| Житомирська політехніка | Міністерство освіти і науки України<br>Державний університет «Житомирська політехніка» |
|---|---|

# Лекція 13
# ОСНОВНІ СПОСОБИ ВЕДЕННЯ ПРОМИСЛОВОГО ШПИГУНСТВА

Навчальна та виховна мета:
ознайомлення студентів з теоретичними основами щодо способів та методів ведення промислового шпигунства

Література: Л.9.-Л.11, Л.16, С. 45-74, Л.17, С.26-36, Л.39, С.37-49, Л.41, С. 12-34

# План лекції

*13.1. Види та методи конкуренції*

*13.2. Основні напрями забезпечення захищеності і попередження погроз безпеки компанії*

*13.2.1. Концепція безпеки компанії*

*13.2.2. Забезпечення охорони офісу компанії*

*13.3. Інформаційна безпека компанії*

*13.4. Комп'ютерна безпека*

*13.5. Поняття і призначення корпоративної розвідки*

*13.5.1. Система корпоративної розвідки*

*13.5.2. Процес корпоративної розвідки*

*13.5.3. Розвідувальна діяльність фірми*

*13.5.4. Система комерційної розвідки*

*13.5.5. Контррозвідувальна діяльність*

# 13.1. Види та методи конкуренції

**Добросовісна конкуренція** – це прагнення отримання максимального прибутку шляхом створення кращих товарів і надання якісніших послуг, зниження витрат виробництва, впровадження досягнень науково-технічного прогресу і ноу-хау, раціоналізації і т.д.

Під **недобросовісною конкуренцією** розуміється запекла боротьба, що ведеться між конкурентами з використанням незаконних, деколи протиправних дій, засобів і методів з метою досягнення конкурентних переваг.

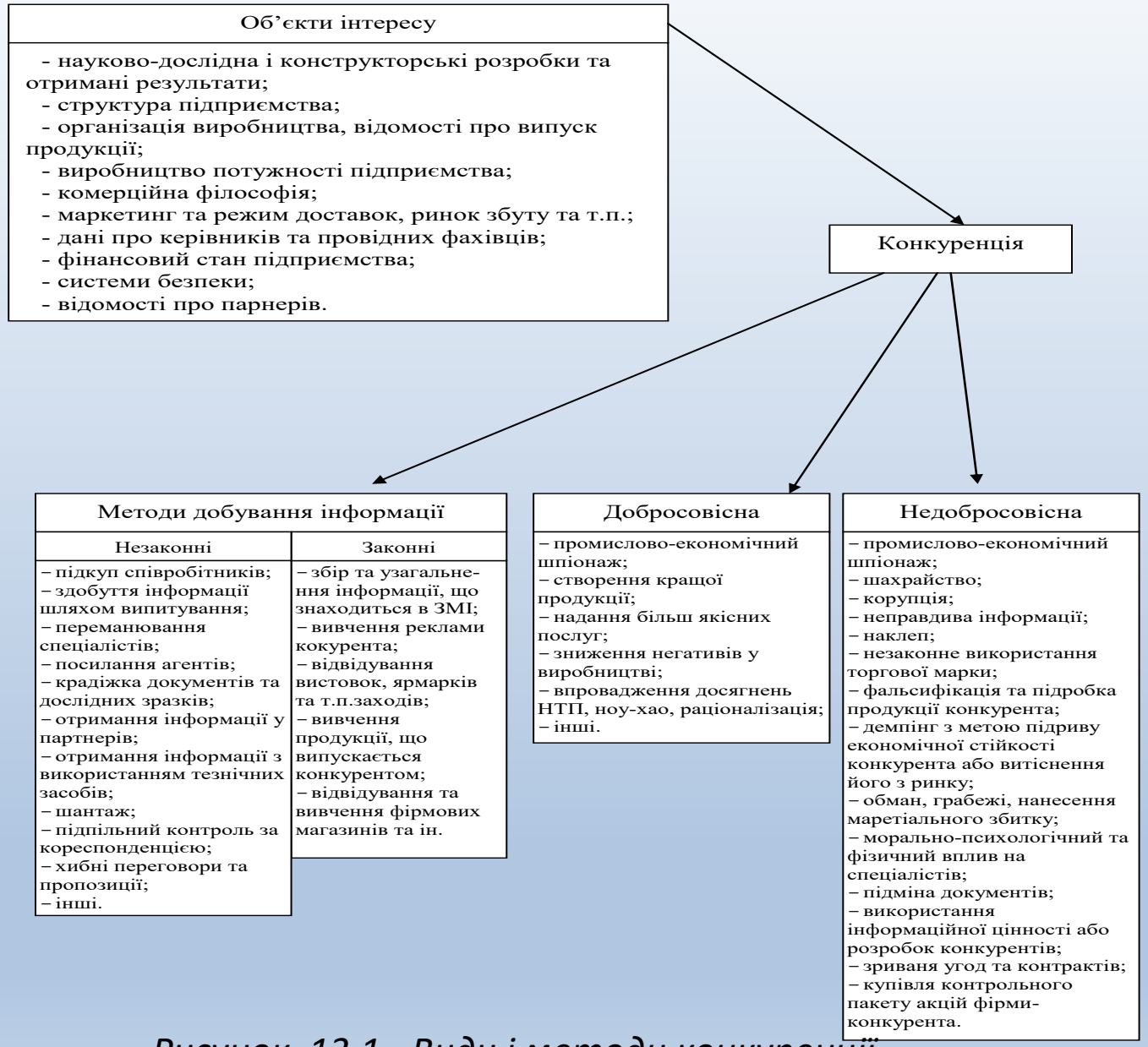


*Рисунок 13.1 - Види і методи конкуренції*

# Висновки до першого питання

1. Визначено об’єкти інтересу конкурентів.

2. Визначено, що конкуренція може бути добросовісною та недобросовісною, визначено методи та засоби даних видів конкурентної боротьби.

2. Визначено, що методи добування інформації можуть бути законними та незаконними, представлено механізми їх реалізації.

# 13.2. Основні напрями забезпечення захищеності і попередження погроз безпеки компанії

## 13.2.1. Концепція безпеки компанії

## 13.2.2. Забезпечення охорони офісу компанії

# 13.2.1. Концепція безпеки компанії

*Для створення надійної системи безпеки компанії необхідно об'єктивно оцінити ситуацію, в якій вона знаходиться.*

*Перш за все необхідно вивчити середовище на макро- і регіональному рівнях, а також на рівні партнерів і конкурентів.*

*Особлива увага повинна приділятися вивченню: партнерів; конкурентів; зовнішнього і внутрішнього середовища організації.*

# Аналіз

- забезпечення виробничого процесу різного роду ресурсами;
- міри захищеності об'єктів безпеки компанії;
- надійності кадрового потенціалу і перш за все тих, хто має доступ до комерційної таємниці і приймає відповідальні ризикові управлінські рішення;
- стану фінансового, інформаційного, кадрового, техніко-технологічного, екологічного, інтелектуального, політико-правового і силового складових економічної безпеки;
- можливості компанії по створенню, вмісту і оснащенню власної служби безпеки і так далі.

Найважливішим стратегічним напрямом забезпечення безпеки компанії є виявлення, запобігання, нейтралізація, припинення, локалізація, відбиття небезпек і погроз.

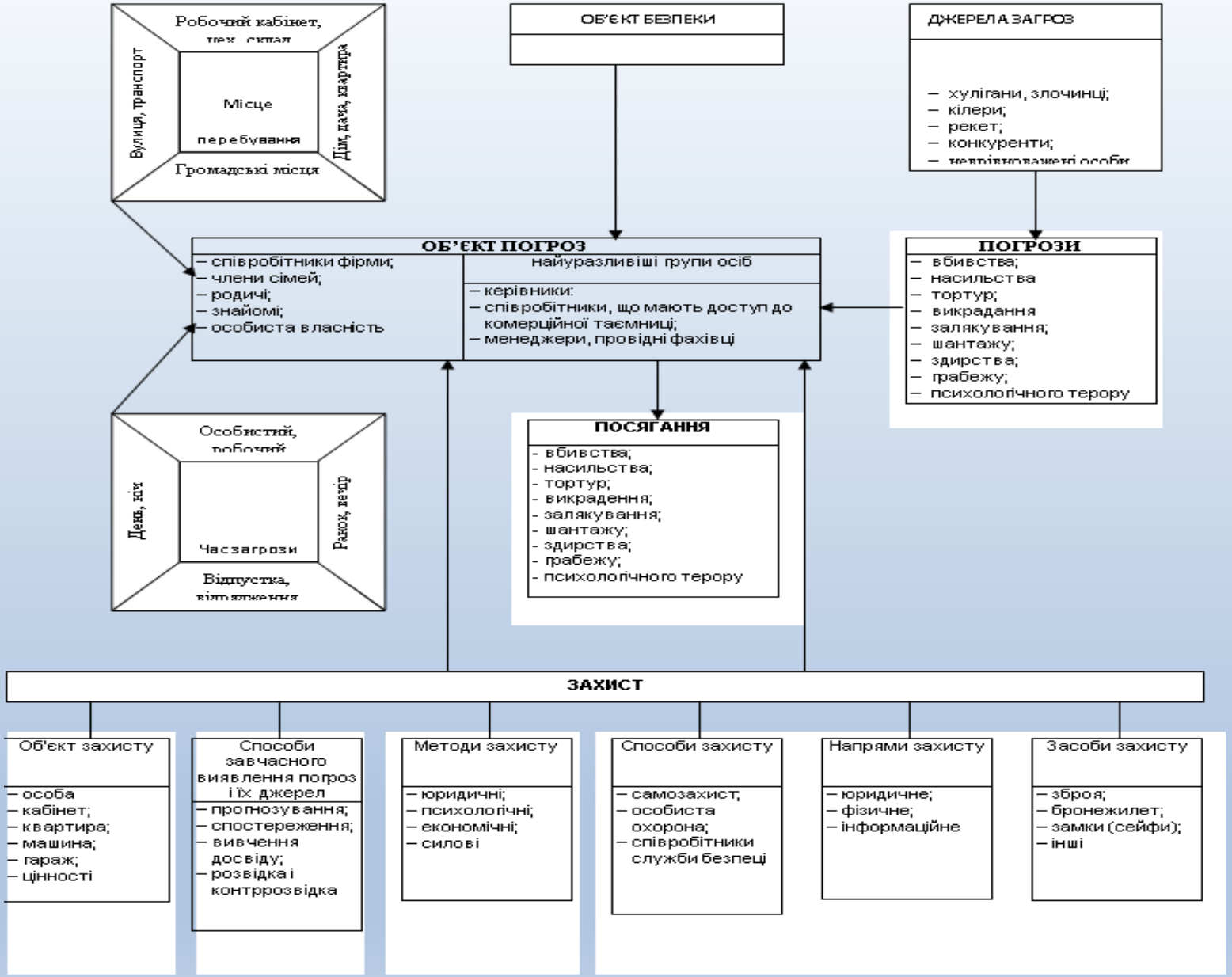


Рисунок 13.2 - Принципова модель забезпечення безпеки персоналу компанії

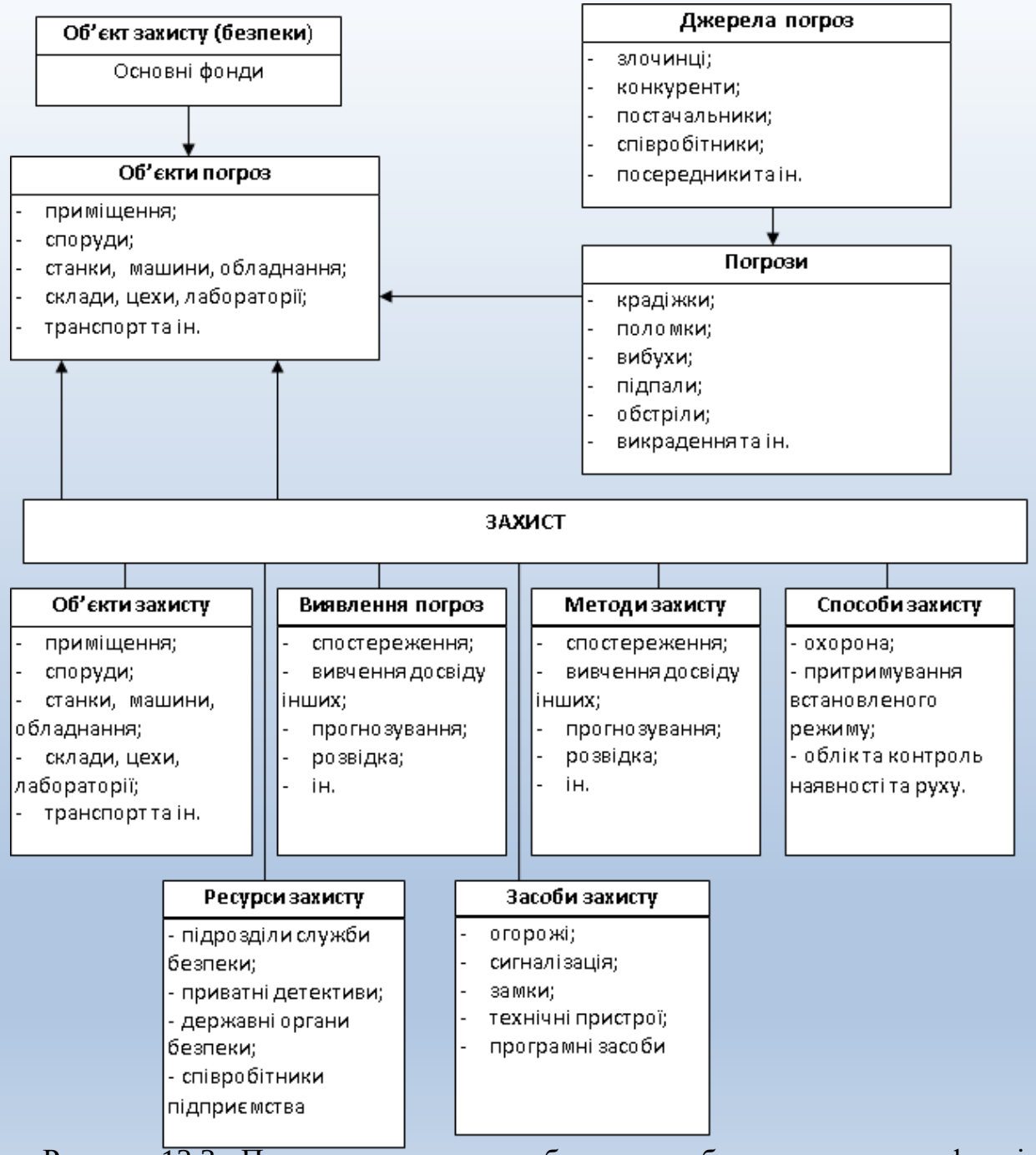


Рисунок 13.3 - Принципова модель забезпечення безпеки основних фондів

# 13.2.2. Забезпечення охорони офісу компанії

Система охорони офісу є базисом корпоративної безпеки.

Система охорони залежить від цілої низки факторів, а саме:

- географічне положення будівлі офісу в місті;
- величина загальної площі приміщень офісу;
- сусідство з іншими адміністративними будівлями або приміщеннями;
- чисельний склад адміністрації, що постійно працює в офісі;
- режим роботи адміністрації (протягом робочого дня або цілодобово);
- характер діяльності компанії і витікаючи звідси специфіка роботи з клієнтами.

# Завдання внутрішньої охорони

- виявлення і видалення небажаних осіб, яким вдалося проникнути через зовнішню охорону;
- безпосередня охорона приміщень офісу від можливих недоброзичливих дій з боку сусідів;
- забезпечення внутрішнього порядку, контроль за дотриманням прийнятих в приміщеннях офісу режимів;
- недопущення несанкціонованого винесення працівниками фірми або клієнтами з приміщень офісу майна, техніки, документів фірми;
- особиста охорона керівника фірми або інших членів адміністрації, якщо в тому є необхідність.

*У разі, коли компанія займає під офіс всю будівлю цілком або частина будівлі з окремим входом, організація як зовнішньої, так і внутрішньої охорони – справа самої компанії.*

# Висновки до другого питання

1. Для створення надійної системи безпеки компанії необхідно об'єктивно оцінити ситуацію, в якій вона знаходиться. При цьому необхідно приділити увагу вивченню зовнішнього та внутрішнього середовища, партнерів, конкурентів.
2. На основі отриманої узагальненої нформації розробляється і офіційно затверджується концепція безпеки компанії.
3. Найважливішим стратегічним напрямом забезпечення безпеки компанії є виявлення, запобігання, нейтралізація, припинення, локалізація, відбиття небезпек і погроз.
4. Для реалізації стратегічного напряму безпеки для кожного об'єкту безпеки (матеріальні цінності, продукція, персонал, інформація і т. д.) має бути розроблена принципіальна, концептуальна модель (алгоритм) безпеки.
5. Від ефективності системи охорони офісу компанії багато в чому залежить безпека компанії в цілому, у тому числі економічна і інформаційна. Таким чином, система охорони офісу є базисом корпоративної безпеки.

# 13.3. Інформаційна безпека компанії

Сукупність відомостей, що використовуються і циркулюють в підприємницькій діяльності, зазвичай групують по таких напрямах:

1.Підприємницька (комерційна) інформація, яка включає відомості про виробничі фонди, стан кадрового потенціалу, чинники, що позитивно, або негативно впливають на сферу господарювання і комерції, і ін.

2. Правова інформація (відомості про чинне законодавство, що регламентує різні сфери діяльності компанії).

3. Спеціально-оперативна інформація (відомості про способи, сили і засоби забезпечення безпеки підприємницької інформації від доступу третіх осіб).

## Групи інформації, що не потребують захисту:

1. Інформація, яка не може складати комерційну таємницю.
2. Група відомостей, які невигідно приховувати від оточення самої компанії. Це стосується, перш за все, рекламної інформації.
3. Відомості, які представляють господарську цінність для компанії і є комерційною таємницею для зовнішнього середовища компанії.

# Основні етапи розробки заходів захисту конфіденційної інформації:

- визначення переліку відомостей, що відносяться до комерційної таємниці даної компанії;
- виявлення зловмисників, що можуть зазіхнути на комерційну таємницю підприємства;
- оцінка збитку, який може бути нанесений підприємству, якщо якась інформація буде розголошена;
- виявлення можливих джерел, каналів просочування інформації;
- визначення можливості їх захисту;
- розрахунок витрат на захист інформації
- визначення засобів і способів захисту комерційної таємниці.

# Висновки до третього питання

1. Сукупність відомостей, що використовуються і циркулюють в підприємницькій діяльності, зазвичай групують у підприємницьку, правову та спеціально-оперативну.
2. Визначено групи інформації, що не потребують захисту.
3. Визначено основні етапи розробки заходів захисту конфіденційної інформації.

# 13.4. Комп'ютерна безпека

Забезпечення інформаційної безпеки передбачає, з одного боку, отримання інформації, що цікавить, будь-яким шляхом, з іншої – ретельний, цілеспрямований і постійний захист власної інформації.

У сучасній теорії безпеки сформульовано три базові принципи комп'ютерної інформаційної безпеки:

цілісність даних – захист від збоїв, що ведуть до втрати інформації, а також неавторизованого створення або знищення даних;

конфіденційність інформації;

її доступність лише для авторизованих користувачів.

# Найбільш поширені погрози і види злочинів, пов'язаних з втручанням в роботу комп'ютерів:

1. Несанкціонований доступ до інформації, що зберігається в комп'ютері.
2. *Введення в програмне забезпечення «логічних бомб»* із заздалегідь визначеними задачами.
3. *Розробка і поширення комп'ютерних вірусів*.
4. *Відмови і збої («зависання») в процесі експлуатації програмно-обчислювальних комплексів*.
5. *Помилки забезпечення і підробка комп'ютерної інформації*. На жаль, ніхто не може гарантувати відсутність помилок в програмі. Вони важко виявляються і можуть мати найрізноманітніші наслідки.
6. *Розкрадання комп'ютерної інформації* в основному зводиться до несанкціонованого копіювання програмного забезпечення.
7. *До форс-мажорних обставин*, загрозливих комп'ютерній безпеці, слід віднести: *пожежі, повені, бойові дії, землетруси, терористичні акти і ін*.

## ЗАСОБИ ЗАХИСТУ:

1. *Засоби фізичною захисту*, що включають засоби захисту кабельної системи, систем електроживлення, засоби архівації, дискові масиви і так далі
2. *Програмні засоби захисту*, у тому числі антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу.
3. *Адміністративні заходи захисту*, що включають контроль доступу в приміщення, розробку стратегії безпеки фірми, планів дій в надзвичайних ситуаціях і так далі

# Висновки до четвертого питання

1. Розглянуті основні принципи комп’ютерної безпеки.
2. Проведено аналіз найбільш поширених  погроз та видів злочину, що пов’язані з використанням комп'ютерної техніки.
3. Представлені засоби захисту .

# 13.5. Поняття і призначення корпоративної розвідки

Система корпоративної розвідки – комплекс людських, матеріальних і інформаційних ресурсів, технічних засобів і технологій, процедур, методів і організаційно-правових заходів, що дозволяють корпорації вести конкурентну розвідку.

Розвідувальна діяльність, таким чином, є невід'ємною складовою частиною діяльності комерційної організації.

# *Призначення корпоративної розвідки полягає в наступному:*

*1.Забезпечити своєчасне отримання і надання надійної і всебічної інформації про майбутні можливості кожного з основних конкурентів.*

*2.Визначити, яким чином дії основних конкурентів можуть зачіпати поточні інтереси корпорації.*

*3.Постійно надавати інформацію про всі події в конкурентному оточенні і на ринку, які можуть мати важливе значення для корпорації.*

*4.Виключити дублювання і добиватися ефективності в зборі, аналізі і поширенні інформації про конкурентів і їх технологічні можливості.*

*5.5.Забезпечувати своєчасне і якісне задоволення всіх інформаційних потреб керівництва і провідних фахівців корпорації.*

# *Об'єктами корпоративної розвідки є:*

1. *Конкуренти – виробники товарів і послуг.*
2. *Постачальники матеріальних ресурсів.*
3. *Маркетингові посередники, що забезпечують просування, збут і розповсюдження товарів:*

*а) торгівельні посередники;*

*б) фірми по організації руху товару;*

*в) агентства по наданню маркетингових послуг;*

*г) кредитно-фінансові організації.*

*4. Клієнти: окремі покупці, організації і установи, що набувають товарів і послуг.*

*5. Контактні організації і групи: фінансові кола, засоби масової інформації, рекламні агентства і ін.*

*6. Адміністративні органи, що володіють офіційною інформацією про стан комерційної діяльності.*

# 13.5.1. Система корпоративної розвідки

*Система корпоративної розвідки включає ряд підсистем*:

- *підсистему отримання необхідної інформації з метою задоволення інформаційних потреб керівництва і фахівців;*
- *підсистему збору і обробки інформації;*
- *підсистему накопичення і зберігання інформації у вигляді автоматизованого банку розвідувальних даних і довідково-інформаційного фонду;*
- *підсистему інформаційного обслуговування керівників і виконавців|виконувачів| відповідного рівня.*

# 5.5.2. Процес корпоративної розвідки

*Дії корпоративної розвідки необхідно планувати з врахуванням вирішень наступних проблем:*

- *як знаходити відповіді на поставлені питання;*
- *які використовувати джерела інформації;*
- *з ким необхідно працювати;*
- *які тимчасові обмеження для дій.*

*Організація процесу добування і збору необхідної інформації:*

- *використання відкритих джерел і засобів масової інформації (ЗМІ);*
- *використання власних даних;*
- *обробка і аналіз розвідувальної інформації:*
- *систематизація і структуризація даних;*
- *всебічний системно-структурний аналіз інформації;*
- *розробка звітів і пропозицій для ухвалення рішень керівництвом.*

# *Способами добування і збору розвідувальної інформації є:*

1. *Аналіз відкритих відомостей з матеріалів засобів масової інформації, газет, журналів, реклами, радіо і телебачення і так далі.*
2. *Відвідування ярмарків, виставок, конференцій, симпозіумів з метою здобуття матеріалів і запису доповідей і виступів.*
3. *Вивчення матеріалів наукового і технічного характеру.*
4. *Вивчення патентів і матеріалів стандартизації.*
5. *Закупівля і зворотний інжиніринг продукції і товарів конкурентів.*

# 13.5.3. Розвідувальна діяльність фірми

*Розвідка є широкою і багатогранною сферою діяльності. Прямо або побічно вона пов'язана майже зі всіма галузями знань.*

*Розвідувальну діяльність можна поділити на добування матеріалу на місці (легальними і нелегальними способами), складання розвідувальної інформації і розсилку її зацікавленим особам. Для виконання цієї роботи необхідні особливі органи і всілякі|різноманітні спеціальні методи.*

*Розвідувальна інформація є осмисленими відомостями, що засновані на зібраних, оцінених фактах, викладених таким чином, що ясно видно їх значення для вирішення якого-небудь конкретного завдання.*

# 13.5.4. Система комерційної розвідки фірми

*Під терміном «система комерційної розвідки» розуміється організаційна структура, яка займається питаннями добування, збирання, перевірки (верифікації), обробки і аналізу даних по різних аспектах економічної діяльності підприємства, його партнерів з подальшим використанням отриманої інформації для вирішення конкретних завдань господарської діяльності.*

# 13.3.3 Контррозвідувальна діяльність

*Мета контррозвідувальної діяльності* *протидія розвідувальним заходам конкурентів і припинення правопорушень з боку протиправних груп та окремих осіб, що зазіхали на інтереси підприємства або його окремих співробітників.*

*На відміну від розвідки, об'єктом контррозвідувальної діяльності є не зовнішня, а внутрішнє середовище функціонування підприємства.*

## *Внутрішнє середовище функціонування підприємства включає наступні елементи:*

*Керівний склад підприємства* (директор, його заступники, головний бухгалтер і т. д.) як потенційні об'єкти розвідувальних заходів з боку конкурентів.

*Особи з допоміжного персоналу,* що мають доступ до комерційної таємниці (секретарі, працівник канцелярії і т. д.).

*Співробітники*, з боку яких потенційно існує небезпека надання злочинним елементам таких відомостей, які допоможуть їм скоїти злочини (сторож, охоронці, водії персональних машин і т. д.).

*Співробітники самої служби безпеки.*

*Особи, що мають судимість* з числа працівників підприємства.

*Співробітники підприємства, родичі яких працюють у конкурентів.*

*Особи, що раніше звільнилися з підприємства.*

*Особи, які через свої посадові обов'язки регулярно приймають відвідувачів підприємства.*

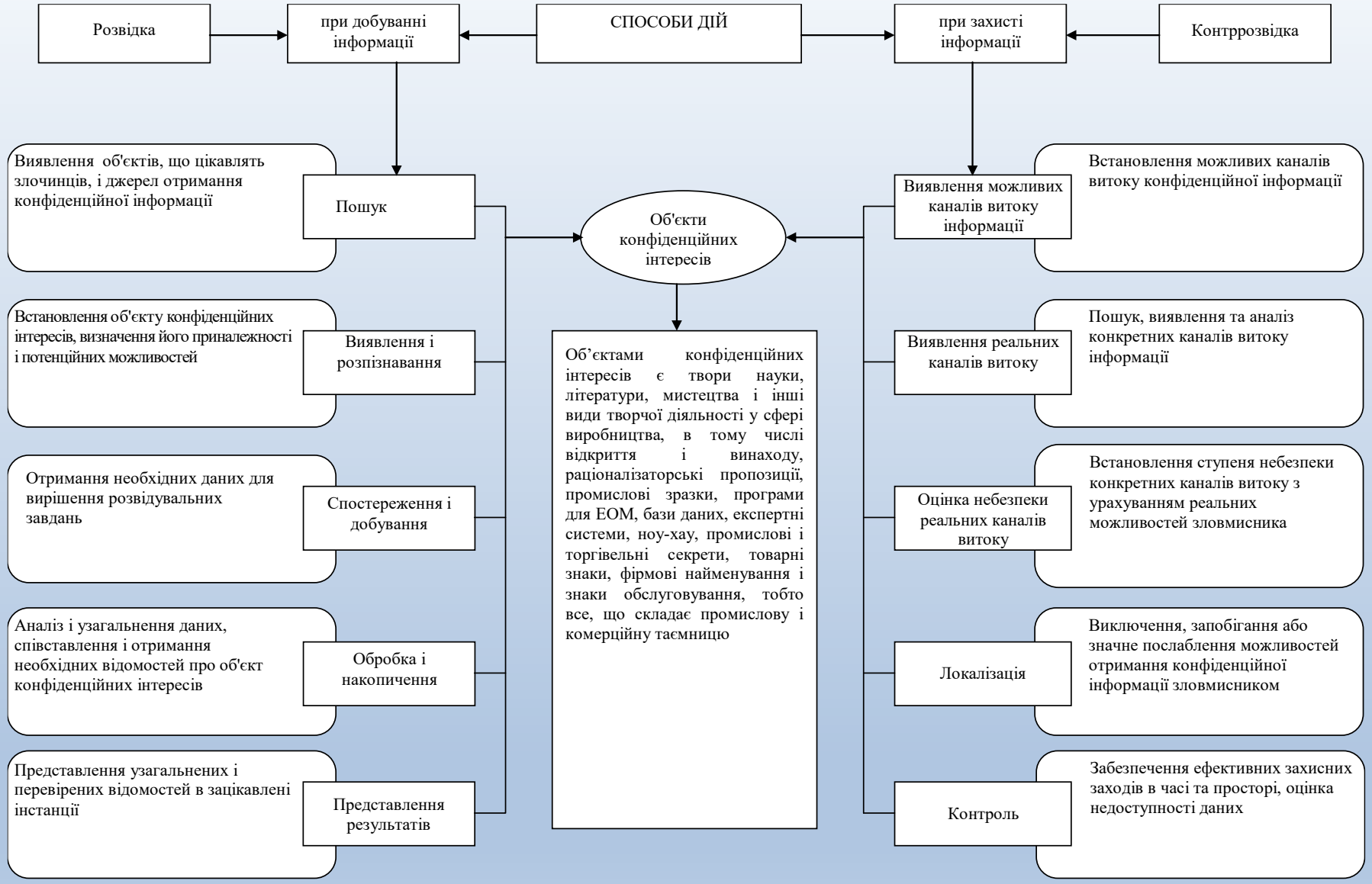


рис. 8.5. Взаємодія органів розвідки і контррозвідки по відношенню до об'єктів конфіденційних інтересів

# Висновки до п’ятого питання

1. *Розглянуті поняття та основна мета корпоративної розвідки.*
2. *Розглянуто систему та процес, що використовуються в  корпоративній розвідці*
3. *Розглянуті питання методів та щасобів розвідувальної діяльність фірми.*
4. *Проведено аналіз системи комерційної розвідки*
5. *Представлено методи, засоби та заходи*

*контррозвідувальної діяльності*