  
**та представників сторонніх організацій до відомостей,**  
**які складають комерційну таємницю підприємства**

**ЗМІСТ**

1. Загальні положення.
2. Права та обов'язки посадових осіб стосовно доступу співробітників підприємства до документів, відомостей та спецвиробів, які містять комерційну таємницю.
3. Права та обов'язки підрозділу безпеки стосовно доступу співробітників підприємства до комерційних секретів.
4. Повноваження посадових осіб стосовно доступу співробітників до документів та відомостей, які складають комерційну таємницю.
5. Загальні вимоги до оформлення доступу співробітників до документів та відомостей, що складають комерційну таємницю.
6. Порядок видачі документів, що містять комерційну таємницю, на робочі місця співробітників.
7. Порядок доступу до документів категорії “КТ-особливо важливо”.
8. Порядок доступу співробітників до документів оперативного листування.
9. Порядок розмноження та адресування документів, які складають комерційну таємницю, у зовнішні організації і підрозділи підприємства.
10. Порядок доступу до документів і відомостей, які містять комерційну таємницю, представників сторонніх організацій.
11. Порядок доступу на наради і засідання для обговорення комерційних секретів.

**1. Загальні положення**

1.1. Дане положення розроблене у відповідності з вимогами Господарського кодексу, законів України “Про прокуратуру”, “Про міліцію”, “Про службу безпеки України”, “Про державну податкову службу України” з метою забезпечення правомірного доступу співробітників підприємства та інших осіб, вказаних у Положенні, до ві-

домостей, документів та робіт, які складають комерційну таємницю підприємства.

1.2. Під доступом розуміється письмово оформлений дозвіл керівника підприємства або іншої уповноваженої посадової особи підприємства на роботу або ознайомлення з конкретними відомостями, які складають комерційну таємницю, співробітників підприємства та представників сторонніх організацій.

1.3. Доступ співробітників підприємства до документів і відомостей, які містять комерційну таємницю, вважається правомірним, якщо співробітник:

- має оформлене у встановленому порядку право на допуск до документів і відомостей, які містять комерційну таємницю підприємства;
- призначений наказом на відповідну посаду і згідно зі своїми функціональними обов'язками повинен мати допуск до документів і відомостей, які містять комерційну таємницю;
- пройшов інструктаж щодо загальних правил збереження комерційних секретів та дав зобов'язання про нерозголошення комерційної таємниці;
- ознайомлений з “Положенням про комерційну таємницю підприємства” та засвоїв його (перевірку здійснює керівник підрозділу безпеки);
- пройшов додатковий інструктаж у керівника підрозділу, в який він призначений або вже працює, про дотримання вимог щодо збереження конфіденційної інформації з переліком конкретних особливостей підрозділу та своїх службових обов'язків.

Доступ особи, яка не є співробітником підприємства, вважається правомірним, якщо вона:

- має документ, підписаний керівником установи (партнером, відділом міліції, СБУ і т. ін.), який підтверджує необхідність ознайомлення особи з певними документами і відомостями, які містять комерційну таємницю;
- особа ознайомлена з загальними правилами режиму на підприємстві і згодна підписати угоду про конфіденційність.

1.4. Керівники підприємства та його структурних підрозділів, яким надано право допускати співробітників до відомостей, які складають комерційну таємницю, несуть особисту відповідальність за дотримання правомірності доступу цих співробітників до таких документів і відомостей.

1.5. Неправомірне ознайомлення співробітників з документами і відомостями, які містять комерційну таємницю, розглядається як розголошення конфіденційної інформації і тягне за собою відповідальність, передбачену законодавством України.

1.6. За розголошення комерційної таємниці, за втрату документів, спецвиробів та продукції, в яких міститься подібна інформація, а також за порушення вимог “Положення про комерційну таємницю підприємства” у випадках, коли внаслідок цього завдано суттєвих матеріальних збитків підприємству, винні особи можуть бути притягнені до кримінальної відповідальності у згідно з чинним законодавством України.

1.7. Контроль за дотриманням вимог даного Положення покладається на керівника підрозділу безпеки, керівників структурних підрозділів підприємства, в яких можуть знаходитись відомості, що складають комерційну таємницю.

## **2. Права та обов’язки посадових осіб стосовно доступу співробітників підприємства до документів, відомостей та спецвиробів, які містять комерційну таємницю**

*(якщо не обумовлено спеціально, маються на увазі заступники керівника підприємства, начальники управлінь, відділів, цехів, лабораторій, їх заступники, керівники зовнішньоекономічних та інших структур)*

2.1. Посадові особи мають право:

- допускати у встановленому на підприємстві порядку до конкретних документів, відомостей, зразків виробів, які містять комерційну таємницю, співробітників, якщо це викликано прямою службовою необхідністю;
- відмінити надані підлеглими керівниками дозволи на ознайомлення з документами і відомостями, які складають комерційну таємницю;
- вносити в підрозділ безпеки або керівникам підприємств пропозиції щодо удосконалення дозвільної системи з метою більш оперативного використання конфіденційної інформації при вирішенні службових завдань;
- ставити перед керівником підприємства питання про заохочення підлеглих співробітників, які виявили ініціативу у припиненні дій співробітників, які порушують вимоги даного Положення та “Положення про комерційну таємницю підприємства”.

## 2.2. Посадові особи зобов'язані:

- допускати співробітників до комерційної таємниці тільки відповідно до вимог даного Положення;
- своєчасно інформувати підрозділ безпеки про зміни обсягу та (або) змісту документів і відомостей, які складають комерційну таємницю, необхідні їм для виконання службових обов'язків. Не допускати адресування документів підлеглим співробітникам до переоформлення їх обов'язків;
- знати склад і зміст номенклатурних справ з тематики свого підрозділу, при адресуванні окремих документів у справу враховувати можливість доступу до них тих осіб, у яких немає необхідності знайомитись зі справами в цілому;
- відслідковувати дійсну необхідність доступу співробітників до комерційних секретів, не припускаючи випадків їх невинного ознайомлення з тими документами і відомостями, які безпосередньо не стосуються службових обов'язків співробітників;
- забезпечувати ознайомлення з конфіденційною інформацією ділових партнерів лише в межах проведення ділових комерційних переговорів, або попереднього обговорення можливості, або вивчення доцільності укладання договорів та контрактів;
- вести виховну і роз'яснювальну роботу з метою попередження витоку комерційних секретів. Проводити спеціальні інструктажі співробітників з урахуванням конкретних умов роботи в підрозділах;
- присікати дії підлеглих співробітників, які можуть привести до порушення встановленого порядку збереження комерційних секретів і даного Положення;
- своєчасно ставити перед керівником підприємства питання про покарання осіб, які виявляють халатність або нехтують вимогами режиму, аж до позбавлення права роботи з документами і відомостями, які складають комерційну таємницю.

## **3. Права і обов'язки підрозділу безпеки стосовно доступу співробітників підприємства до комерційних секретів**

### 3.1. Підрозділ безпеки має право:

- ставити перед керівництвом питання щодо неправомірності доступу, який дозволений конкретному співробітникові нижчестоящими керівниками, та не видавати йому документи, які містять

комерційну таємницю; не допускати його на наради, на яких обговорюються конфіденційні комерційні інтереси підприємства до повного з'ясування питання;

- ставити перед керівництвом питання щодо неправомірності адресування керівниками підрозділів документів, які містять комерційну таємницю, у зовнішні організації (або в підрозділи підприємства) та не відправляти ці документи до повного з'ясування питання;
- вимагати письмових роз'яснень від співробітників, які допустили порушення вимог цього Положення;
- ставити перед керівництвом питання про заохочення працівників, які виявляють ініціативу в знешкодженні дій осіб, які порушують вимоги цього Положення та Положення “Про комерційну таємницю підприємства”

### 3.2. Підрозділ безпеки зобов'язаний:

- контролювати правомірність доступу конкретних співробітників до конкретних документів та інформації, які складають комерційну таємницю;
- контролювати правильність розмноження та розсилки документів, які містять комерційну таємницю, в інші підприємства та установи (в тому числі і партнерам) та переадресацію документів в інші підрозділи підприємства, не допускаючи необґрунтованого адресування таких документів в організації (підрозділи підприємства), які не мають до них безпосереднього відношення;
- припиняти дії співробітників, які можуть призвести до порушення вимог діючих нормативних документів щодо забезпечення збереження конфіденційних комерційних інтересів підприємства;
- разом з посадовими особами виявляти інформацію, яка не включена до “Переліку відомостей, які складають комерційну таємницю” з тим, щоб своєчасно вжити заходів щодо збереження такої інформації, не допустити доступу до неї співробітників, які не мають до неї відношення;
- вивчати ефективність та достатність заходів, які вживаються, для забезпечення необхідного режиму роботи з комерційними секретами на робочих місцях співробітників;
- вимагати від керівників підрозділів здійснювати у встановлені строки коригування усіх раніше оформлених дозволів на допуск підлеглих до роботи з комерційними секретами та брати участь в цій роботі;

- знайомитися з усіма наказами та розпорядженнями, які пов'язані зі змінами посадових та функціональних обов'язків співробітників;
- враховувати допущені порушення режиму забезпечення збереження комерційних секретів, зауваження та пропозиції щодо його удосконалення, аналізувати їх та вживати відповідних заходів;
- своєчасно ставити перед керівництвом підприємства питання про притягнення до відповідальності осіб, які виявляють халатність або нехтують вимоги режиму щодо забезпечення збереження комерційних секретів, практично до не допуску на право роботи з документами та відомостями, які складають комерційну таємницю.

#### **4. Повноваження посадових осіб стосовно доступу співробітників до документів та відомостей, які складають комерційну таємницю**

Допускати співробітників до документів та відомостей, які складають комерційну таємницю, мають право:

- керівник підприємства — до всіх документів та відомостей, які складають комерційну таємницю з усіх питань діяльності підприємства — усіх співробітників;
- заступники керівника та інші керівники підприємства — до документів та відомостей, які складають комерційну таємницю, відповідно до їх функціональних обов'язків — усіх співробітників;
- начальники (завідуючі) відділів, цехів, самостійних лабораторій, керівники СКТБ (спеціальне конструкторсько-технологічне бюро), ОКТБ (особливе конструкторсько-технологічне бюро), наукові керівники НДДКР — до документів та відомостей, які складають комерційну таємницю, власниками яких вони є — своїх підлеглих співробітників. Окремі керівники, відповідно до затвердженого списку, мають це право стосовно представників сторонніх організацій;
- начальники лабораторій, груп, які входять до складу відділів — стосовно документів, які містять комерційну таємницю, та розроблені цим підрозділом, а також документів, які надійшли на їх ім'я — тільки підлеглим працівникам.

## **5. Загальні вимоги до оформлення доступу співробітників до документів та відомостей, які складають комерційну таємницю**

5.1. Документальне (письмове) оформлення доступу може здійснюватися такими способами:

- складанням іменних списків, в яких вказуються прізвища імена та побатькові, займані посади, категорії документів та відомостей, з якими дозволяється працювати співробітникові (списки на право користування справами, на право участі в нарадах при обговоренні комерційних секретів та інше);
- у вигляді розпорядчих написів (резолуцій) на самих документах;
- складанням посадових списків з переліком посад та обсягу конкретних документів та інформації, якими необхідно користуватися тим або іншим особам;
- складанням переліку конкретних документів, які затверджуються керівником підприємства, і з якими дозволяється знайомити конкретних співробітників без наявності розпорядчого надпису.

5.2. Кожен дозвіл повинен мати дату його оформлення.

Дія оформлених дозволів переглядається не менше двох разів на рік.

5.3. У розпорядницькому написі на документі про право на ознайомлення кола осіб керівник повинен, при необхідності, визначити обмеження в доступі конкретних співробітників до відомостей, викладених у документі, і визначити відповідальних за виконання документа.

5.4. Реалізація прав керівників стосовно доступу співробітників до документів і відомостей, що складають комерційну таємницю, здійснюється під контролем підрозділу безпеки.

Іменні і посадові списки, списки конкретних документів (див. п.5.1) візуються підрозділом безпеки, віза якого підтверджує правомірність доступу визначених співробітників до конкретних документів і відомостей.

Працівник підрозділу безпеки перед видачею співробітникові документів відповідно до списків або їхнього допуску на нараду з обговоренням комерційних секретів перевіряє:

- наявність дозволу, підписаного відповідним керівником, і термін його дії;
- відповідність робочого місця співробітника режимним вимогам (див. п. 6) при видачі документів на робочі місця.

Перед видачею співробітникам документів з розпорядницькими написами на них працівник підрозділу безпеки перевіряє повноваження

конкретного керівника стосовно доступу і правомірність доступу співробітників.

5.5. Керівник підрозділу безпеки анулює дозвіл на видачу документів і відомостей, що складають комерційну таємницю, співробітникові, службові або функціональні обов'язки якого були змінені наказом або розпорядженням керівника підприємства, якщо в цьому наказі або розпорядженні не оговорено, що згідно з новими обов'язками співробітникові потрібні документи і відомості, до яких він був раніше допущений.

## **6. Порядок видачі документів, що містять комерційну таємницю, на робочі місця співробітників**

6.1. Документи можуть бути видані на робочі місця співробітників за умови відсутності в цих приміщеннях осіб, які не мають права доступу до цих документів.

6.2. У службові кабінети керівника підприємства, його заступників можуть бути видані будь-які документи з їх поверненням наприкінці дня в підрозділ безпеки.

6.3. Список приміщень, у які дозволяється видавати документи, що складають комерційну таємницю, візується підрозділом безпеки і затверджується одним з керівників підприємства.

## **7. Порядок доступу до документів категорії “КТ-особливої важливості”**

7.1. До таких документів належать зведені річні і перспективні плани комерційної діяльності, звіти про їхнє виконання, програми і календарні плани випуску продукції, інші важливі відомості. Віднесення таких документів до категорії “КТ-особливої важливості” визначають керівник підприємства, його заступники (відповідно до функціональних обов'язків), про що робиться розпорядницький напис на самому документі. На цих документах підрозділ безпеки ставить штамп “КТ-особливої важливості”.

7.2. Такі документи можуть бути видані тільки за письмовим дозволом керівника підприємства, його заступників (відповідно до функціональних обов'язків) і візою керівника підрозділу безпеки.

У такому ж порядку здійснюється зняття копій і право виписок з документів “КТ-особливої важливості”.

7.3. Зведені плани комерційної діяльності, звіти про їхнє виконання й інші важливі документи беруться на інвентарний облік і в справі не підшиваються.

## **8. Порядок доступу виконавців до документів оперативного листування**

8.1. Документація, що містить важливу конфіденційну комерційну інформацію, листи організацій-партнерів доповідаються керівникові підприємства.

8.2. Окремі документи, відповідно до переліку, затвердженого керівником підприємства, можуть передаватися підрозділом безпеки безпосередньо виконавцеві, минаючи його керівника.

Перелік таких документів складається керівниками відділів, цехів і самостійних лабораторій разом з підрозділом безпеки і затверджується керівником підприємства або його заступником.

8.3. Вхідні документи можуть бути видані виконавцю на підставі розпорядничього напису на самому документі посадових осіб підприємства відповідно до їх повноважень (див. п. 4).

8.4. З копіями вихідних документів співробітники (крім безпосередніх виконавців документів і осіб, що візують їх), можуть бути ознайомлені з дозволу посадових осіб відповідно до їх повноважень (див. п. 4).

## **9. Порядок розмноження й адресування документів, що складають комерційну таємницю, у зовнішні організації і підрозділи підприємства**

9.1. Дозвіл на розмноження, з вказівкою про кількість екземплярів документів, що складають комерційну таємницю, дає посадова особа, що має повноваження допускати виконавців до цих документів.

Розмноження документів здійснюється в суворо визначеній кількості примірників, дійсно необхідних для виробничої, господарської й іншої діяльності.

9.2. Необхідність розсилки документів і їхнє адресування визначає керівник підрозділу. Направлятися документи повинні тільки в ті зовнішні організації або підрозділи підприємства, що мають безпосереднє відношення до відомостей, які містяться в адресованому документі.

9.3. Необхідність розмноження підтверджується підписом керівника підрозділу безпеки.

9.4. Усі документи, що направляються в зовнішні організації або передаються в підрозділи підприємства, візуються керівником підрозділу безпеки, який у таких випадках перевіряє:

- правильність адресування документа конкретним керівником;

- наявність у документі зайвих відомостей, повідомлення про які не викликане прямою виробничою або іншою необхідністю;
- правильність визначення грифа конфіденційності документа і необхідність кількості екземплярів, що розсилаються.

9.5. Працівник підрозділу безпеки перед відправленням таких документів перевіряє наявність усіх необхідних підписів і віз на документі, у тому числі візи керівника підрозділу безпеки.

### **10. Порядок доступу представників сторонніх організацій до документів і відомостей, що містять комерційну таємницю**

До представників сторонніх організацій належать:

- співробітники інших установ, підприємств, організацій, що перебувають на підприємстві у зв'язку з питаннями його основної діяльності;
- представники органів суду, прокуратури, міліції й інших органів, що мають право контролю або перевірки тих чи інших аспектів діяльності підприємства; їх права, компетенція і відповідальність за збереження комерційної таємниці підприємства визначаються Господарським кодексом України, законами України “Про прокуратуру”, “Про службу безпеки України”, “Про міліцію”, “Про державну податкову службу України” тощо.

10.1. Зазначені особи можуть бути ознайомлені з документами та відомостями, що складають комерційну таємницю, керівником підприємства або його заступниками (в межах їхніх функціональних обов'язків) при наявності письмового запиту керівників сторонніх організацій, постанови про порушення кримінальної справи, ордера прокурора на проведення обшуку або виїмки. Дозвільний напис повинен чітко визначати коло питань чи документів, з якими варто ознайомити відвідувачів підприємства.

Керівник відділу, цеху, лабораторії на підставі дозвільного напису визначає працівника, якому доручається прийняти відвідувача підприємства, і перелік документів, з якими його можна ознайомити. Правомірність видачі документів підтверджується керівником служби безпеки.

10.2. Представникам правоохоронних і інших органів, що мають право контролю за діяльністю підприємства, документи і відомості, які містять комерційну таємницю, можуть бути видані у встановленому законодавством України порядку і відповідно до положення про комерційну таємницю підприємства і правил її збереження.

10.3. Ознайомлення зазначених осіб з комерційними секретами здійснюється в присутності працівника підприємства. Ці особи зобов'язані розписатися про ознайомлення на документі, з яким вони були ознайомлені, і підписати угоду про конфіденційність з відвідувачем підприємства.

10.4. Співробітникам підприємства категорично забороняється знайомити відвідувачів із зайвими документами і відомостями, що містять комерційну таємницю, які виходять за коло питань, визначених керівником підприємства.

### **11. Порядок доступу осіб на наради і засідання для обговорення комерційних секретів**

Доступ посадових осіб на різні наради і засідання, на яких обговорюються питання, пов'язані з комерційною таємницею (за винятком робочого обговорення таких питань), у тому числі і запрошених представників інших установ, здійснюється за списком із зазначенням питань, в обговоренні яких дозволено взяти участь кожному учаснику наради.

Зміни в списках учасників наради можуть вноситися тільки керівником підприємства або його заступниками.

Список візується керівником підрозділу безпеки.

### **Підрозділ безпеки підприємства**

*З Положенням повинні бути ознайомлені всі співробітники підприємства, що мають відношення до робіт, документів і відомостей, які складають комерційну таємницю підприємства.*

## ЗОБОВ'ЯЗАННЯ

співробітника підприємства про збереження комерційної таємниці

м. \_\_\_\_\_ “ \_\_\_\_\_ ” \_\_\_\_\_ 200\_р.

Я, \_\_\_\_\_, будучи прийня-  
тим на роботу в \_\_\_\_\_  
на посаду, \_\_\_\_\_ зобов'язуюсь:

- не розголошувати відомості, які складають комерційну таємницю підприємства та які мені будуть довірені або стануть відомі сферою діяльності;
- виконувати усі вимоги наказів, розпоряджень, інструкцій, положень щодо забезпечення захисту комерційної таємниці, з якими мене ознайомлять;
- негайно повідомляти свого керівника та підрозділ економічної безпеки підприємства про:
  - а) спроби сторонніх осіб, у тому числі іноземців, отримати (вивідати) у мене інформацію, яка складає комерційну таємницю;
  - б) втрати мною документів (виробів та ін.), які містять комерційну таємницю;
- зберігати комерційну таємницю іноземних юридичних і фізичних осіб, а також установ та організацій України, з якими підприємство налагодило ділові відносини;
- не копіювати або передруковувати документи, які містять відомості, віднесенні до комерційної таємниці підприємства, без письмового дозволу керівника підприємства;
- не передавати третім особам та не розкривати публічно інформацію в будь-якому вигляді (формі), віднесена до комерційної таємниці, без письмового дозволу керівника підприємства.

Я попереджений, що в разі порушення цього зобов'язання зі мною може бути розірваний трудовий договір з ініціативи адміністрації підприємства відповідно до ст.ст. 40, 41 КЗпП України, та я можу бути притягнутий до відповідальності в порядку, встановленому чинним законодавством України.

З Переліком відомостей, які складають комерційну таємницю підприємства та порядком їх захисту я ознайомлений

\_\_\_\_\_ (підпис співробітника)

Проінструктував \_\_\_\_\_  
(Прізвище співробітника підрозділу безпеки)

## **ЗОВОВ'ЯЗАННЯ – ПОПЕРЕДЖЕННЯ**

**про збереження комерційної таємниці при звільненні з підприємства**

Вельмишановний \_\_\_\_\_

(прізвище, ім'я, по батькові)

У зв'язку з Вашим звільненням керівництво підприємства нагадує Вам, що під час Вашої роботи на підприємстві Ви були ознайомлені з важливими для нашого підприємства відомостями, які складають комерційну таємницю, що є власністю підприємства. Не забувайте, що раніше надане Вами зобов'язання про нерозголошення комерційної таємниці зберігає свою силу протягом \_\_\_\_\_ років після Вашого звільнення з підприємства. Підприємство готове захищати свої інтереси, в тому числі і в судовому порядку.

В свою чергу я, як колишній співробітник Вашого підприємства зобов'язуюсь не розголошувати відомості, які містять комерційну таємницю та які стали мені відомі, не використовувати їх в особистих інтересах на новому місці роботи або при інших обставинах. Я розумію, що за розголошення відомостей, які містять комерційну таємницю підприємства, буду нести відповідальність відповідно до чинного законодавства України.

\_\_\_\_\_ (підпис співробітника, дата)

Зобов'язання-попередження відібрав

\_\_\_\_\_ (посада, ПІБ, підпис співробітника підрозділу безпеки)

## УГОДА про конфіденційність з відвідувачем підприємства

В зв'язку з тим, що я \_\_\_\_\_  
(прізвище, ім'я, по батькові, посада та назва організації)

отримав дозвіл та ознайомився з \_\_\_\_\_  
(коротко суть відомостей)

які є виключною власністю підприємства та складають його комерційну таємницю, згоден, що ніколи без письмового дозволу керівника Вашого підприємства не розголошу та не опублікую будь-яку інформацію про ці відомості.

Дана угода не належить до тієї інформації, яка:

- а) була отримана мною без будь-яких зобов'язань відносно конфіденційності перед підприємством;
- б) яку можна отримати законним шляхом із офіційних відкритих публікацій та інших аналогічних джерел;
- в) є або стане надбанням громадськості.

Я визнаю та підтверджую, що дане мною зобов'язання при необхідності може бути використано Вами проти мене.

Підпис відвідувача \_\_\_\_\_

Дата \_\_\_\_\_

Затверджуючий підпис співробітника  
підрозділу безпеки, дата, печатка  
підприємства \_\_\_\_\_

## ПАМ'ЯТКА

### працівнику про збереження комерційної таємниці підприємства

Працівник підприємства, допущений до комерційної таємниці, зобов'язаний ретельно зберігати відомості, що є комерційними секретами підприємства, його власністю. Комерційні секрети визначені в “Переліку відомостей, що становлять комерційну таємницю підприємства”.

Працівник повинен знати і пам'ятати, що розголошення комерційних секретів, що стали відомі йому згідно з родом виконуваної роботи, втрата документів, що містять їх, передача третім особам тягнуть за собою кримінальну, матеріальну або дисциплінарну відповідальність відповідно до законодавства України. В однаковій мірі така відповідальність настає й у випадку, якщо працівник використовує цю інформацію в несанкціонованих діях в інтересах конкурентів, що може нанести матеріальний і моральний збиток підприємству.

Працівник зобов'язаний пам'ятати та знати, що підприємство закріпило за собою право на комерційну таємницю та її захист в Статуті підприємства, колективному договорі, правилах внутрішнього трудового розпорядку. Порядок поводження з відомостями, що складають комерційну таємницю підприємства, визначений Положенням про комерційну таємницю і правилами її збереження, введеним у дію наказом № \_\_\_\_\_ від \_\_\_\_\_ 200\_р., основними вимогами якого Вам необхідно керуватися при користуванні конфіденційною інформацією підприємства.

Працівник повинен знати коло осіб, яким дозволено працювати із відомостями, до яких він сам допущений, і в якому обсязі ця інформація може бути доведена до відома інших співробітників.

Не слід створювати без необхідності документи, у яких міститься конфіденційна інформація або включати в них зайвий обсяг відомостей, якщо цього можна уникнути. Виявляти особливу обережність у складанні і збереженні чернеток документів, дотримувати вимог по веденню діловодства документів із грифом “комерційна таємниця”. Необхідно пам'ятати, що порушенням порядку поводження із відомостями, що складають комерційну таємницю, є включення їх без потреби в ті документи, які є відкритими. Не дозволяється готувати документи, що містять комерційні секрети, у присутності сторонніх осіб.

У випадку втрати документів, дослідних зразків виробів, що містять комерційну таємницю, працівник зобов'язаний негайно довести до відома

підрозділ безпеки підприємства і за його вимогою надати всі документи, які значаться за ним, що містять комерційну таємницю.

Знайомити з документами, що містять комерційну таємницю, представників сторонніх організацій, фірм, партнерів та конкурентів можна тільки відповідно до вимог і положень, передбачених дозвільною системою підприємства. Якщо з боку таких осіб будуть відзначатися спроби одержати такого роду конфіденційну інформацію, необхідно негайно повідомити про це в підрозділ безпеки підприємства.

Для того, щоб чітко знати і правильно дотримуватись усіх вимог щодо збереження конфіденційної інформації, працівникові необхідно уважно вивчити діючі на підприємстві інструкції і положення, які регламентують роботу з документами, що становлять комерційну таємницю.

### **Підрозділ безпеки підприємства**

“КТ-конфіденційно”

**ПАМ'ЯТКА**  
**для використання при укладанні трудової угоди**  
**(договору-підрядку, контракту) на виконання роботи,**  
**що містить комерційну таємницю підприємства**

На відміну від трудового договору про прийом на роботу співробітника з зарахуванням його в штат підприємства, в трудовій угоді (договорі-підряді, контракті) вказуються конкретні відомості, що становлять комерційну таємницю підприємства, передбачаються умови її захисту і залежні від цього зобов'язання виконавця щодо забезпечення збереження комерційної таємниці, що стала йому відомою.

У трудовій угоді (договорі-підряді, контракті) чітко регламентується обов'язок адміністрації підприємства забезпечувати умови виконання роботи для того, щоб передбачені угодою відомості, що складають комерційну таємницю, не стали відомі іншим особам. Неодмінно вказується гриф конфіденційності, перелік відомостей, що містять комерційну таємницю, а також документи і вироби, у яких міститься інформація, що не підлягає розголошенню.

У трудовій угоді (договорі-підряді, контракті) повинні бути передбачені наступні зобов'язання виконавця роботи:

1. Не розголошувати і не передавати нікому, ні в якій формі, а також без дозволу керівника підприємства не використовувати у своїх інтересах або інтересах третьої сторони обумовлені в трудовій угоді (договорі-підряді, контракті) відомості, віднесені до комерційної таємниці, як під час виконання робіт, так і після їхнього завершення.
2. Виконувати роботи, а також зберігати документи і вироби в місцях, зазначених у трудовій угоді (договорі-підряді, контракті).
3. негайно повідомляти керівника робіт і в підрозділ безпеки підприємства про випадки:
  - спроби сторонніх осіб добути (вивідати) інформацію, що становить комерційну таємницю підприємства;
  - втрати документів (виробів, дослідних зразків та ін.), що містять комерційну таємницю.
4. Не копіювати і не розмножувати документи (виготовляти копії виробів), віднесені до категорії “комерційна таємниця”, без письмового дозволу керівника підприємства або посадових осіб, яким делеговане це право.

5. По закінченні робіт здати в підрозділ безпеки всі одержані для їхнього виконання документи і вироби.

У договірних документах варто також передбачити, що у випадку невиконання встановлених вимог, а також зобов'язань виконавцем робіт підприємство має право в односторонньому порядку розірвати з ним трудову угоду (договір-підряду, контракт) і притягти до відповідальності відповідно до чинного законодавства України.

Перераховані зобов'язання працівника, що залучається до виконання робіт категорії “комерційна таємниця”, можуть бути оформлені у вигляді самостійного (окремого документа), або ж на додаток до основної трудової угоди. Будучи підписаними ним, вони при необхідності використовуються в процесі розгляду у зв'язку з витоком комерційної таємниці підприємства.

### **Підрозділ безпеки підприємства**

## **ПАМ'ЯТКА** **працівнику підрозділу кадрів підприємства** **(менеджеру персоналу)**

При вирішенні питання про прийом на роботу осіб, що будуть допущені до відомостей, які складають комерційну таємницю, варто мати на увазі, що чинне законодавство України право на захист цих відомостей делегує підприємству. Виходячи з цього, власники підприємства мають право розробляти і використовувати власну (не всупереч законодавству України) методологію добору, вивчення і перевірки кандидатів для роботи, пов'язаної з відомостями, що становлять комерційну таємницю.

Виходячи з цього, працівник кадрів при вирішенні питання про прийом на роботу, поряд із традиційною перевіркою документів, що засвідчують особу (паспорт, військовий квиток, трудова книжка та ін.) може в разі потреби:

- запросити рекомендаційні листи і використовувати стосовно прийнятого на роботу усні характеристики або рекомендації, що виходять від осіб, які не викликають сумніву;
- використовувати послуги приватних організацій зі збирання даних, що характеризують особу, яка приймається на роботу, якщо вони мають юридично оформлені ліцензії;
- використовувати тестові методики, зокрема: бланкові, ММРІ, СМІЛ, Томаса, УСК, Шмишека й ін.;
- порушити питання перед керівниками підприємства про доцільність або необхідність використовувати поліграф (детектор брехні).

Крім того, працівник кадрів зобов'язаний погодити питання про прийом на роботу особи, що наймається, з керівником підрозділу (відділу, лабораторії, цеху, групи тощо) і підрозділом безпеки підприємства.

При звільненні працівника необхідно:

- взяти у керівника підрозділу (відділу, лабораторії, групи) погоджене з підрозділом безпеки письмове підтвердження про здачу особою, яка звільняється, всіх отриманих і розроблених (виготовлених, розмножених) документів, у тому числі чернеток, виробів, що містять комерційну таємницю підприємства;
- впевнитися, що особою, яка звільняється, підписано зобов'язання-попередження про нерозголошення відомостей, що стали йому відомі і належать до категорії “комерційна таємниця”.

Лише при виконанні вказаних у “Пам’ятці” вимог проект наказу про прийом на роботу співробітника або його звільнення може подаватися на розгляд керівникові підприємства або особі, що його заміщає.

### **Підрозділ безпеки підприємства**

## **ПАМ'ЯТКА**

**для використання при укладанні господарських договорів,  
які містять відомості, що складають комерційну таємницю,  
між суб'єктами господарювання України**

Відповідно до зі ст. 67 Господарського кодексу відносини підприємств з іншими підприємствами, організаціями і громадянами у всіх сферах господарської діяльності здійснюються на основі договорів. В умовах ринкової економіки договірна система стає одним з основних видів відносин між підприємствами, причому договори найчастіше можуть містити конфіденційну комерційну інформацію, у зв'язку з чим вимагають певних захисних заходів.

Конфіденційні відомості можуть стосуватися багатьох розділів договору: предмета угоди, умов його виконання, фінансування, розрахунків, обсягу і характеру виконуваних робіт, іншої інформації, що міститься в договорі.

У зв'язку з цим сторони зобов'язані брати на себе зобов'язання по збереженню в таємниці комерційних секретів, що містяться в договорі.

Як правило, з цією метою у договорі передбачається спеціальний розділ, у якому викладаються відомості, що складають комерційну таємницю, визначаються вимоги до кожної сторони щодо запобігання витоку інформації, порядок використання конфіденційної комерційної інформації, а також передбачаються відповідні санкції на випадок розголошення комерційних секретів або порушень вимог щодо захисту конфіденційності угоди. Перед укладанням договору сторони можуть вивчити можливості один одного із забезпечення необхідних заходів режиму.

В процесі виконання робіт і послуг, передбачених договором, може здійснюватись взаємна перевірка вжитих заходів щодо запобігання витоку конфіденційної комерційної інформації. Виявлені порушення умов конфіденційності і фактів порушень погоджених режимних заходів дають підставу постраждалій стороні розірвати договір або звернутися в судові органи для відшкодування понесених збитків.

Якщо в договорі містяться відомості, які складають комерційну таємницю, йому необхідно присвоювати відповідний обмежувачий гриф.

**Підрозділ економічної безпеки підприємства**

## ПАМ'ЯТКА

### для використання при укладанні з іноземною фірмою договору (контракту), що містить відомості, які складають комерційну таємницю

Розробка і вживання необхідних заходів, що забезпечують збереження комерційної таємниці, є одним з основних зобов'язань, яке повинно взяти на себе підприємство й іноземна фірма при укладанні договору (контракту), що містить конфіденційну комерційну інформацію.

До числа взаємоузгоджуваних сторонами заходів, поряд з іншими, доцільно віднести:

1. Визначення документів, виробів, технологічного устаткування, продукції та ін., що підлягають захисту як суворо конфіденційні.
2. Попередження спроб передачі третій стороні оригіналів документів, виробів, продукції тощо, їх копій або репродукції будь-якого роду.
3. Допуск обмеженого числа осіб до ознайомлення з предметом договору (контракту).
4. Визначення терміну дії, умов конфіденційності після припинення договору (контракту).
5. Санкції за невиконання однією із сторін передбаченого договором (контрактом) зобов'язання щодо захисту від розголошення, витоку інформації, що складає комерційну таємницю. (Наприклад: Винна сторона несе фінансову (матеріальну) відповідальність по відшкодуванню збитків, втраченої вигоди і моральної шкоди перед потерпілою стороною у випадку невиконання нею зобов'язання щодо захисту комерційної таємниці, допущеного витоку інформації, що становить комерційну таємницю).

Умови конфіденційності повинні бути передбачені чинним законодавством країни, вибраної сторонами.

На стадії розробки угоди (контракту) доцільно залучати юристів, що знають законодавство країни, до якої належить фірма-партнер.

**Довідка:** при укладенні зовнішньоекономічного договору (контракту) необхідно керуватись законом "Про зовнішньоекономічну діяльність" від 16.04.91 р., Указом "Про застосування міжнародних правил інтерпретації комерційних термінів" від 4.10.94 р., Правилами "Інко-

термс”, наказом Міністерства зовнішньоекономічних зв’язків та торгівлі № 75 від 5.10.95 р. “Про затвердження положення про форму зовнішньоекономічних договорів (контрактів)”.

### **Підрозділ безпеки підприємства**

Затверджую керівник підприємства  
 “ \_\_\_ ” \_\_\_\_\_ 200\_р.

**РЕКОМЕНДАЦІЙНИЙ ПЛАН**  
**виховання і навчання співробітників підприємства**  
**з питань збереження комерційної таємниці підприємства**

№ з/п	Зміст	Термін	Хто проводить заняття
1	Ринкова економіка і необхідність захисту конфіденційної інформації. Поняття комерційної таємниці, її ознаки.		
2	Практика (досвід) захисту комерційних секретів у країнах із традиційною ринковою економікою.		
3	Необхідність і значення захисту комерційних секретів підприємства в умовах ринку.		
4	Вивчення положення про комерційну таємницю підприємства і правил її збереження.		
5	Правові основи захисту комерційної таємниці.		
6	Методика визначення відомостей, що становлять комерційну таємницю підприємства.		
7	Категорії відомостей, що підлягають захисту на підприємстві. Вивчення переліку відомостей, що становлять комерційну таємницю		
8	Дозвільна система доступу до відомостей і документів, що становлять комерційну таємницю.		
9	Обов'язки, права і відповідальність працівників підприємства при користуванні документами і відомостями, що становлять комерційну таємницю. Види відповідальності за розголошення комерційних секретів.		
10	Основні причини й обставини можливого витоку конфіденційної інформації.		
11	Вимоги до укладання договору, контракту, угоди про господарську діяльність, що містять конфіденційну інформацію. Порядок забезпечення режиму в роботі з іноземними юридичними і фізичними особами, представниками органів державного управління, партнерами, клієнтами і засобами масової інформації.		
12	Роль підрозділу безпеки в організації і проведенні роботи зі збереження комерційних секретів.		
13	Порядок забезпечення режиму при обробці комерційних секретів на ЕОМ і користування ними.		

**Керівник підрозділу безпеки**

**Затверджую**  
Керівник підприємства  
“ \_\_\_\_\_ ” \_\_\_\_\_ 200\_р.

## ІНСТРУКЦІЯ

**щодо організації і ведення на підприємстві діловодства документів,  
що містять комерційну таємницю**

Введена в дію наказом  
№ \_\_\_\_\_ від \_\_\_\_\_

### І. Загальні положення

1.1. Система захисту комерційних секретів передбачає організацію спеціального діловодства з документами-носіями комерційної таємниці підприємства, що встановлює порядок їхньої підготовки, маркування (тобто присвоєння відповідного грифа), розмноження, розсилання, прийому й обліку, групування в справи, використання, збереження, знищення і перевірки наявності.

1.2. Система діловодства документів із грифом “комерційна таємниця” — це організована сукупність сил, а також засобів, правил, методів і прийомів діяльності по діловодству і режимному забезпеченню комерційних секретів, пов’язаних зі створенням, збереженням і використанням документів, в яких міститься комерційна таємниця.

1.3. Дана інструкція розроблена з урахуванням положень “Єдиної державної системи документального забезпечення управління”, “Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави”, яка затверджена постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893, а також діючих ДСТів на організаційно-розпорядницьку документацію.

1.4. Діловодство з документами з грифом “комерційна таємниця” організує і здійснює підрозділ економічної безпеки в спеціально виділених окремих приміщеннях, обладнаних надійними закриваючими пристроями, охоронною сигналізацією, за наявності необхідної кількості сейфів і металевих шаф для збереження документів, зразків виробів, продукції, що містять комерційну таємницю.

1.5. Облік вхідних, внутрішніх і вихідних документів здійснюється за журналами. Основним принципом обліку є однократність присвоєння реєстраційного номера вхідним, внутрішнім і вихідним документам.

1.6. Заведення необхідних журналів обліку документів, виробів і продукції визначається номенклатурою справ і журналів, розроблюваною на початок поточного року, що затверджується керівником підприємства. Аркуші журналів повинні бути пронумеровані, прошиті й опечатані печаткою підприємства. На останньому аркуші журналу робиться напис про кількість у ньому аркушів, що завіряється керівником підрозділу економічної безпеки.

1.7. У журналах обліку відображаються дані про рух документів з моменту їхнього одержання або підготовки до завершення виконання і підшивки в справи, відправлення адресатам або знищення.

У журналах забороняється робити підчищення, а також виправлення з застосуванням коригувальної рідини. Внесення співробітником підрозділу економічної безпеки інших виправлень обумовлюється і завіряється його підписом із проставленням дати.

1.8. Дозвіл на роботу виконавців з конкретними документами дається в посадових або іменних списках, наказах, вказівках, дорученнях у резолюції, написаній на самих документах.

1.9. У випадку тимчасової відсутності працівника підрозділу економічної безпеки, що здійснює діловодство (хвороба, відпустка, відраження), його обов'язки може виконувати інший працівник підприємства, визначений наказом по підприємству як той, що його заміщує.

## **II. Облік документів із грифом “комерційна таємниця”**

### **2.1. Складання й оформлення документів.**

2.1.1. Документи складаються і друкуються в суворо обмеженій кількості екземплярів, яку визначає керівник підприємства або структурного підрозділу. Документи обмеженого користування (ДОК) підготовляються з дозволу керівників підприємства, беруться на інвентарний облік і в справи не підшиваються. На таких документах підрозділ безпеки проставляє штамп “ДОК”.

2.1.2. Кожен вид документа повинен мати визначену сукупність реквізитів і їхнє розташування відповідно до вимог ДСТ.

2.1.3. Кожен додаток до документа повинен мати самостійну порядкову нумерацію аркушів або сторінок.

При відправленні документа із супровідним листом після слова “Додаток” у листі вказується найменування кожного додатка, його реєстраційний номер, номери і кількість доданих примірників, їхній гриф і кількість сторінок.

2.1.4. Документи, що підлягають реєстрації, здаються виконавцями в підрозділ безпеки разом з чернетками.

Збраковані або надруковані зайві документи здаються в підрозділ безпеки для знищення за актом.

2.1.5. Якщо документ, підготовлений і надрукований як несекретний, за рішенням керівника підприємства або керівника підрозділу безпеки підпадає під категорію “Комерційна таємниця”, він реєструється в підрозділі економічної безпеки. Для цього надаються всі екземпляри надрукованого документа і чернетки. Кількість екземплярів надрукованого документа і сторінок зданих чернеток підтверджується підписами виконавців і працівника підрозділу безпеки на звороті останнього екземпляра зданого документа.

У випадку нестачі сторінок, екземплярів або чернеток керівником підрозділу економічної безпеки здійснюється службове розслідування.

2.1.6. Як правило, документи з грифом “комерційна таємниця” виконуються у зареєстрованих робочих зошитах, що видаються виконавцям підрозділом економічної безпеки. Дозволяється виготовлення чернеток документа на окремих сторінках, зареєстрованих у підрозділі економічної безпеки.

2.1.7. Уся кореспонденція, що надходить на адресу підприємства із грифом “комерційна таємниця”, приймається тільки працівником підрозділу економічної безпеки, що перевіряє правильність адреси, цілість упаковки і відбитків печаток, їхню відповідність найменуванню відправника, звіряє номери вкладень, зазначені на пакеті, з номерами, зазначеними в реєстрі (розносній книзі або розписці). При виявленні ушкоджень упакування й інших невідповідностей складається акт. Пакети реєструються в журналі форми № 1.

2.1.8. При розкритті пакетів перевіряється відповідність вказаних на них облікових номерів номерам, що знаходяться в пакеті документів, їх кількість і наявність усіх сторінок документів. При розбіжностях складається акт.

2.1.9. Пакети з позначкою “Особисто” розкриваються особисто адресатом. У журналі форми № 2 робиться запис “Пакет з позначкою особисто”.

2.1.10. Помилково надіслані документи повертаються відправнику.

2.1.10. Після розкриття пакетів документи негайно реєструються в журналі форми № 2. При реєстрації на першій сторінці вхідного документа проставляються обліковий (вхідний) номер, дата реєстрації, кількість сторінок основного документа і додатків до нього. Несекретні додатки до

документа, якщо вони не підлягають спільному зберіганню, передаються в канцелярію під розписку на супровідному листі.

2.1.11. Після реєстрації документи передаються для розгляду керівникам підприємства або особі, якій вони адресовані.

## 2.2. Друкування і розмноження документів.

2.2.1. Друкування документів із грифом “комерційна таємниця” здійснюється в приміщенні підрозділу економічної безпеки. До початку друкування документи реєструються в журналі форми № 2.

2.2.2. На кожному надрукованому екземплярі документа проставляється в правому ріжку поля ступінь грифа важливості документа, визначеного як такий, що містить комерційну таємницю, а при необхідності — позначкою “Особисто”.

На останній сторінці кожного екземпляра надрукованого документа вказуються: реєстраційний номер, кількість надрукованих екземплярів, з чого друкувався документ, список адресатів, прізвища виконавця і друкарки (оператора ПК), дата друкування. Реєстраційний номер проставляється на кожній сторінці документа.

2.2.3. Зняття копій і проведення виписок з документів здійснюється за письмовим дозволом керівника структурного підрозділу або підрозділу економічної безпеки. Копії документів і виписки з них враховуються за новими обліковими номерами. При цьому на документах і в журналі обліку робиться позначка, коли і скільки екземплярів знято, за якими номерами вони на обліку.

## 2.3. Оформлення, адресування і відправлення вихідних документів.

2.3.1. Вихідна кореспонденція з грифом “комерційна таємниця” відправляється тільки підрозділом економічної безпеки через спецв'язок.

2.3.1. Облік підготовлених документів здійснюється в журналі форми № 2.

2.3.2. Перед вкладанням у пакет документи обгортаються світлопроникним папером. Пакет заклеюється і прошивається хрест-навхрест нитками або скріпками з таким розрахунком, щоб були захоплені всі його клапани. Якщо вкладені документи не можна проколювати, то пакет прошивається хрест-навхрест через середину всіх його країв так, щоб нитка туго схоплювала вміст і зав'язувалася в центрі зворотного боку пакета. Паперова наклейка з відбитком печатки “Для пакетів” наклеюється силікатним клеєм на центр зворотного боку пакета, щоб вузол прошивання був закритий наклейкою.

2.3.4. На пакеті проставляються наступні реквізити: гриф пакета — у правому верхньому ріжку і завірений печаткою пакетів підпис особи, що здійснювала пакування; нижче — адреса одержувача, адреса відправника і реєстраційні номери вкладених документів.

2.3.5. Кореспонденція відправляється по реєстрах через органи спецзв'язку. У межах міста кореспонденція може доставлятися адресатам за розносними книгами або розписками виконавцем документа або кур'єром підприємства за згодою керівника підрозділу економічної безпеки, на службовому автотранспорті або особистих автомашинах.

#### 2.4. Оформлення, облік і зберігання робочих зошитів.

2.4.1. Для ведення записів конфіденційного характеру виконавцям видаються робочі зошити, що обліковуються в журналі (форма № 3). Аркуші зошитів нумеруються, прошиваються, опечатуються і завіряються підписом працівника підрозділу безпеки.

2.4.2. Чернетки документів із грифом “комерційна таємниця” дозволяється робити на окремих аркушах, що підлягають обліку в журналі № 3 (друга половина журналу).

#### 2.5. Складання номенклатури. Зберігання справ.

2.5.1. З метою правильного формування справ, надійного зберігання документів розробляється номенклатура справ, у яку повинні включатися всі справи, що ведуться на підприємстві. Номенклатура справ повинна містити наступні позиції: порядковий обліковий номер справи; її заголовок, гриф, прізвище виконавця, якому надане право користуватися справою; дата початку складання і закінчення справи; термін зберігання; примітка.

2.5.2. Номенклатура справ розробляється підрозділом економічної безпеки разом з керівниками структурних підрозділів наприкінці поточного року на наступний рік. Номенклатура справ підписується керівником підрозділу економічної безпеки і затверджується керівником підприємства.

2.5.3. Формування справ, їх оформлення здійснюються згідно з постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

2.5.4. На обкладинці справи (тому) указується гриф (відповідно до ступеня важливості відомостей, що становлять комерційну таємницю), номер справи (тому), заголовок (найменування справи) або при необхідності шифр теми, дата початку складання справи, кількість сторінок справи (тому), а також термін його зберігання.

2.5.5. Усі закінчені виробництвом справи повинні бути правильно оформлені: аркуші справи зброшуровані і пронумеровані, складений внутрішній опис, на описі і на спеціально підшитій сторінці наприкінці справи (тому) зроблений напис, що засвідчує кількість сторінок, які знаходяться в справі, і документів (цифрами і прописом).

2.5.6. Вилучення зі справи документів здійснюється у виняткових випадках із залишенням у справі довідки-заступника. У випадку безповоротного вилучення зі справи документів у внутрішньому описі справи і формах обліку робляться відповідні відмітки.

2.5.7. Номенклатура справ зберігається постійно, а реєстраційні журнали — не менше 5 років.

2.5.8. Закінчені виробництвом справи зберігаються на підприємстві протягом 5 років.

### **III. Знищення документів**

3.1. Знищенню підлягають документи і справи, що втратили практичне значення і не мають наукової, історичної або комерційної цінності.

3.2. Документальні матеріали знищуються на підставі рішення експертної комісії, що створюється на підприємстві.

3.3. Справи і документи з закінченими термінами зберігання знищуються в комісійному порядку зі складанням відповідного акта (зразок додається), що підписується всіма членами комісії і затверджується керівником підприємства.

3.4. Знищення документальних матеріалів здійснюється шляхом спалювання або подрібнення на спеціальних машинах.

### **IV. Перевірка наявності документів**

4.1. Співробітники підрозділу економічної безпеки не менше одного разу в квартал перевіряють наявність всіх отриманих і надрукованих документів із грифом “комерційна таємниця”, облікованих за період, що перевіряється, з оцінкою про результати перевірки в спеціальному робочому зошиті.

4.2. Відразу після закінчення року здійснюється перевірка наявності всіх документів і справ з грифом “комерційна таємниця”, для чого наказом по підприємству призначається спеціальна комісія в складі не менше трьох співробітників з числа осіб, що мають пряме відношення до документів, які перевіряються.

4.3. За результатами перевірки складається акт, у якому вказується:

- а) вид перевірки;
- б) склад комісії;
- в) загальна кількість взятих на облік документів і справ;
- г) дані про наявність цих документів;
- д) виявлені порушення вимог даної інструкції й інших порушень режиму в роботі з конфіденційною інформацією;
- е) висновки і пропозиції за результатами перевірки.

Акт підписується членами комісії і затверджується керівником підприємства або його заступником.

4.4. Нестача документів з грифом “комерційна таємниця” розглядається як надзвичайна подія і про це негайно доповідається керівникові підприємства.

4.5. Підрозділ економічної безпеки не менше одного разу в квартал перевіряє дотримання виконавцями порядку зберігання документів з грифом “комерційна таємниця” і роботу з ними на робочих місцях.

## **V. Обов'язки, права і відповідальність співробітників підрозділу безпеки по веденню діловодства документів, що становлять комерційну таємницю**

5.1. Співробітники підрозділу безпеки зобов'язані:

5.1.1. Організовувати і вести належний облік документів із грифом “комерційна таємниця”, забезпечувати їхнє надійне зберігання.

5.1.2. Забезпечувати чітке обслуговування діловодством виконавців.

5.1.3. Суворо дотримуватись вимог “Положення про дозвільну систему доступу виконавців до документів і відомостей, що складають комерційну таємницю підприємства”, видавати документи для роботи тільки тим виконавцям, яким надане право користування ними.

5.1.4. Здійснювати кварталну і річну перевірку наявності документів із грифом “комерційна таємниця”, перевіряти порядок поводження з ними виконавців на робочих місцях, знищувати в комісійному порядку документи, що не потрібні в роботі.

5.1.5. Проводити з виконавцями роз'яснювальну роботу з питань режиму поводження з документами і відомостями, що складають комерційну таємницю.

## 5.2. Співробітники підрозділу мають право:

5.2.1. Вимагати від виконавців і контролювати забезпечення встановленого даною інструкцією порядку обліку, зберігання, розмноження і користування документами, що містять комерційну таємницю.

5.2.2. Вживати заходів щодо запобігання розголошенню і витоку комерційних секретів при веденні діловодства, а також при веденні відкритого службового листування і публікації матеріалів, звільнених від цензурського контролю.

5.2.3. Здійснювати перевірки стану режиму поводження з документами з грифом “комерційна таємниця” на робочих місцях виконавців.

5.2.4. Вимагати від працівників підприємства надання письмових пояснень за фактами розголошення комерційних секретів, втрати документів, виробів або продукції, що містять таку інформацію, подавати керівникам підприємства клопотання про покарання виконавців за зазначені вище факти й інші порушення при роботі з документами, що містять комерційну таємницю.

## 5.3. Співробітники підрозділу безпеки несуть відповідальність:

5.3.1. За збереження документів із грифом “комерційна таємниця”.

5.3.2. За невиконання обов’язків і використання прав, передбачених теперішньою інструкцією.

5.3.3. За правильність рекомендацій, що надаються виконавцям з питань підготовки, розмноження і поводження з документами з грифом “комерційна таємниця”.

5.3.4. За своєчасність і якісне проведення перевірки наявності документів із грифом “комерційна таємниця”, а також за їх знищення.

## **Підрозділ економічної безпеки підприємства**

## Форма №1

### ЖУРНАЛ обліку пакетів

Номер та дата реєстру (Розписки, розносної книги). Кількість пакетів	Номери пакетів по порядку та їх гриф конфіденційності	Номери документів, зазначених на пакеті	Розписка фельд'єгера (кур'єра), який доставив кореспонденцію, з зазначенням дати та часу	Розписка співробітника підрозділу безпеки з зазначенням дати та часу отримання пакетів
1	2	3	4	5

## Форма №2

Гриф конфіденційності

### ЖУРНАЛ обліку вхідних, вихідних та внутрішніх документів

Порядковий №	Дата реєстрації	№, дата вхідного (вихідного) документа, гриф конфіденційності	Звідки надійшов або куди відправлений документ	Короткий зміст документа	Прізвище виконавця внутрішнього документа	Кількість				Кому виданий документ	Розписка в отриманні документа, дата	Розписка в прийомі документа від виконавця, дата	Місце знаходження документа (№ справи, № акта про знищення, дата)	примітка
						Примірників	Сторінок в примірнику	Сторінок основного документа	Сторінок додатка					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Форма №3

**ЖУРНАЛ**  
обліку робочих зошитів

Порядковий №	Дата реєстрації	Гриф конфіденційності	Кількість аркушів	Кому виданий (підрозділ, прізвище, ініціали)	Розписка виконавця в отриманні і дата	Примітка
1	2	3	4	5	6	7

Форма №4

**ЖУРНАЛ**  
обліку карток про допуск до конфіденційної інформації

Порядковий №	П.І.Б співробітника. Гриф конфіденційності	Посада співробітника	Прізвище керівника, який надав допуск до конфіденційної інформації	Дата надання допуску	Дата припинення допуску	Номер та дата акта розміщення карточки про допуск	Примітка
1	2	3	4	5	6	7	8

## Гриф конфіденційності

**КОНТРОЛЬНА КАРТКА**  
попереднього обліку відомостей  
(матеріалів, виробів, дослідних зразків),  
які можуть складати комерційну таємницю

1. Найменування відомостей \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

2. Гриф конфіденційності \_\_\_\_\_

3. Список осіб, які мають (можуть мати) доступ до цих відомостей  
(зразків, виробів) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(прізвище, ініціали, посада)

4. Місцезнаходження документів, виробів, зразків \_\_\_\_\_  
\_\_\_\_\_

5. Відповідальний за збереження \_\_\_\_\_  
\_\_\_\_\_

(прізвище, ініціали, посада)

6. Строк знаходження на контролі \_\_\_\_\_

**Керівник підрозділу**

« \_\_\_\_ » \_\_\_\_\_ 200\_\_ р.

**Гриф конфіденційності**

Затверджую

Керівник підприємства

« \_\_\_\_ » \_\_\_\_\_ 200\_\_ р.

**АКТ****на знищення документів та справ**

Комісія в складі \_\_\_\_\_

(прізвище, ініціали, посада)

відібрала для знищення наступні документи, що втратили практичне значення та не мають наукової і історичної цінності:

1	2	3	4	5	6	7	8
№	Обліковий номер та дата документа або справи	Гриф конфіденційності	Найменування документа або справи	Кількість примірників	№ примірників, томів	Кількість сторінок в примірнику, томі	Всього сторінок

Всього підлягає знищенню \_\_\_\_\_

(прописом)

найменування документів у кількості \_\_\_\_\_

(прописом)

Примірників справ у \_\_\_\_\_ томах.

ПІДПИСИ:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Правильність виконаних записів в акті з даними обліку звірів

\_\_\_\_\_ (підпис, прізвище, ім'я, по батькові, посада)

Документи та справи перед знищенням з записами в акті звірили та повністю знищили шляхом \_\_\_\_\_

« \_\_\_\_ » \_\_\_\_\_ 200\_\_ р.

**ЧЛЕНИ КОМІСІЇ**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(підписи)

“ \_\_\_\_ ” \_\_\_\_\_ 200\_\_ р.

## ПЕРЕЛІК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Конституція України //Закони України: В 11 т. — К.: Ін-т законодавства, 1997. — Т 10. — С.3–41. //www.zakon.rada.gov.ua
2. Господарський кодекс України №436-IV від 16 січня 2003 р. — К.: Велес, 2006. — 160 с. //www.zakon.rada.gov.ua
3. Кодекс законів про працю України від 10 грудня 1971 р. — Х.:Рубікон, 1997. //www.zakon.rada.gov.ua
4. Кримінальний кодекс України №2341-III від 5 квітня 2001 р. //Голос України. — 2001. — 19 червня //www.zakon.rada.gov.ua
5. Цивільний кодекс України №435-IV від 16 січня 2003 р. — К.: Кондор, 2004. — 402 с. //www.zakon.rada.gov.ua
6. Про банки і банківську діяльність: Закон України №2121-III від 7 грудня 2000 р. //ВВРУ. — 2001. — №5–6 //www.zakon.rada.gov.ua
7. Про господарські товариства: Закон України №1576-XII від 19 вересня 1991 р. // ВВРУ. — 1991. — №49 //www.zakon.rada.gov.ua
8. Про державну таємницю: Закон України №3855-XII від 21 січня 1994 р. //Бюлетень законодавства і юр. практики України. — 1998, №7. — 272 с. //www.zakon.rada.gov.ua
9. Про захист від недобросовісної конкуренції: Закон України №236/96 від 07.06.1996 р. //ВВРУ. — 1996. — №36 //www.zakon.rada.gov.ua
10. Про захист економічної конкуренції: Закон України №2210-III від 11 січня 2001 р. //ВВРУ. — 2001. — №12.
11. Про інформацію: Закон України №2657-XII від 2 жовтня 1992 р. //Бюлетень законодавства і юр. практики України. — 1998, №7. — 272 с. //www.zakon.rada.gov.ua
12. Про колективні договори та угоди: Закон України №3356-XII від 1 липня 1993 р. // ВВРУ. — 1993. — № 36 //www.zakon.rada.gov.ua

13. Про комерційну таємницю: проект закону №4188 від 7 грудня 1999 р. // [www.zakon.rada.gov.ua](http://www.zakon.rada.gov.ua)
14. Про науково-технічну інформацію: Закон України №3322-ХІІ від 25 червня 1993 р. // [www.zakon.rada.gov.ua](http://www.zakon.rada.gov.ua)
15. Про перелік відомостей, які не є комерційною таємницею: Постанова Кабінету Міністрів України № 611 від 9 серпня 1993 р. // Збірник постанов Уряду України. — 1993. — № 12 // [www.zakon.rada.gov.ua](http://www.zakon.rada.gov.ua)
16. *Адрианов В., Бородин В., Соколов А.* Шпионские штучки и устройства для защиты объектов информации. Справочное пособие. — СПб.: Лань. 1996.
17. Альбом до семінару “Забезпечення комплексної безпеки підприємницьких структур”. Українська економічна студія. — К., 1998.
18. *Андрощук Г.А., Крайнев П.П.* Экономическая безопасность предприятия: защита коммерческой тайны: Монография. — К.: Издательский Дом “Ин Юре”, 2000. — 400 с.
19. *Анин Б.* Радиоэлектронный шпионаж. — М.: Центрполиграф, 2000.
20. *Атаманенко И.* Шпионские страсти. — М., 2000.
21. *Батулин Ю., Жодзишский А.* Компьютерная преступность и компьютерная безопасность. — М.: Юридическая литература, 1991.
22. *Безопасность.* Дайджест. — Харьков: Альфа-Б, 1992
23. *Безопасность бизнеса: Справоч. пособие /* Под ред. Ю. И. Когута. — К., 1993.
24. *Бержье Ж.* Промышленный шпионаж.— К.: Норматив, 1993.
25. *Боженкова А.* Слышащий спецпенек // *Новости разведки и контрразведки.* — 1997. — №4.
26. *Боттом Н., Галатти Р.* Экономическая разведка и контрразведка: Практическое пособие. — Новосибирск, 1994, (пер. с англ.).
27. *Вартаросян В.* Радиоэлектронная разведка. — М.: Воениздат, 1991.
28. *Вопросы изучения клиентов с позиции службы безопасности,* 1996.
29. *Всемирная история шпионажа. (История тайной дипломатии и разведывательной деятельности секретных служб мира).* Автор-составитель М.И. Умнов — М., 2000.
30. *Галатенко В.* Информационная безопасность// *Компьютерное обозрение.* — 1996. — № 33–35.
31. *Гасанов Р.М.* Промышленный шпионаж на службе монополий. — М.: Междунар. отношения, 1996.
32. *Гасанов Р.М.* Шпионаж и бизнес. — М.: ТОО ПКФ “Сааги”, 1993. — 320 с.

33. *Гелен Р.* Война разведок. Тайные операции спецслужб Германии 1942–1971. — М., 1999 (пер. с нем.).
34. *Гераскин Б.В.* За семью печатями. Записки военного контрразведчика. — М.: Международные отношения, 2000.
35. *Гончаров В.В.* В поисках совершенствования управления. Руководство для высшего управленческого персонала. Опыт лучших промышленных фирм США, Японии и стран Западной Европы. — М., 1992.
36. *Грунин О.А., Грунин С.О.* Экономическая безопасность организации. — СПб.: Питер, 2002. — 160 с.
37. *Гуленко В.В., Молодцов А.В.* Соционика для руководителя. Кн. I. Введение в соционику: Метод, рекомендации. — 2-е изд. — К.: МЗУ-УП, 1993.
38. *Гуленко В.В., Молодцов А.В.* Соционика для руководителя. Кн. II. Основы социоанализа: Метод, рекомендации. — 2-е изд. — К.: МЗУ-УП, 1993.
39. *Давыдов И.* Тайна фирмы. — К.: “Фирма-колир 2”, 1993.
40. *Даллес А.* Искусство разведки: Пер. с англ. с сокращениями. — М.: Междунар. отношения, 1992. — 288 с.
41. *Де Лутиш Д.* История итальянских секретных служб. — М., 1989 (пер. с итал.).
42. *Доронин А.И.* Бизнес-разведка. — М.: Издательство “Ось-89”, 2002. — 288 с.
43. *Доронин А.И.* Основы экономической разведки и контрразведки. Тула.: Гриф и К., 2000. — 276 с.
44. *Доронин А.И.* Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия. — Тула.: Гриф и К., 2000. — 116 с.
45. *Драга А.* Комплексное обеспечение безопасности фирмы. — М., 1996.
46. *Духов В.Е.* Экономическая разведка и безопасность бизнеса. — К.: ИМСО МО Украины, НВФ “Студцентр”, 1997. — 176 с.
47. *Кавеладдзе И.Т.* Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации). “Экокнсалтинг”. — М., 1992.
48. *Казакевич О.Ю.* Предприниматель в опасности: способы защиты. Практическое руководство для предпринимателей и бизнесменов. Объединение УП-ПИКС. — М., 1992.
49. *Калмыков М.* Шпион Востока? //Новости разведки и контрразведки. — 1996. — № 24.

50. Компьютерный терроризм: новейшие технологии на службе преступного мира/ Автор-составит. Т. Н. Ревяко. — М.: Литература, 1997. — 640 с.
51. *Кристофер Э., Гордиевский О.* КГБ. История внешнеполитических операций от Ленина до Горбачева. — М.: МП “Принт-Комплекс”, Изд. “NotaVene”. — 766 с.
52. *Крысин А.В.* Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996.
53. *Кузнецов И.Н.* Учебник по информационно-аналитической работе. М.: Яуза, 2001. — 320 с.
54. *Ларичев В.Д.* Как уберечься от мошенничества в сфере бизнеса. — М., 1996.
55. *Лисичкин В.А., Шелепин Л.А.* Третья мировая информационно-психологическая война. — М., 1999.
56. *Лотц В.* Шпион в шампанском. — М.: Центрполиграф, 2001 (пер. с нем.).
57. *Лукашин В.И.* Экономическая безопасность: Учебно-практическое пособие / Моск. гос. ун-т экономики, статистики и информатики. — М.: МЭСИ, 1999.
58. *Лысов А., Остапенко А.* Телефон и безопасность. — СПб.: Лаборатория ПППШ, 1995.
59. *Лямин И.* Внутренняя безопасность фирмы // Бизнес-информ. — 1992. — № 21.
60. *Лямин И.* Служба безопасности: скупой платит дважды // Бизнес-информ. — 1992. — № 6.
61. *Мак-Мак В.П.* Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности. — М.: Мир безопасности, 1999.
62. *Маккей Х., Карлоф Б.* Как уцелеть среди акул: опередить конкурентов в умении продавать, руководить, стимулировать, заключать сделки. Деловая стратегия: концепция, содержание, символы. — М., 1993 (пер. с англ.).
63. *Меньшиков А.А.* Правовые вопросы передачи ноу-хау в международной торговле: Автореф. дисс. на соискание ученой степени к.ю.н. — М.: ИГПАН СССР, 1983.
64. Министр обороны или агент // Новости разведки и контрразведки. — 1997. — № 1.
65. *Мироничев С.* Коммерческая разведка и контрразведка, или Промышленный шпионаж в России и методы борьбы с ним. — М., 1995.

66. Мобильные телефоны таят угрозу // Новости разведки. — 1996. — № 20.
67. *Нікіфоров Г.К., Нікіфоров С.С.* Підприємництво та правовий захист комерційної таємниці: Навч.-практ. посіб.для вищих навч. закл. — К.: Олан, 2001. — 208 с.
68. Основные и первоочередные задачи службы безопасности. — Безопасность. Дайджест. — Харьков: Альфа-5, 1992.
69. Основы экономической безопасности. Учебно-практическое пособие под ред. Е.А. Олейникова — М.: ЗАО “Бизнес-школа “Интел-Синтез”, 1997.
70. Охотники за секретами. //Новости разведки и контрразведки. —1997.
71. Охотницы за чужими тайнами // Новости разведки и контрразведки. — 1997. — № 5.
72. *Панарин И.Н.* Информационная война и власть. — М.; Мир безопасности, 2001.
73. *Полмар Н., Аллен Т.* Энциклопедия шпионажа. — М., 1999 (пер. с англ.).
74. *Портер М.* Международная конкуренция. — М., 1993 (пер. с англ.).
75. *Почепцов Г.Г.* Психологические войны. — М., 2000.
76. Практика защиты коммерческой тайны и интеллектуальной собственности в США. — К.: Хрещатик, 1996.
77. *Пешков В.* Петербургские программисты сказали пароль и пошли// Коммерсантъ. — 1992. — № 33.
78. *Путилов С.* Тайная дипломатия Ватикана// Новости разведки и контрразведки. — 1996. — № 20.
79. Рекомендации по организации защиты коммерческой тайны в ИЭС им. Е.О. Патона. Научный руководитель В.Н. Сериков. — К., 1991.
80. *Ричелсон Д.Т.* История шпионажа XX века. — М., 2000 (пер. с англ.).
81. *Саниахметова И.О.* Правовий захист підприємництва в Україні. — К.: Юрінком Інтер, 1999.
82. *Свердлов Ш.Б.* Вольный экономист против всей королевской рати // ЭКО. — 1990. — № 12.
83. *Севрук В.Т.* Риски финансового сектора РФ: Практическое пособие. — М.: ЗАО “Финстат информ”, 2001.
84. *Сибирский Б.* Избежание угрозы// Новости разведки и контрразведки. — 1996. — № 24.
85. *Скотт Синк Д.* Управление производительностью. — М.: Прогресс., 1989.

86. *Соловьёв Э.* Коммерческая тайна и её защита. — М.: ЗАО “Бизнес-школа “Интел-Синтез”, 1997.
87. *Степашин С.В., Шульц В.Л.* Вопросы безопасности в системе государственного и муниципального управления. Ч. 1. Общие принципы и геополитические аспекты безопасности РФ. — СПб.: СПбГТУ, 1994.
88. *Суворов В.* Аквариум. — Черкассы: Сияч, 1993.
89. *Сунь-Цзы.* Трактат о военном искусстве. — М.: Воениздат, 1935.
90. *Терентьев Д.* Пираты XXI века // Вне закона. — 1998. — № 2.
91. *Тотров Ю.* Как Япония добывает развед. информацию // Новости разведки и контрразведки. — 1996. — № 19.
92. *Хаит Ч., Захарьян В.* Разведка на службе вашего предприятия. — К.: Укрзакордонвизасервис, 1992.
93. *Чернявский А.А.* Безопасность предпринимательской деятельности. Конспект лекций. — К.: МАУП, 1998. — 124 с.
94. *Чернявский А.А.* Промышленный шпионаж и безопасность предпринимательства. — К.: МАУП, 1996. — 64 с.
95. *Шаваев А.Г.* Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы. — М.: Концерн “Банковский Деловой Центр”, 1998.
96. *Шаваев А.Г.* Криминологическая безопасность негосударственных объектов экономики. — М.: ИНФРА-М, 1995.
97. *Шевырев А.Г.* Технические средства выявления устройств контроля. — К.: Безопасность информации, 1995.
98. *Шелленберг В.* Лабиринт. — М. — СПб.: Дом Бируни, 1991.
99. *Шльков В.В.* Комплексное обеспечение экономической безопасности предприятия. — СПб.: Алетейя, 1999.
100. *Штумпф Г.* Договор о передаче ноу-хау. — М.: Прогресс, 1976. — С. 25.
101. *Юдина Е.* В режиме коммерческой тайны // Диалог. — 1992. — №№ 4–5.
102. *Ярочкин В.И., Бузанова Я.* Недобросовестная конкуренция. — М., 2000.
103. *Ярочкин В.И.* Предприниматель и безопасность. Часть 1. Несанкционированный доступ к источникам конфиденциальной информации. — М.: Экспертное бюро, 1994.
104. *Ярочкин В.И.* Предприниматель и безопасности. Часть 2. Библиотека делового человека. — М.: Выпуск II, 1994.
105. *Ярочкин В.И.* Система безопасности фирмы. — М.: Ось-89, 1997.

106. *Ladas S.P.* Licensing agreements on know-how in the United States // International Review of Industrial Property and Copyright Law. – 1972. – V. 2. – P. 184.
107. *Reimer.* Unlauter Wettbewerb, Bd III. N315.
108. *Vida A.* Immatirialguterrechtlicher Sonderschutz des know-how in Ungarn // GRUR. – 1979. – № 7. – С 333–336.
109. *Journal Loi.* The International Property Law of Japan. Sijthoff und Wordhoff. – 1990.
110. Republic aviation Corp. v. Schenk. 152. USPA830.
111. Trade secrets. Poger M. Milgrim. Matthen Bender, 1974.
112. *Zydon J.C.* The Deterrent Effect of the Uniform Trade Secrets Act // 1PTOS. – 1987. – V. 8. – P. 437–438.
113. *Soltysinski S.* The Trade Secrets Property IIC, 1981.V. 17. № 3, P. 332.
114. *Jager M.F.* A comparison of trade secret laws in Asia7/LES Nouvelles 1997. – V. XXXII. – № 2. – P. 54–59.

НАВЧАЛЬНЕ ВИДАННЯ

Тетяна Миколаївна ІВАНЮТА  
Анатолій Олександрович ЗАЇЧКОВСЬКИЙ

# ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

НАВЧАЛЬНИЙ ПОСІБНИК

Керівник видавничих проєктів – *Б. А. Сладкевич*  
Дизайн обкладинки – *Б. В. Борисов*  
Редактор – *Л. І. Єросова*  
Коректор – *С. С. Савченко*

Підписано до друку 03.10.2008. Формат 60x84 1/16.  
Друк офсетний. Гарнітура PetersburgC.  
Умовн. друк. арк. 14,4.  
Наклад 1000 прим.

Видавництво «Центр учбової літератури»  
вул. Електриків, 23  
м. Київ, 04176  
тел./факс 425-01-34, тел. 451-65-95, 425-04-47, 425-20-63  
8-800-501-68-00 (безкоштовно в межах України)  
e-mail: office@uabook.com  
сайт: WWW.CUL.COM.UA

Свідоцтво ДК № 2458 від 30.03.2006