

З.Б. ЖИВКО

ЕКОНОМІЧНА БЕЗПЕКА
ПІДПРИЄМСТВА:
СУТНІСТЬ, МЕХАНІЗМ
ЗАБЕЗПЕЧЕННЯ
ТА УПРАВЛІННЯ

Монографія

Львів
Ліга-Прес
2012

УДК 33(075.8)
ББК 65я73

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 5 від 26 грудня 2012 року).

Рецензенти:

О.О. Сунцова, доктор економічних наук, професор,
професор кафедри фінансів та банківської справи ВНЗ
«Національна академія управління»,

академік Української академії економічних наук;

М.І. Флейчук, доктор економічних наук, професор,
професор кафедри міжнародних економічних відносин
Львівської комерційної академії;

І.В. Пенькова, доктор економічних наук, професор,
професор кафедри «Зовнішньоекономічна діяльність»
Донецького національного технічного університету;

В.В. Борщевський, доктор економічних наук, доцент,
завідувач відділу прогнозування та моделювання розвитку регіону
Інституту регіональних досліджень НАН України.

Живко З. Б.

Ж66 Економічна безпека підприємства: сутність, механізм забезпечення та управління: монографія / З. Б. Живко. – Львів : Ліга-Прес, 2012. – 256 с.

ISBN 978-966-397-132-6

У монографії висвітлюються теоретико-методологічні та методичні засади забезпечення безпеки підприємства. Розроблено механізм управління комплексною системою економічної безпеки підприємства та створено концепцію управління економічною безпекою на мікрорівні. Здійснено аналітичне дослідження та на основі нього, за допомогою математичного моделювання, побудовано ієрархічні моделі загроз для економічної безпеки вітчизняних підприємств. З метою збільшення ефективності функціонування комплексною системою економічної безпеки підприємства приділено увагу кадровій безпеці та сформовано відповідні концептуальні основи управління. Належне місце у монографії знайшли організаційно-методологічні особливості конкурентної розвідки та протидії рейдерству з врахуванням реального стану економічної безпеки в Україні.

Для студентів економічних спеціальностей, аспірантів, викладачів, науковців, усіх, хто цікавиться розвитком новітньої економічної думки.

УДК 33(075.8)
ББК 65я73

ISBN 978-966-397-132-6

© Живко З.Б., 2012
© Видавництво «Ліга-Прес», 2012

ЗМІСТ

ПЕРЕДМОВА	5
Розділ 1	
УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА	7
1.1. Гносеологічні основи безпеки та поняття «економічна безпека підприємства».....	7
1.2. Методологічні засади формування комплексної системи економічної безпеки підприємства.....	20
1.3. Концепція управління економічною безпекою підприємства.....	39
Література до першого розділу.....	47
Розділ 2	
ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА	57
2.1. Фінансово-економічні результати діяльності підприємства в оцінюванні економічної безпеки....	57
2.2. Визначення та ідентифікація ключових загроз економічної безпеки підприємства в Україні.....	75
2.3. Моделювання загроз економічній безпеці вітчизняних підприємств.....	98
Література до другого розділу.....	108
Розділ 3	
УДОСКОНАЛЕННЯ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА	112
3.1. Кадрова безпека в економічній безпеці підприємства.....	112
3.2. Загрози зі сторони персоналу та можливі шляхи їхньої нейтралізації.....	122
3.3. Концептуальні основи управління кадровою безпекою підприємства.....	138
Література до третього розділу.....	157

Розділ 4	
РОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ	
ТА КОНКУРЕНТНА РОЗВІДКА У ЗАБЕЗПЕЧЕННІ	161
ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА...	
4.1. Розвідувальна діяльність як засіб конкурентної боротьби у світовому економічному просторі.....	161
4.2. Сучасне трактування та напрямки розвитку конкурентної розвідки.....	175
4.3. Методичні аспекти здійснення конкурентної розвідки.....	181
4.4. Конкурентна розвідка та контррозвідка як складові системи економічної безпеки підприємства.....	200
Література до четвертого розділу.....	213
Розділ 5	
ПРОТИДІЯ РЕЙДЕРСТВУ ЯК ЗАГРОЗИ	
ЕКОНОМІЧНОЇ БЕЗПЕЦІ ПІДПРИЄМСТВА.....	216
5.1. Рейдерство: сутність та роль в ринковій економіці.....	216
5.2. Світовий досвід протидії рейдерству.....	221
5.3. Практика рейдерства в Україні та засади захисту вітчизняних підприємств.....	232
Література до п'ятого розділу.....	250
ПІСЛЯМОВА.....	254

ПЕРЕДМОВА

Питання національної безпеки постало для України з моменту проголошення незалежності понад двадцять років тому – у 1991 році. Інтеграція нашої держави до міжнародного співтовариства у процесі поширення глобалізації та мегарегіоналізації викликали не лише позитивні зміни, але й посилили небезпеки. Активізація міжнародного тероризму, жорсткої конкурентної боротьби на зовнішніх і внутрішніх ринках у сфері бізнесу і підприємництва, складна криміногенна ситуація у країні, недосконалість законодавчої, матеріально-технічної бази державної системи управління безпекою у інформаційній, економічній, соціальній, криміногенній, екологічній та інших сферах – загрози, що виникли протягом останніх десятиліть і викликають обґрунтоване занепокоєння громадян, організацій усіх видів діяльності і форм власності, органів державної влади різних рівнів ієрархії управління та українського суспільства загалом.

Система забезпечення безпеки держави, сформована на сьогоднішній момент, недостатньо швидко реагує на зміни як у внутрішньому, так і у зовнішньому середовищі, особливо це стосується забезпечення безпеки сфери підприємництва, де існує набагато більша кількість загроз, нещасних випадків, криміналу, надзвичайних ситуацій, катастроф і конфліктів, що спричиняють загибель людей, економічні (фінансові та матеріальні) втрати.

Саме на мікрорівні зароджується та розвивається тіньова економіка, обсяг якої, за оцінками експертів, подолав межу у 50%, що становить суттєву загрозу економічній безпеці усєї країни. Тому з однієї сторони державна політика, з метою протидії загрозам та реалізації економічних інтересів, повинна містити забезпечення безпеки підприємств як окремий самостійний напрям і постійно підтримувати високу ефективність програм і заходів у межах здійснення такої політики, а з іншої не може бути пасивною і позиція кожного окремого суб'єкта господарювання.

У порівнянні із ситуацією, яка була притаманна для планової економіки, коли фактичне управління кожним підприємством здійснювала держава, вона ж і гарантувала його безпеку, сьогодні стан справ є суттєво відмінним: суб'єкти господарювання отримавши свободу діяльності позбавлені прямої державної опіки, вони самі повинні протистояти зовнішнім і внутрішнім загрозам і нести

відповідальність за результати свої діяльності. Саме цей аспект вивів проблему забезпечення економічної безпеки на мікрорівні на перший план, адже захист та збереження бізнесу є не менш важливим ніж його заснування та розвиток.

Складною проблемою у сфері економічної безпеки є й те, що фактично теоретичні напрацювання її забезпечення на мікрорівні розпочалися порівняно недавно і попри актуальність та необхідність їх впровадження у практичну діяльність, вони перебувають лише на ранніх етапах формування. Не сприяє вирішенню проблеми й іноземний досвід, адже в наслідок специфіки умов національної економіки його не можливо прямо застосувати, потрібна науково обгрунтована адаптація, яка потребує співпраці науковців та підприємців.

Розробці питань щодо підтримки достатнього рівня економічної безпеки підприємства багато уваги приділяють вітчизняні та зарубіжні науковці, зокрема: Л. Абалкін, В. Абрамов, В. Андрійчук, О. Ареф'єва, О. Барановський, О. Білорус, З. Варналій, О. Власюк, В. Воротін, Т. Васильців, Я. Гончарук, В. Горбулін, В. Дикань, М. Єрмошенко, Я. Жаліло, О. Захаров, Н. Куркін, О. Ляшенко, В. Мунтян, Є. Олейніков, В. Ортинський Г. Пастернак-Таранушенко, В. Пономаренко, Н. Реверчук, В. Тамбовцев, М. Флейчук, В. Франчук, О. Черняк, М. Швець, В. Щелкунов, Л. Шемаєва, С. Шкарлет, В. Шликов, О. Шляйфер та ін.

Віддаючи належне науковій та практичній значущості праць названих учених, слід зазначити, що у вітчизняній літературі та на практиці господарювання підприємств досі недостатньо досліджені важливі питання забезпечення їх економічної безпеки, які б у повній мірі враховували специфіку та непрогнозованість змін національної економіки. Переважає вибірково-фрагментарний підхід до окресленої проблеми, який унеможливує її вирішення. Отже, актуалізується питання необхідності удосконалення теоретико-методологічної та методичної баз управління економічною безпекою підприємств, що й обумовило вибір теми дослідження.

Метою проведення дослідження стала необхідність розгляду ключових аспектів гарантування економічної безпеки на мікрорівні і зосередження уваги на малодосліджених, які зокрема стосуються кадрової безпеки, необхідності активного використання ділової розвідки й контррозвідки та розроблення програми протидії рейдерським атакам.

Розділ 1

УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

1.1. Гносеологічні основи безпеки та поняття «економічна безпека підприємства»

Незважаючи на зрозумілу на перший погляд змістовну характеристику поняття безпеки у вітчизняній та іноземній літературі, існує значна кількість його трактувань, що свідчить про складність і багатогранність його ідентифікації та підтверджує відсутність єдиного наукового підходу до визначення. В історичному ракурсі трактування безпеки розглядається як стан захищеності від постійної загрози посягання на устрій, уклад, свободу, життя та господарські надбання (за визначенням Р. Четвертакова [126]). Розвинуто цей підхід у словниках В. Даля та С. Ожегова [96], однак поняття «безпеки» отримало власне наповнення, а згодом – продовження в словниках і підручниках зі спеціалізованих дисциплін та нормативних актах. За семантичним і морфологічним трактуванням безпеки існують два концептуальні підходи: (1) статичний (безпека як стан) і (2) дієвий, або діяльнісний (безпека як діяльність), підвалини яких закладено Г. Іващенком [53].

Саме в роботі цього науковця «Про поняття «безпека» сформульовано таке визначення поняття безпеки, яке раціональним і несуперечливим чином пояснює всі випадки його вживання: і як безпека особи, і як безпека мореплавання, і як безпека виробничих процесів, і все інші, виділені в науці, види безпеки: політичну, військову, радіаційну, екологічну і так далі. З іншого боку, використання цього підходу дозволяє розробляти загальну доктрину і політику, а також методики щодо управління безпекою діяльності підприємств із застосуванням принципів і взаємозв'язків між

суб'єктами діяльності. У відповідності до основних позицій роботи Г. Іващенко, безпека, в загальному вигляді – це специфічна сукупність умов діяльності. Знаходиться в безпеці – означає перебувати в безпечних умовах, тобто в таких, які суб'єкт в змозі контролювати в процесі своєї діяльності, в процесі самореалізації.

В науковій літературі, здебільшого, феномен безпеки розглядається у двох аспектах: науковому та прикладному. У науковому плані його ключовими детермінантами є: 1) філософія стану; 2) парадигма діяльності; 3) сфера існування; 4) філософське прагнення та 5) цілісність і гармонія [49].

Слід погодитися з авторами [76], які стверджують, що у найбільш загальному розумінні, поняття «безпека» – це стан захищеності від будь-чого. Його можна застосувати як для загальних речей, так і конкретних ситуацій, пов'язаних з особистістю, підприємством, державою [77]. Зокрема, З. Варналія [18], систематизовано міждисциплінарний підхід до визначення поняття безпека (рис. 1.1):

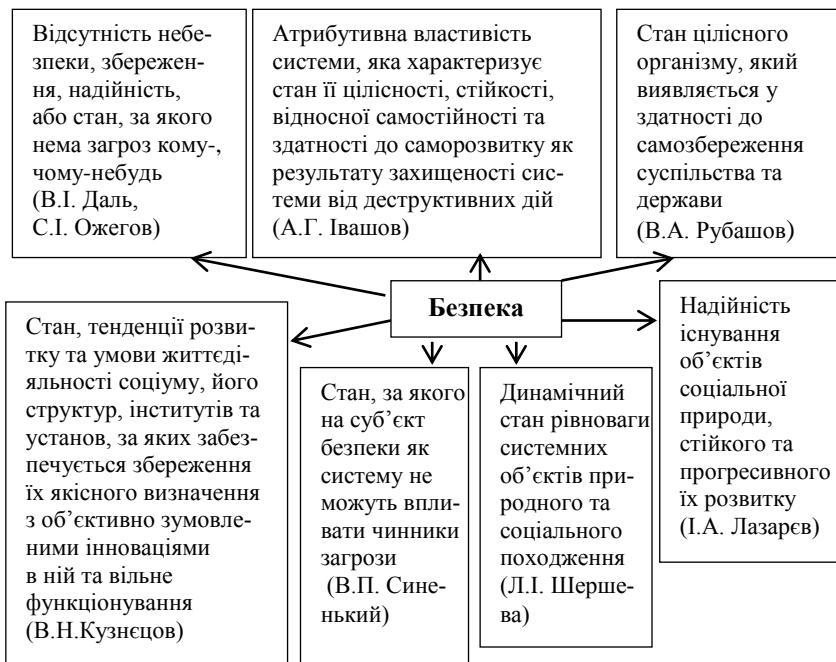


Рис. 1.1. Міждисциплінарні підходи до визначення поняття безпека (складено автором за [18])

Узагальнюючи напрацювання вітчизняних та закордонних науковців, можна стверджувати, що:

- безпека є умовою існування будь-якої соціально-економічної системи, в т.ч. підприємства;

- безпека – це здатність протидії впливу зовнішнього середовища;

- ключовими для існуючих визначень безпеки є терміни «захищеність», «відсутність небезпеки», «спокій», «незалежність», «стабільність», «допустимі межі», «безпечні та контрольовані умови», «збереження», «надійність», «захист від небезпеки (загроз)», «механізм запобігання загрозам», «зменшення впливу загроз», «зниження ризику»;

- опосередкованими категоріями є «прогресивний розвиток», «існування», «цілісність», «життєдіяльність соціуму та його структур», «розвиток», «впевненість», «рівновага», «самозбереження».

Суттєві відмінності у поглядах на природу поняття «безпека», а також окремих складових, які супроводжують його існування вимагає більш детального вивчення їх природи та взаємозв'язок в межах однієї системи таких складових як «небезпека», «загроза» та «ризик».

Розпочнемо з того, що в загальному поняття «небезпека» трактується як протилежність безпеці, тобто вони сприймаються як два полюси стану об'єкта дослідження.

Для формування власного розуміння небезпеки згадаємо, що філософське трактування понять «безпека» та «небезпека» формувалось ще у давнину, зокрема вони згадувались у працях Цицерона (106-43 рр. до н.е.) та інших мислителів. Щодо сучасного розуміння цих категорій доцільно зазначити, що в словнику В. Даля «безпека» – це стан, властивість, означає безпечний, незагрозливий той, що не може спричинити зла або шкоди, нешкідливий, збережений, вірний, надійний, «небезпека» – ненадійний, загрозливий, той, що завдає шкоду, біду, хворобу, нещастя. У словнику С. Ожегова [97] небезпеку подають як «можливість, загроза чого-небудь дуже поганого», а «безпеку» – як «стан, за якого не загрожує небезпека, є захист від небезпеки».

Проведене дослідження дозволило виявити, що серед науковців сформувалось схоже трактування небезпеки, але яке все-таки

у кожного з них має певні відмінності, тому процитуємо окремі. Так, Е. Олейніков дотримується думки, що небезпека – це цілком усвідомлена, але не фатальна ймовірність заподіяння шкоди, що визначається наявністю об'єктивних або суб'єктивних факторів, яким притаманні певні негативні властивості [101]. В. Ярочкін подає небезпеку як наміри, плани підготовка дій та самі дії, спрямовані на знищення, підпорядкування, послаблення і т. д. [133]. Український науковець М. Єрмошенко доводить необхідність трактування небезпеки як об'єктивно існуючої можливості негативного впливу на якесь явище, систему, механізм, соціальний організм, унаслідок чого йому може бути заподіяна шкода, що призведе до занепаду, кризового стану тощо [48].

Узагальнюючи вище подані трактування нами зроблено висновок, що окрім іншого їх об'єднує визначення небезпеки як ймовірності заподіяння шкоди, яка може мати фатальні наслідки для певної системи.

У свою чергу, В. Манілов та М. Дзілієв подають небезпеку як заподіяння шкоди важливим національним інтересам і національній безпеці в обмежених (локальних) масштабах [84; 35]. Небезпеку на національному рівні Н. Нижник, Г. Ситник та В. Білоус трактують як практичні дії однієї держави (або їх груп), юридичних осіб щодо завдання шкоди національним інтересам іншої країни, тобто процес безпосереднього практичного завдання шкоди національним інтересам держави [92]. Небезпеку стосовно регіону З. Герасимчук та Н. Вавдіюк визначають як стан, за якого відбувається деструктивний вплив дестабілізуючих чинників на економіку регіону, внаслідок чого нищиться його економічний потенціал, втрачається здатність до самовідтворення та захисту, що призводить до незадоволення потреб та інтересів населення, колапсу регіону [26].

Спільними для процитованих визначень можна вважати те, що в них небезпека подається як факт, реальність, послідовність певних дій, які мають негативний характер і можуть призвести до завдання шкоди.

Підсумовуючи, можна стверджувати, що попри схожість поглядів науковців на суть небезпеки, нами виділено два підходи: перший – ймовірнісний, коли розглядається можливість виникнення негативних наслідків; другий – реальний, коли йдеться

про конкретні дії, які завдають шкоди певній соціально-економічній системі.

Наступним кроком стане дослідження наукових підходів щодо трактування поняття «загроза». Поняття «загроза», як попередньо розглянуті, також не має єдиного визначення. Російський науковець В. Ярочкін загрозу подає як небезпеку на стадії переходу із можливості у дійсність, висловлений намір або демонстрація одних заподіяти шкоду іншими [133]. Схожої думки дотримуються і М. Абдурахманов та В. Баришполец трактуючи загрозу як безпосередню небезпеку завдання збитків, посягання на цінності та інтереси, що охороняються правом власності; висловлений у будь-якій формі намір завдати фізичний, матеріальний або інший збиток особі, суспільству, державі [78]. Як конкретна і безпосередня форма небезпеки або сукупність негативних чинників чи умов визначає загрозу М. Єрмошенко [48]. Е. Олейніков доводить необхідність визначення загрози як найбільш конкретну і безпосередню форму небезпеки або сукупність умов і факторів, що утворюють небезпеку інтересам громадян, суспільства і держави, а також національним цінностям і національному способу життя [101].

Узагальнюючи вище подані трактування, їх можна об'єднати в один підхід, згідно якого загрозу ототожнюють із небезпекою.

Деяко відмінної точки зору дотримуються В. Манілов та М. Дзілієв у трактуванні яких загроза унеможливує досягнення життєво важливих національних інтересів і знижує рівень національної безпеки, виходячи за локальні межі і стосуючись основних національних цінностей (суверенітету, державності, територіальної цілісності) [84; 35]. З. Герасимчук та Н. Вавдіюк визначають загрозу як існування негативних чинників, які здійснюють дестабілізуючий вплив на функціонування економіки регіону, порушуючи її стійкість до задоволення потреб населення [26]. Загроза в розумінні О. Ареф'євої та В. Кузенко – це сукупність умов, процесів, факторів, які перешкоджають реалізації національних економічних інтересів або створюють небезпеку для них та суб'єктів господарської діяльності [5]. Схоже трактування подає і В. Амітаном у розумінні якого загроза – це потенційно чи реально можлива подія, дія, процес чи явище, що здатне порушити його стійкість і розвиток чи призвести до зупинки його діяльності [2] та В. Шлемко й І. Бінько, у науковій праці яких досліджуване поняття подається як явні

або 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 [46]. Б. Губський виникнення загрози пов'язує з дією факторів, що безпосередньо чи у перспективі унеможливають або ускладнюють реалізацію національних економічних інтересів, створюючи перешкоди на шляху нормального розвитку економіки і безпеку незалежному державному існуванню та добробуту народу [33].

Узагальнюючи можна стверджувати, що другий підхід передбачає трактування загрози як сукупності умов, процесів та факторів, які негативно впливають на стан та динаміку розвитку соціально-економічної системи.

Підсумовуючи можна стверджувати, що, на нашу думку, поняття «загроза» потрібно трактувати не як безпосередню небезпеку, а як одну із її форм, виникнення і розвиток якої спричинено негативною дією зовнішнього середовища та неможливістю проконтролювати і здійснювати ефективне управління внутрішнім середовищем системи.

Як і визначення поняття «безпека», трактування «ризик» також відрізняється у науковій літературі. Наприклад, у «Словнику банкіра» не включено пояснення поняття ризику, хоча існує характеристика видів ризику, серед яких: валютний, кредитний, процентний та ін. [34].

Проведене ретельне дослідження дозволило розглянути трактування ризику та згрупувати їх з метою виділення ключових підходів.

В. Манілов та М. Дзілієв розглядають ризик як існування або можливість виникнення ситуації, за якої формуються передумови (накопичується потенціал) протидії реалізації національних цінностей, інтересів та цілей забезпечення національної безпеки [35; 84]. У трактуванні Е. Олейнікова ризик – це можливість виникнення несприятливих або небажаних наслідків діяльності самого суб'єкта [101]. Близьким до зазначеного визначення є твердження І. Лукасевич, згідно якого ризик – це можливість настання деякої несприятливої події, що тягне за собою виникнення різного роду втрат [81]. Схожої думки, але стосовно регіону, дотримуються З. Герасимчук та Н. Вавдіюк, які визначають ризик як ймовірність виникнення

несприятливої ситуації в економіці регіону [26]. Доволі близькими є визначення досліджуваного поняття у наукових працях Є. Стоянова [124] та Г. Кірейцева [123] у відповідності з яким ризик подається як можливість виникнення збитків, внаслідок дії зовнішнього середовища.

Узагальнюючи можна стверджувати, що відповідно до вище поданих трактувань ризик визначається як ймовірність настання негативних наслідків.

Дещо відмінна точка зору присутня в наукових працях наступних науковців. Так Я. Белінська визначає ризик як економічну категорію, сутність якої полягає у невизначеності реального очікуваного результату в ситуації управління та оцінювання і яка має діалектичну об'єктивно-суб'єктивну структуру [9]. Згідно міркувань В. Вітлінського та П. Верченко, ризик – це економічна категорія, що пов'язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору у процесі виробничо-господарської діяльності. Вона відображає міру (ступінь) відхилення від цілей, бажаного (очікуваного) результату, а також ступінь невдачі з урахуванням впливу керованих і некерованих чинників, прямих та зворотних зв'язків стосовно об'єкта керування [22]. Схожої думки дотримується і А. Доронін, адже він подає ризик як діяльність, спрямована на подолання невизначеності, яка виражається у стійких відносинах між суб'єктами виробництва з приводу оптимізації своїх інтересів до максимізації прибутку при об'єктивній неможливості врахувати і кількісно визначити весь комплекс одночасно діючих факторів, що породжують визначеність економічної системи [39]. Близьким за суттю є і визначення, яке дає А. Альгін [1], переконуючи, що ризик – це діяльність, що пов'язана з подоланням невизначеності в ситуації неминучого вибору, у процесі якої є можливість кількісно та якісно оцінити ймовірність досягнення бажаного результату, невдачі та відхилення від мети, яка міститься в альтернативах, що вибираються.

Узагальнюючи можна стверджувати, що у відповідності із другим підходом, ризик трактується як невизначеність та дії спрямовані на подолання цієї невизначеності.

Третій підхід, на нашу думку, представлений у напрацюваннях Л. Романенко й А. Коротеєва [112] та В. Глущенко [27]. Згідно міркувань Л. Романенко й А. Коротеєва ризик – це подія, що може

відбутися або ні. У разі настання такої події можливі три економічних результати: негативний (програв, збиток), нульовий і позитивний (виграш, вигода, прибуток). Водночас з точки зору В. Глущенко під цим поняттям потрібно розуміти невизначеність щодо настання тієї чи іншої події у майбутньому, причому ризик в економічному контексті може бути як негативним, так і позитивним явищем.

Узагальнюючи можна стверджувати, що відповідно до цього підходу ризик не передбачає чітко визначеного результату, він може бути або позитивним, або негативним.

На нашу думку, серед інших трактувань потрібно виділити в окремих підхід ще одне, а саме В. Ярочкіна, згідно якого ризик подається як можлива небезпека невдачі застосованих дій, або самі дії, що пов'язані з такою небезпекою [133], тобто ризик фактично отожднюється із небезпекою.

Окремо, на нашу думку, потрібно взяти до уваги і економічну сутність ризику. Так, дослідники, пропонуючи власні визначення категорії ризику, акцентують увагу, в основному, на негативних наслідках ризику: імовірності втрат, настанні несприятливих подій, небезпеці виникнення збитків, проте, виникнення ризику не завжди пов'язано з негативними наслідками, інакше підприємці не займалися б господарською діяльністю.

Оскільки однією з ключових ознак підприємницької діяльності є ризик, він апіорі супроводжує будь-яке підприємницьке рішення, і часом пов'язаний не з можливістю втрат, а лише з недоотриманням прибутку. Тому ризик варто розглядати як можливість настання ситуації при будь-якій діяльності, яка може відхилитись від поставленої мети (спричинити виникнення втрат чи недоотримання прибутку) або залишатися незмінною.

Метою підприємницької діяльності, що здійснюється на власний ризик і під особисту майнову відповідальність є одержання прибутку, а економічний результат такої діяльності може бути як позитивним, так і нейтральним чи негативним (рис.1.2).

Ризики у підприємницькій діяльності виникають як під впливом внутрішніх, так і зовнішніх чинників: соціальні ризики; ризики зміни політичної ситуації у світі та в країні; економічні ризики (макроекономічних потрясень; комерційні; валютні; кредитні; фінансові; інвестиційної діяльності; страхові); ризики зміни законо-

давства; інформаційні ризики; ризики зміни кон'юнктури ринку; екологічні ризики та ін., – що при переході у критичний стан реалізуються як загрози підприємницькій діяльності.

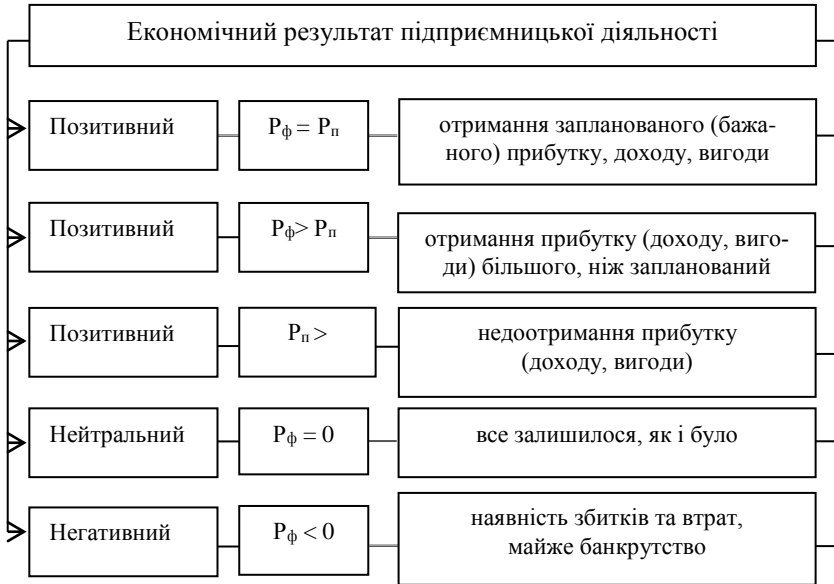


Рис. 1.2. Характеристики ризику підприємницької діяльності за ознакою економічного результату

Підсумовуючи можна стверджувати, що у нашому трактуванні ризик поруч із загрозою є формою небезпеки, реалізація якої може мати як позитивний, так і негативний наслідки; в першому випадку це спричинить зростання рівня безпеки, а в другому – приведе до виникнення загрози, а в подальшому і небезпеки.

Дослідження сутності понять «безпека», «небезпека», «загроза» й «ризик» та отримані в результаті, на нашу думку, доцільно прийняти як підґрунтя до ретельного розгляду категорії «економічна безпека підприємства» та подальшого удосконалення процесу гарантування економічної безпеки на мікрорівні.

Ретельно розглянувши різноманіття підходів до трактування категорії «економічна безпека підприємства» ми дійшли висновку, що їх як і раніше розглянуті доцільно згрупувати.

Розпочнемо з того, що значна кількість науковців подає доволі схоже визначення економічної безпеки підприємства, пов'язуючи його суть із найбільш ефективним використанням корпоративних ресурсів. Такої точки зору дотримуються: Е. Олейников [101], С. Ілляшенко [54], А. Крисін [76], І. Ципіна, Ю. Кваша [125], В. Сенгалова [137], А. Кириєнко [63], О. Арефєва, Т. Кузенко [5], В. Кириленко [64], О. Грунін [31], Л. Мельник [135]. Для чіткості розуміння сутності економічної безпеки підприємства, у відповідності до визначеного першого підходу, процитуємо кілька визначень. Так, Е. Олейников трактує економічну безпеку підприємства як стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз і забезпечення стабільного функціонування підприємства у теперішній час і в майбутньому [101]. В загальному, дотримуючись суті цього підходу О. Ареф'єва та Т. Кузенко акцентують увагу на тому, що під даним поняттям потрібно розуміти стан ефективного використання ресурсів і наявних ринкових можливостей, що дозволяє підприємству уникнути внутрішніх і зовнішніх загроз, забезпечує йому тривале виживання та стійкий розвиток на ринку відповідно до обраної місії [5]. Схоже визначення знаходимо і в науковій праці О. Груніна, де економічна безпека підприємства подається як такий стан суб'єкта господарювання, у якому він при найбільш ефективному використанні корпоративних ресурсів досягає запобігання, послаблення або захисту від існуючих небезпек та загроз або непередбачених обставин і в основному забезпечує досягнення цілей бізнесу в умовах конкуренції та господарчого ризику [31].

Суттєво відмінної точки зору дотримується група науковців, зокрема Є. Воробйов [23], Н. Капустін [61], Е. Раздіна [109], С. Дубецька [40], Н. Подлужна [98], які вважають, що для економічної безпеки підприємства пріоритетним є забезпечення його стійкості, захист інтересів та уможливлення розвитку. Знову ж таки процитуємо кілька визначень. Так, Є. Воробйов трактує економічну безпеку підприємства як сталість соціально-економічної системи, спроможність її до саморозвитку і взаємодії в умовах глобалізації господарського життя [23]. Схоже за суттю визначення дає і Н. Подлужна, при цьому наполягаючи, що економічна безпека підприємства – це характеристика системи, що самоорганізовується та саморозвивається, стан, за якого економічні параметри дозволя-

ють зберегти головні її властивості: рівновагу і стійкість при мінімізації загроз [98].

Поруч із охарактеризованими вище двома підходами, нами виділено третій, у відповідно до якого пріоритетним для економічної безпеки підприємства є його захист від зовнішніх та внутрішніх загроз. Такої точки зору дотримуються: Л. Бендіков [10], В. Ярочкін [134], В. Іванов, В. Шликов [52], А. Могильний [90], А. Козаченко, В. Пономарьов, А. Ляшенко [67], В. Забродский, Н. Капустін [50], Д. Ковалев, Т. Сухарукова [66], А. Колосов [139]. Характерним для цього підходу є визначення яке дає Л. Бендіков, у відповідності з яким економічна безпека підприємства – це захищеність його науково-технічного, технологічного, виробничого і кадрового потенціалу від прямих та непрямих економічних загроз, що пов'язані з неефективною науково-промисловою політикою держави або формуванням несприятливого зовнішнього середовища та здатність підприємства до відтворення [10]. У трактуванні А. Колосова економічна безпека підприємства – це стан захищеності життєво важливих економічних інтересів підприємства від внутрішніх і зовнішніх джерел небезпеки [139]. Доцільно звернути увагу і на думку Д. Ковалева й Т. Сухарукової, адже у їх розумінні економічна безпека підприємства – це захищеність його діяльності від негативних впливів зовнішнього середовища, а також здатність швидко усунути по-різному варіантні чи погрози, пристосуватися до існуючих умов, що не позначаються негативно на його діяльності [66].

Фактично універсальним, адже воно включає усі вище охарактеризовані підходи, можна вважати визначення Т. Васильціва, згідно з яким економічною безпекою підприємства вважаються такий стан функціонування, за якого підприємство і його продукція є конкурентоспроможними на ринку та одночасно гарантується: найбільш ефективне використання ресурсів, інтелектуального та кадрового потенціалу; стабільність функціонування, стійкість та прогресивність розвитку; можливість протидіяти негативним впливам зовнішнього і внутрішнього середовища його функціонування [19].

Підсумовуючи, можна стверджувати, що забезпечення економічної безпеки підприємства є передумовою його існування, комплексним видом діяльності, постійним процесом підтримання його функціональних складників на певному рівні з метою досяг-

нення максимального ефекту за своєчасного реагування на негативні впливи внутрішніх і зовнішніх чинників. Відповідно, узагальнюючи різноманітні підходи, зауважимо, що економічна безпека підприємства – це стан, за якого забезпечується економічний розвиток і стабільність діяльності підприємства, захист її життєво важливих інтересів, економічних (матеріальних, інформаційних, фінансових, трудових) ресурсів, та здатність своєчасно, адекватно і без суттєвих втрат реагувати на зміни внутрішньої і зовнішньої ситуації та негативний вплив дестабілізуючих факторів. Таке визначення перегукується з аналогічним трактуванням економічної безпеки на макрорівні, що має зміст, враховуючи, що рівень підприємства є підсистемою національного рівня безпеки і повинен бути її невід’ємним елементом.

Беручи до уваги зроблені вище узагальнення та висновки, можна стверджувати, що економічна безпека підприємства розглядається як протилежне поняття до терміну небезпека, а згідно з діалектичним підходом, ці крайні економічні стани підприємства реально існують і опосередковано взаємодіють через ризики та загрози. Ключовими ознаками стану економічної безпеки підприємства є: стійкість, стабільність та здатність до розвитку; відсутність збитків; висока платоспроможність; висока ділова активність; достатня рентабельність та конкурентоспроможність, якісна реалізація всіх планів та угод.

Потенційне виникнення несприятливої ситуації для підприємства створює ризик для його існування, що відображає можливість формування передумов для негативного впливу чинників на економіку підприємства. Ключовими характеристиками стану економічного ризику підприємства є можливість: зниження стійкості, стабільності та здатності до розвитку; збитків; зниження платоспроможності; зниження ділової активності; зниження рентабельності, конкурентоспроможності.

Перетворення ймовірності в реальність створює економічну загрозу, тобто стан існування негативних чинників, які здійснюють дестабілізуючий вплив на функціонування економіки підприємства, визначальними рисами якої є: порушення стійкості, стабільності та здатності до розвитку; наявність збитків; зниження поточної та загальної платоспроможності; зниження ділової активності; зниження рентабельності, конкурентоспроможності (табл. 1.1).

Визначальні характеристики станів економічної безпеки

Стан	Безпека	Ризик	Загроза	Небезпека
Ключові ознаки	стійкість, стабільність та здатність до розвитку	можливість зниження стійкості, стабільності та здатності до розвитку	порушення стійкості, стабільності та здатності до розвитку	втрата стійкості, стабільності та здатності до розвитку
	відсутність збитків	можливість збитків	наявність збитків	наявність збитків в катастрофічних розмірах
	висока платоспроможність	можливість зниження платоспроможності	зниження поточної та загальної платоспроможності	втрата платоспроможності
	висока ділова активність	можливість зниження ділової активності	зниження ділової активності	втрата можливості отримати кредит
	достатня рентабельність та конкурентоспроможність, якісна реалізація планів та угод	можливість зниження рентабельності, конкурентоспроможності	зниження рентабельності, конкурентоспроможності	втрата конкурентоспроможності

У стані економічної небезпеки відбувається вплив дестабілізуючих чинників на економіку підприємства, що спричиняє втрату матеріально-технічної бази, здатності до простого відтворення та захисту від банкрутства, тобто настають деструктивні граничні зміни в соціально-економічній системі, викликані реальними втратами, пов'язаними з реалізацією загрози.

З метою забезпечення економічної безпеки підприємствам потрібно протидіяти загрозам, щоб уможливити виникнення економічної небезпеки, подолати яку значно важче. Таким чином, економічна безпека підприємства – це його стан в межах граничних значень і здатність протидіяти загрозам та забезпечувати реалізацію економічних інтересів.

1.2. Методологічні засади формування комплексної системи економічної безпеки підприємства

Проблема забезпечення економічної безпеки підприємства належить до розряду пріоритетних, що обумовлюється такими причинами: нестабільністю економічної ситуації в країні; посиленням зовнішнього конкурентного впливу; зниженням купівельної спроможності населення; зростанням злочинності; збільшенням випадків рейдерських атак на підприємства; необхідністю реструктуризації бізнесу на базі найновітніших інформаційних технологій, що сприяють появі інформаційно-обчислювального та телекомунікаційного обладнання, яке вимагає особливого захисту; необхідністю підвищення конкурентоспроможності підприємства тощо. Останнім часом витрати підприємств на створення систем безпеки невпинно зростають, що також підтверджує неможливість стабільної діяльності підприємства без забезпечення надійного рівня його безпеки. Як свідчить практика, співвідношення витрат, здійснених до моменту настання негативної події та завдання шкоди підприємству, і витрат на ліквідацію наслідків загрози та відновлення майна і ресурсів дорівнює 1/15 [21].

Забезпечення необхідного для безперервного функціонування та розвитку рівня безпеки є неможливим без ґрунтовних наукових досліджень, результатом здійснення яких повинно стати розроблення відповідних методологічних засад на базі активного застосування системного підходу. Зазначене обумовлено тією обставиною, що впевнений розвиток системного підходу у науковому пізнанні та його експансія у все більшу кількість сфер знань зумовили оформлення системного підходу у якості наукової теорії, яка отримала назву загальної теорії систем. Автором терміну «загальна теорія систем» є австрійський біолог-теоретик Людвіг фон Берталанфі. Він достатньо вдало сформулював загальні принципи теорії систем та є розробником емпірично-інтуїтивного підходу до проведення системних досліджень [13].

У відповідності до наукових праць [13; 87; 103; 141] можна виділити декілька суттєвих переваг системного підходу, які зумовлюють його наукове та практичне розповсюдження та необхідність застосування в сфері економічної безпеки:

– по-перше, дозволяє встановити оптимальний ступінь аналітичного розчленування об'єкта та визначити таку адекватну «аналітичну одиницю», що надалі не розкладається. Це дає можливість встановити найбільш цінні структурні та динамічні властивості об'єкта, що зумовлюють його цілісне функціонування;

– по-друге, породжує принципово новий спосіб проведення досліджень, який дає можливість максимально повно встановити типологію, структуру та логіку взаємозв'язків елементів об'єкта, що зумовлюють цілісність його функціонування;

– по-третє, виводить наукове пізнання на принципово новий якісний рівень та забезпечує незрівнянно вищу пізнавальну цінність своїх висновків.

Потреба використання системного підходу для дослідження та формування методологічних засад управління економічною безпекою підприємства пояснюється тим, що своєю кінцевою метою він має угруповання всіх суттєво важливих чинників, які, в свою чергу, створюють позитивні умови для безпечного функціонування та розвитку підприємства. Саме системний підхід дозволяє не тільки по-новому підійти до вирішення багатьох актуальних проблем, але й аналізувати конкретні позиції, дії, ситуації і цілі в комплексі логічних чинників. Суть системного підходу, при вирішенні проблем безпечного існування підприємств, полягає в тому, що діяльність колективу, функціонування підприємства, та вплив зовнішніх і внутрішніх факторів – розглядаються як динамічна система в сукупності її найважливіших зв'язків, яка сприяє знаходженню шляхів оптимізації цієї системи. О. Головченко розглядає системний підхід, як напрям методології наукового пізнання і соціальної практики, в основі якого лежить розгляд об'єктів як систем. Він орієнтує дослідників на розкриття цілісності об'єкта, виявлення різноманітних типів зв'язків у ньому і зведення їх в єдину теоретичну картину [28].

В сучасних умовах господарювання, підприємства, як правило, самостійно визначають свою економічну спрямованість, організовують виробничий і збутовий процеси, і несуть повну відповідальність за результати своєї діяльності. Це обумовлює життя комплексних заходів, спрямованих на захист господарчої діяльності підприємства, які відображаються у необхідності створення системи економічної безпеки.

Системний підхід є одним з основних напрямків методології спеціального наукового пізнання і сприяє формуванню суті досліджуваних процесів або проблем. Тому його мета і завдання полягають, перш за все, у дослідженні певних об'єктів як складних систем.

Для того, щоб більш глибоко зрозуміти сутність поняття «система», необхідно виділити її основні властивості:

- багатокomпонентність системи. Перш за все система являє собою сукупність елементів з яких вона складається. В деяких випадках елементи можуть розглядатися як самостійні системи;

- наявність істотних зв'язків між елементами, а також залежність властивостей цих елементів від їх розташування у системі, функцій та інших параметрів, які знаходяться у середині цілого;

- залежність поведінки системи в цілому від поведінки її окремих елементів, їх властивостей та структури. Треба зазначити, що властивості системи не завжди визначаються повністю своїми елементами, тому система не зводиться до простої сукупності елементів, і розчленувавши її на окремі частини, не можна пізнати всі системні властивості в цілому;

- залежність системи не тільки від внутрішнього, як було зазначено у попередньому пункті, але й від зовнішнього середовища. В даному випадку сама система є активною стороною взаємодії, оскільки саме вона, разом зі всіма своїми елементами реагує на зовнішні впливи. В контексті цього доцільно згадати, що в найбільшій мірі на рівень економічної безпеки вітчизняних підприємств негативно впливає саме зовнішнє середовище;

- ієрархія системи, в якій кожна ланка являє собою більш обмежену структурну систему Системи економічної безпеки, на різних рівнях свого існування можуть класифікуватися на суперсистеми, великі системи, підсистеми і їх елементи. Великі системи ефективно використовувати у системах економічної безпеки, при цьому кількість елементів, та зв'язків між ними, може бути зовсім невеликим, оскільки основна відмінність між системою і великою системою має не кількісний, а якісний характер.

Узагальнюючи можна стверджувати, що саме завдяки застосуванню системного підходу можна проектувати та реалізувати ефективну систему економічної безпеки підприємства. Водночас в науковій літературі сьогодні відсутнє єдине визначення поняття

«система безпеки підприємства». Так, на думку В. Мак-Мака, система безпеки підприємства включає наукову теорію безпеки, політику і стратегію безпеки засобу і методи забезпечення безпеки і концепцію безпеки підприємства [83]. У свою чергу В. Ірочкін визначає систему безпеки як організовану сукупність спеціальних органів, служб, засобів, методів заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства, держави від внутрішніх і зовнішніх загроз [38]. Схоже визначення, але стосовно мікрорівня сформовано у роботі Л. Шарого, де економічна безпека підприємства визначена як взаємопов'язана сукупність спеціальних структур, засобів, методів і заходів, які забезпечують безпеку бізнесу від внутрішніх і зовнішніх загроз. У цьому контексті систему охарактеризовано комплексом управлінських, страхових, правових, економічних, охоронних, режимних, судово-правових та інших заходів із захисту бізнесу від незаконних посягань, мінімізації або уникнення матеріальних та інших втрат [8]. М. Зацеркляний та О. Мельников трактують це поняття як сукупність взаємозалежних заходів організаційно-правового характеру, здійснюваних із метою захисту підприємницької діяльності від реальних або потенційних дій фізичних чи юридичних осіб, які можуть призвести до істотних економічних втрат.

В науковій праці О. Долженкова, Ж. Жуковської та О. Головченко присутнє таке визначення «...комплексна система гарантування економічної безпеки як складова комплексної системи безпеки підприємництва – це сукупність взаємозалежних заходів організаційно-правового характеру, здійснюваних з метою захисту підприємницької діяльності від реальних чи потенційних дій фізичних чи юридичних осіб, що можуть призвести до істотних економічних втрат» [102].

У своїх працях М. Камлик дає наступне визначення комплексній системі економічної безпеки підприємства – це комплекс взаємопов'язаних заходів організаційно-правового характеру, що здійснюються спеціальними органами, службами, підрозділами суб'єкта господарювання, спрямованих на захист життєво важливих інтересів особистості, підприємства і держави від протиправних дій з боку реальних або потенційних фізичних чи юридичних осіб, що можуть призвести до істотних економічних втрат та забезпечення сталого росту підприємства у майбутньому [59].

Більшість науковців погоджуються з тією позицією, що в основі розробки комплексної системи забезпечення економічної безпеки підприємництва повинна знаходитися певна концепція, яка включає мету, завдання, об'єкти, суб'єкти та інші складові. Єдиної думки щодо структури КСЕБП не існує, але можна виділити кілька ключових точок зору. Так, В. Франчук у своєму науковому виданні «Основи економічної безпеки» так графічно зображає структуру системи на мікрорівні (рис. 1.3).

Іншої точки зору дотримуються Л. Донець та Н. Ващенко, які вважають, що одним із основних елементів системи безпеки підприємства, окрім тих, що виділяє В. Франчук, має бути і «політика безпеки», яка включає в себе визначення мети, функцій, принципів та розроблення стратегії (рис. 1.4) [38].

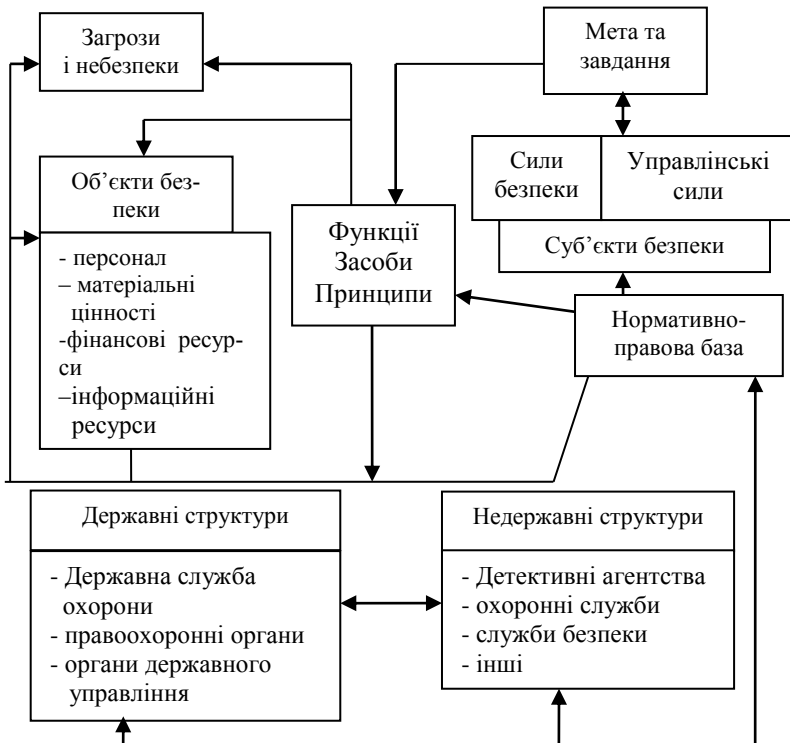


Рис. 1.3. Система безпеки підприємства

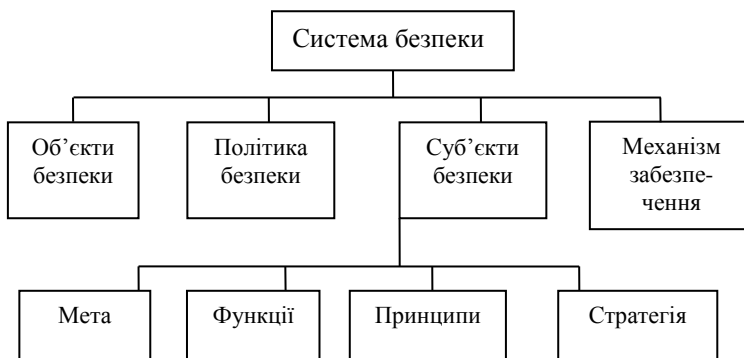


Рис. 1.4. Система економічної безпеки підприємства

У книзі В. Ортинського, І. Керницького, З. Живко та ін. [45] представлена трьохвимірна модель системи безпеки фірми (підприємства, організації) (рис. 1.5).

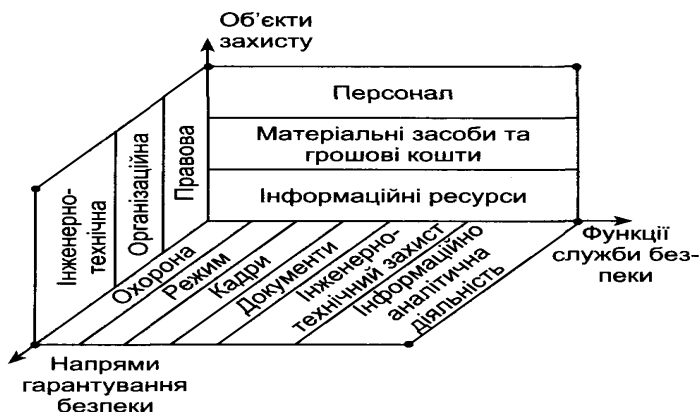


Рис. 1.5. Типова тривимірна модель комплексної системи економічної безпеки фірми (підприємства, організації)

Зважаючи на вже існуючі напрацювання стосовно забезпечення економічної безпеки підприємства, вважаємо за доцільне в подальшому використовувати термін «комплексна система економічної безпеки підприємства» (КСЕБП) та поставити собі за мету

удосконалити засади формування та управління нею. Окрім цього, погоджуємося, що під КСЕБП потрібно розуміти сукупність взаємопов'язаних заходів організаційно-економічного і правового характеру, що здійснюються з метою захисту діяльності підприємства від реальних чи потенційних дій фізичних або юридичних осіб, які можуть призвести до економічних втрат.

Мету КСЕБП, із врахуванням результатів дослідження гносеологічних основ безпеки та сутності поняття «економічна безпека підприємства», які викладені у попередньому підрозділі, можна сформулювати наступним чином: мінімізація зовнішніх і внутрішніх загроз для підприємства, у тому числі завдяки ефективному використанню його фінансових, матеріальних, інформаційних та кадрових ресурсів на основі розроблення і реалізації комплексу заходів економіко-правового та організаційного характеру. У процесі досягнення поставленої мети здійснюється вирішення конкретних завдань, які об'єднують всі напрямки забезпечення безпеки. До завдань, що вирішуються системою забезпечення економічної безпеки, зазвичай належать:

- прогнозування можливих загроз для економічної безпеки;
- організація діяльності з попередження можливих загроз (превентивні заходи);
- виявлення, аналіз і оцінка виникнення реальних загроз для економічної безпеки підприємства;
- прийняття рішень і організація діяльності нейтралізації та ліквідації наслідків реалізації загрози;
- постійне вдосконалення системи забезпечення економічної безпеки підприємства.

Організація і функціонування КСЕБП з метою максимальної ефективності повинна ґрунтуватися на певних принципах. Про це писали багато авторів, у тому числі й В. Мак-Мак, який виділяє наступні принципи системи безпеки підприємства: пріоритет заходів попередження; законність; комплексне використання сил і коштів; координація і взаємодія всередині і поза підприємством; поєднання гласності з конспірацією; компетентність; економічна доцільність; планова основа діяльності; системність [83].

На нашу думку, цей перелік принципів потрібно дещо розширити та більш чітко окреслити суть кожного з них.

Принцип безперервності. Для ефективного захисту діяльності підприємства, в умовах підвищеного ризику та конкуренції

необхідне безперервне функціонування та виконання своїх завдань системою економічної безпеки;

Принцип законності. Порушення закону призводить до негативних наслідків таких, як застосування штрафних санкцій з боку правоохоронних органів, послаблення системи економічної безпеки, шантажу з боку кримінальних структур і т.д. Внаслідок такої ситуації даний принцип передбачає, що діяльність підприємства повинна плануватись відповідно до вимог чинного законодавства;

Принцип економічної доцільності. Полягає у тому, що витрати на проведення заходів безпеки не повинні бути вищими за доходи підприємства;

Принцип комплексності, тобто поєднання превентивних та реактивних заходів. Превентивні – заходи попереджувального характеру, які зменшують імовірність виникнення чи реалізації загроз для економічної безпеки підприємства. Реактивні – заходи, які здійснюються у випадку реального виникнення загрози або з метою мінімізації її негативного впливу.

Принцип диференціювання. Вибір заходів щодо протидії реалізації загрози відбувається в залежності від її характеру і ступеня важкості наслідків.

Принцип координації. Для виконання поставлених завдань необхідне постійне погодження діяльності різних підрозділів служби безпеки, інших структурних підрозділів підприємства, зовнішніх суб'єктів безпеки.

Принцип контролю. Для оцінки і можливого удосконалення системи економічної безпеки, на підприємстві повинен здійснюватися контроль з боку керівництва за діяльністю співробітників служби економічної безпеки;

Чітке дотримання цих принципів забезпечує логічну послідовність дій всіх співробітників та організованість у реалізації заходів безпеки, що в кінцевому результаті сприятиме підвищенню ефективності роботи системи економічної безпеки підприємства.

КСЕБП – це комплексне поняття, до складу якого входять суб'єкти, об'єкти та механізм реалізації безпеки на підприємстві. Окрім цього, потрібно підкреслити, що система економічної безпеки кожного підприємства є індивідуальною, її повнота і дієвість залежать від чинної в державі законодавчої бази; від обсягу матеріально-технічних і фінансових ресурсів, виділених керівниками

підприємств; від розуміння кожним з працівників важливості гарантування безпеки бізнесу; а також від досвіду роботи керівників служб безпеки підприємств.

Об'єкт і суб'єкт системи забезпечення економічної безпеки підприємства, як показала практика, тісно взаємопов'язані. Об'єктом системи в цілому зазвичай виступає стабільний економічний стан підприємства в поточному і перспективному періоді. Конкретними ж об'єктами захисту частіше виступають ресурси: фінансові, матеріальні, інформаційні, кадрові і т.п. Суб'єкт системи забезпечення економічної безпеки підприємства, як правило, має більш складний характер, оскільки його діяльність обумовлюється не тільки особливостями і характеристиками об'єкта, але і специфічними умовами зовнішнього середовища, що оточує підприємство. Зважаючи на подане, можна виділити дві групи суб'єктів, що забезпечують економічну безпеку підприємства: зовнішні і внутрішні. До зовнішніх суб'єктів належать органи законодавчої, виконавчої та судової влади, покликані забезпечувати безпеку всіх без винятку законотворчих учасників господарських відносин. Причому діяльність цих органів не може контролюватися самими підприємствами. Ці органи формують законодавчу основу функціонування та захисту господарської діяльності в різних її аспектах і забезпечують її виконання. До внутрішніх суб'єктів належать особи, які безпосередньо проводять захист економічної безпеки даного конкретного суб'єкта господарської діяльності. В якості таких суб'єктів можуть виступати: працівники власної служби безпеки підприємства; запрошені працівники зі спеціалізованих фірм, що надають послуги з захисту діяльності підприємства.

Внутрішні суб'єкти, що забезпечують економічну безпеку підприємства, проводять власну діяльність на основі певної стратегії і тактики. Відомо, що стратегія – це довгостроковий підхід до досягнення мети. Генеральна стратегія економічної безпеки виражається через загальну концепцію комплексної системи забезпечення економічної безпеки підприємства. Крім генеральної стратегії виділяються також спеціальні стратегії (наприклад, в залежності від стадії господарської діяльності). Нарешті, можуть застосовуватися функціональні стратегії безпеки. Це може бути стратегія економічної безпеки підприємства, що включає в себе систему превентивних заходів, що реалізується через регулярну, безперервну ро-

боту всіх його підрозділів щодо перевірки контрагентів, аналізу передбачуваних угод, експертизи документів, виконання правил роботи з конфіденційною інформацією і т.п. Служба безпеки в даному випадку виконує роль контролера. І це може бути стратегія реактивних заходів, застосовується у разі виникнення або реально-го здійснення будь-яких загроз економічної безпеки підприємства. Така стратегія, заснована на застосуванні ситуаційного підходу та обліку всіх зовнішніх і внутрішніх факторів, реалізується службою безпеки через систему заходів, специфічних для даної ситуації.

Тактика забезпечення безпеки підприємства припускає застосування конкретних процедур і виконання конкретних дій з метою забезпечення його економічної безпеки. Мова йде про такі процедури та діях як: розширення юридичної служби підприємства; прийняття додаткових заходів щодо збереження комерційної таємниці; створення підрозділу комп'ютерної безпеки; пред'явлення претензій контрагенту-порушнику; звернення з позовом до судових органи; звернення до правоохоронних органів і т.п. Таким чином, комплексна система економічної безпеки підприємства має включати в себе строгий перелік взаємозалежних елементів, що забезпечують безпеку підприємства при досягненні нею основних цілей бізнесу.

Формування системи економічної безпеки та створення її суб'єктів залежать від розмірів підприємства та його можливостей. Як правило, підприємства малого бізнесу користуються послугами зовнішніх спеціалізованих приватних підприємств (консалтингових, охоронних, детективних тощо). Підприємства середнього бізнесу можуть користуватися комбінованою системою економічної безпеки, спираючись на можливості і ресурси власних підрозділів безпеки та, в міру необхідності, залучаючи потенціал зовнішніх організацій. Великим підприємствам доцільно створювати повноцінну систему економічної безпеки з власною службою та потужними ресурсами.

Варто зауважити, що саме поняття системи економічної безпеки підприємства передбачає ефективне використання його ресурсів, що забезпечувало б стабільне функціонування підприємства на теперішньому етапі та стійкий розвиток у майбутньому. Для забезпечення економічної безпеки підприємство використовує всю сукупність своїх корпоративних ресурсів – таких чинників бізнесу,

які використовуються власниками та менеджерами підприємства для досягнення його цілей [29].

Серед них виділяють:

- ресурс капіталу, який дозволяє купувати і підтримувати інші корпоративні ресурси;
- ресурс персоналу, який можна представити сукупністю працівників, їхніми знаннями і досвідом, що є основною з'єднувальною всіх чинників бізнесу, забезпечуючи досягнення його цілей;
- ресурс інформації і технологій – найбільш цінний і найдорожчий ресурс підприємства, що дозволяє йому адекватно реагувати на будь-які зміни зовнішнього оточення бізнесу, ефективно планувати та здійснювати власну господарську діяльність;
- ресурс техніки та обладнання може бути придбаний за наявності вищенаведених ресурсів;
- ресурс прав дозволяє підприємству долучитися до передових новітніх технологій, не проводячи власних наукових досліджень.

Отже, для забезпечення власної безпеки підприємство має такі засоби:

- технічні (охоронно-пожежні системи, відеоапаратура тощо);
- організаційні (створення спеціалізованих підрозділів чи структур, які забезпечуватимуть безпеку підприємства, а також система управління);
- інформаційні (комп'ютери, захисні мережі і сама інформаційна продукція, у т.ч. необхідна для прийняття рішень інформація);
- фінансові, без яких і функціонування системи безпеки буде неможливим;
- правові (у т.ч. розробка локальних правових актів з питань функціонування системи управління та забезпечення безпеки);
- кадрові (передусім, достатня кількість персоналу, який займається питаннями безпеки, його професіоналізм);
- інтелектуальні (залучення висококласних спеціалістів і науковців дозволяє запроваджувати нові системи безпеки).

Варто зазначити, що ці засоби потребують комплексного поетапного застосування, а не одночасного запровадження.

Відповідно до базових засад системного підходу, досягнення необхідного рівня економічної безпеки підприємства повинно забезпечуватися стабільністю та ефективним функціонуванням окремих функціональних складових економічної безпеки підприємства. Коротко охарактеризуємо суть та завдання кожної з них.

Серед функціональних складових економічної безпеки фінансова складова вважається провідною й вирішальною [47], оскільки за ринкових умов господарювання фінанси є «двигуном» будь-якої економічної системи. Фінансова безпека підприємства – це захищеність його діяльності від негативних впливів зовнішнього середовища, а також спроможність швидко усунути різноманітні загрози або пристосуватися до існуючих умов, що не позначаються негативно на його діяльності [7].

Н. Реверчук вважає, що фінансова безпека підприємства – це захист від можливих фінансових втрат і попередження банкрутства підприємства, шлях до досягнення найбільш ефективного використання корпоративних ресурсів. Саме вона, на її думку, є провідною і вирішальною, оскільки за ринкових умов господарювання фінанси є рушієм будь-якої економічної системи [110].

Призначення цієї складової полягає в забезпеченні фінансової стійкості підприємства, його платоспроможності та кредитоспроможності, прийнятному рівні прибутковості та рентабельності, достатньому рівні ліквідності активів, обґрунтуванні й величині дебіторської та кредиторської заборгованості, недопущенні банкрутства.

Друга складова – техніко-технологічна, характеризується необхідністю низьким рівнем фізичного та морального зносу основних засобів та їх окремих складових, високими темпами впровадження прогресивних технологій, своєчасним оновленням основних засобів та ефективним їх використанням.

Третя складова – кадрова безпека, що є синтетичною категорією: економічної теорії, теорії управління персоналом, економіки праці, соціології, політології [86].

Кадрова безпека є уніфікованою категорією, яка виявляється на всіх рівнях від окремо взятого підприємства до національної економіки. Вона спрямована на забезпеченість підприємства працівниками високого інтелектуально-кваліфікаційного рівня, організації ефективної системи управління персоналом їх мотивації

та оплати праці, а також раціональному використанні трудового потенціалу.

Четверта – силова, передбачає захист майна підприємства та його працівників.

П'ята – екологічна, враховує відповідність екологічних результатів діяльності підприємства чинним нормативним параметрам, раціональність використання відходів, втрату прибутків через порушення екологічного законодавства та сплати штрафних санкцій.

Шоста – політико-правова, визначає захищеність підприємства від рейдерських атак, дотримання платіжної дисципліни та трудового законодавства.

Сьома – інформаційна. Як визначає В. Ортинський, І. Керницький, З. Живко та ін. [45], інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Відповідні служби виконують при цьому певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової економічної безпеки.

Восьма – ресурсна, полягає в забезпеченні виробництва основними видами ресурсів, необхідним рівнем якості, забезпечення запасів власними оборотними коштами, здатністю підприємства поповнювати, замінювати, зберігати й використовувати матеріальні ресурси так, щоб результат від перерахованих дій підвищував загальну безпеку.

Подана нами характеристика складових уможливило подальше формування методологічних засад управління економічною безпекою підприємства. Так, до основних функціональних цілей економічної безпеки підприємства можна віднести:

- забезпечення високої фінансової ефективності роботи, фінансової стійкості та незалежності підприємства;
- забезпечення технологічної незалежності і досягнення високої конкурентоспроможності й технічного потенціалу того чи іншого суб'єкта господарювання;
- досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством;
- мінімізація руйнівної дії результатів виробничо-господарської діяльності на стан навколишнього середовища;

- якісна правова захищеність усіх аспектів діяльності підприємства;
- забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів і відділів організації;
- ефективна організація безпеки персоналу підприємства, його капіталу і майна, а також комерційних інтересів
- забезпечення оптимізації та ефективного використання усіх видів ресурсів.

Фахівці зазначають [61], що широкий спектр цілей формування економічної безпеки підприємства у контексті забезпечення гарантій його стабільного та максимально-ефективного функціонування на сучасному етапі господарської діяльності і високого потенціалу розвитку в майбутньому вимагає системного їх розподілу у напрямках технологічної, ресурсної, фінансової, маркетингової і соціальної безпеки, що являють собою комплекс завдань і показників, підвищити які можливо лише успішно працюючи в усіх напрямках одночасно.

З урахуванням викладеного вище можна визначити такі загальні орієнтири дій і ухвалення рішень, які полегшують досягнення цих цілей:

- а) збереження і нарощування ресурсного потенціалу;
- б) проведення комплексу превентивних заходів щодо підвищення рівня захищеності власності й персоналу підприємства;
- в) залучення до діяльності із забезпечення безпеки підприємства всіх його працівників;
- г) професіоналізм і спеціалізація персоналу підприємства;
- д) пріоритетність несилових методів запобігання загрозам і їх нейтралізації;
- е) створення служби економічної безпеки на підприємстві.

Для досягнення цілей, на нашу думку, в умовах певного підприємства доцільно кожному з них конкретизувати сукупністю завдань:

- 1) захист законних прав та інтересів підприємства та його співробітників;
- 2) збір, аналіз, оцінка даних і прогнозування розвитку обстановки;
- 3) вивчення партнерів, клієнтів, конкурентів, кандидатів на роботу в компанії;

- 4) своєчасне виявлення можливих посягань до підприємства та його співробітників з боку джерел зовнішніх загроз безпеки;
- 5) недопущення проникнення на підприємство структур економічної розвідки конкурентів, організованої злочинності та окремих осіб із протиправними намірами;
- 6) протидія технічному проникненню в злочинних цілях;
- 7) виявлення, попередження і припинення можливої протиправної та іншої негативної діяльності співробітників підприємства на шкоду його безпеки;
- 8) захист співробітників підприємства від насильницьких посягань [55];
- 9) забезпечення збереження матеріальних цінностей і відомостей, що становлять комерційну таємницю підприємства;
- 10) добування необхідної інформації для вироблення найбільш оптимальних управлінських рішень з питань стратегії і тактики економічної діяльності компанії;
- 11) фізична і технічна охорона будівель, споруд, території і транспортних засобів;
- 12) формування серед населення та ділових партнерів сприятливої думки про підприємство, що сприяє реалізації планів економічної діяльності та статутних цілей;
- 13) відшкодування матеріальної та моральної шкоди, завданої в результаті неправомірних дій організацій і окремих осіб;
- 14) контроль за ефективністю функціонування системи безпеки, вдосконалення її елементів [55].

Грунтуючись на вище викладеному матеріалі щодо сутності, цілей та завдання системи безпеки, нами побудовано механізм управління КСЕБП (рис. 1.6).

Для оцінки поточного рівня економічної безпеки підприємства можна використати інтегральний показник економічної безпеки, який розраховується за формулою:

$$PB = \prod_{i=1}^M q_i \times \prod_{j=1}^N \frac{I_{jt=1}}{I_{jt}} > 1, \quad (1.1)$$

де q_i – показник контролю включення в модель параметрів економічної безпеки підприємства (даний показник приймається рівним 1 при наявності показника, 0 – при його відсутності);

M – кількість нормативних показників;

I_{it+1}, I_{it} – індекси показників економічної безпеки, які розглядаються в динаміці, відповідно періоду часу t і $t+1$. Інтервал часу t і $t+1$ характеризує крок перерахунку рівня економічної безпеки підприємства [42].

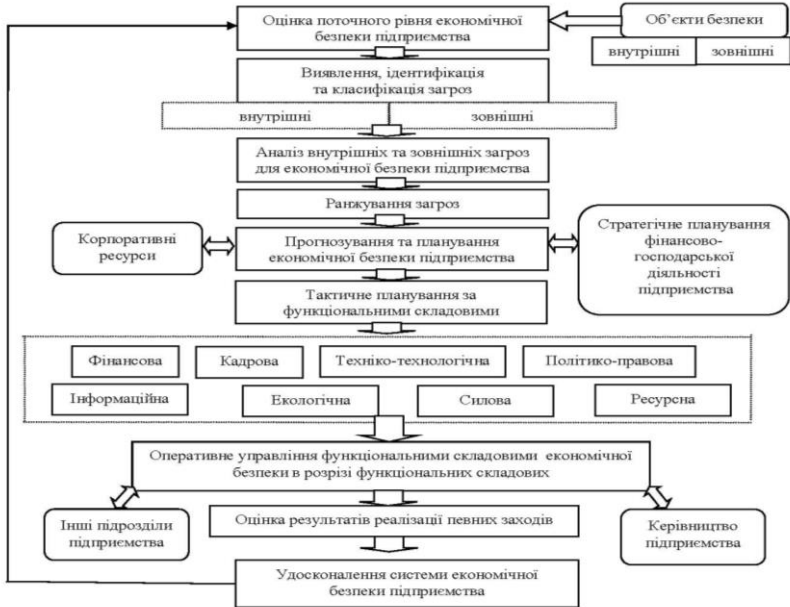


Рис. 1.6. Механізм управління КСЕБП

Були розроблені [42] ще два методи визначення рівня економічної безпеки підприємства. Відповідно до першого методу рівень економічної безпеки може бути встановлений за формулою:

$$Y_{\text{ебн}} = F(X_i) = a_1 \times f(x_1) + a_2 \times f(x_2) + \dots + a_i \times f(x_n), \quad (1.2)$$

де $Y_{\text{ебн}}, F(X_i)$ – рівень економічної безпеки підприємства;

a_1, a_2, \dots, a_n – питома вага значущості кожного показника для забезпечення економічної безпеки підприємства;

i – кількість показників;

$f(x_1), f(x_2), \dots, f(x_n)$ – локальні функції залежності рівня економічної безпеки відповідних показників діяльності підприємства.

Існує другий метод, що пропонує оцінювати рівень економічної безпеки підприємства на основі сукупного критерію за формулою:

$$k^{e6n} = \sum_{i=1}^T h^i \times d^s, \quad (1.3)$$

де h^i – величина окремого критерію за i -ою функціональною складовою;

d^i – питома вага значимості i -ої функціональної складової;

n – кількість функціональних складових економічної безпеки фірми.

Важливим етапом в побудованому механізмі є ідентифікація, створення класифікації, оцінювання і ранжування загроз. Підкреслимо, що є доцільним будувати свою окрему, індивідуальну класифікацію загроз економічній безпеці підприємства для кожного конкретного підприємства з метою їх ідентифікації та для реалізації заходів протидії їм. Під час розробки стратегії заходів із забезпечення економічної безпеки підприємства потрібно визначитися з пріоритетом загроз, тобто ранжувати загрози.

Тактичне планування економічної безпеки за функціональними складовими передбачає визначення наступних пріоритетів:

фінансова – досягнення максимально ефективного використання корпоративних ресурсів;

кадрова – збереження і розвиток інтелектуального потенціалу підприємства, ефективне управління персоналом;

техніко-технологічною – ступінь відповідності застосовуваних на підприємстві технологій сучасним світовим аналогам;

політико-правовою – всебічне забезпечення діяльності підприємства, дотримання чинного законодавства;

інформаційною – ефективне інформаційне забезпечення господарської діяльності;

екологічною – дотримання екологічних норм, мінімізація втрат від забруднення навколишнього середовища;

силовою – забезпечення фізичної безпеки працівників фірми та збереження майна;

ресурсною – забезпечення підприємства усіма ресурсами.

Зауважимо, що систему заходів із забезпечення економічної безпеки підприємства необхідно погоджувати з цілями діяльності підприємства і ресурсами, які є на конкретному підприємстві. Місія підприємства, основні цілі і комплекс заходів із забезпечення рівня його економічної безпеки повинні мати вектори однакової направленості.

Рівень економічної безпеки підприємства залежатиме від того, наскільки ефективно його керівництво буде спроможне уникнути реальних загроз і ліквідувати шкідливі наслідки окремих негативних складових зовнішнього і внутрішнього середовища [14], застосовуючи систему заходів, які перераховані вище.

Надійність і ефективність системи безпеки підприємства визначають за одним критерієм – відсутністю чи наявністю завданих йому матеріальних збитків і моральної шкоди. Зміст цього критерію характеризується такими показниками:

- а) запобігання витоку конфіденційних відомостей;
- б) запобігання протиправним діям з боку персоналу підприємства, його відвідувачів, клієнтів або припинення таких дій;
- в) збереження майна й інтелектуальної власності підприємства;
- г) запобігання надзвичайним ситуаціям;
- д) припинення насильницьких злочинів щодо окремих (спеціально виділених) працівників підприємства і груп їх;
- е) своєчасне виявлення і припинення спроб несанкціонованого проникнення на об'єкти підприємства, що охороняються.

Удосконалення системи економічної безпеки полягає в створенні служби безпеки на підприємстві, якщо такої не існувало, чи системи безпеки на її базі, визначення механізмів її забезпечення та розробка організаційної структури управління системою, розрахунків усіх видів необхідних ресурсів, планування щомісячних витрат на забезпечення функціонування системи економічної безпеки (бюджет) тощо;

Окрім іншого запропонована схема управління КСЕБП передбачає здійснення постійного контролю (під час та після реалізації кожного етапу), коригування й удосконалення напрямів формування системи безпеки, щоб оптимально пристосовуватися і реагувати на зміни у зовнішньому та внутрішньому середовищах,

характері ризиків і загроз, а також зміни в законодавчому полі, появу на ринку недобросовісних конкурентів, зміну форм і методів протиправної діяльності, переліку конфіденційної інформації та інших чинників.

Зазвичай увесь комплекс діяльності із забезпечення економічної безпеки покладається на службу безпеки підприємства (у разі її наявності на підприємстві) як основну ланку системи економічної безпеки. Цю діяльність може координувати один із заступників керівника підприємства або рада з питань безпеки. Служба безпеки підприємства, у процесі реалізації методики, здійснює контрольні та координуючі функції, щоб забезпечити узгоджену роботу всіх працівників і структурних одиниць підприємства для вирішення системою економічної безпеки її основних завдань і досягнення цілей бізнесу.

Запропонована схема безпосередньо враховує специфіку підприємства (структуру, чисельність, напрями діяльність, стадію розвитку тощо) та обстановку, в якій воно функціонує (як зовнішнє середовище, так і внутрішню ситуацію); передбачає та враховує необхідність своєчасного і чіткого виконання запланованих заходів, спрямованих на адекватне реагування на зовнішні та внутрішні загрози; планування й розробку рішень; оптимальний розподіл використання ресурсів; застосування наявних у підприємства засобів забезпечення економічної безпеки; постійний контроль і коригування як повсякденної діяльності підприємства, так і самого процесу формування системи безпеки.

Напрямами зростання рівня економічної безпеки підприємства повинні стати:

- підвищення його фінансової стійкості та незалежності;
- посилення конкурентоспроможності технологічного потенціалу;
- раціоналізація системи управління фінансами;
- підвищення рівня кваліфікації персоналу та повноцінне використання його інтелектуального потенціалу;
- високий рівень екологічності роботи, мінімізація руйнівного впливу результатів діяльності на стан навколишнього середовища;
- поліпшення правової захищеності усіх аспектів діяльності;

– надійний захист інформаційного середовища суб'єкта, його комерційної таємниці та досягнення високого рівня інформаційного забезпечення роботи усіх його служб;

– забезпечення безпеки персоналу, капіталу, майна та комерційних інтересів.

Як підсумок, потрібно ще раз підкреслити, що надійна КСЕБП можлива лише за умови комплексного і системного підходу до її організації. Ця система забезпечує можливість оцінити перспективи зростання підприємства, розробити тактику і стратегію його розвитку, зменшити наслідки фінансових криз і негативного впливу нових загроз та небезпек.

1.3. Концепція управління економічною безпекою підприємства

Сучасні умови розвитку економіки України характеризуються значною кількістю чинників, яким притаманні невизначеність і дестабілізуючий характер дії. Внаслідок нестабільності умов зовнішнього середовища та виникнення екстремальних умов функціонування перед підприємствами постає необхідність набуття здатності до виживання й опору негативним впливам. Такі впливи становлять загрозу руйнування потенціалу підприємства, збільшують ризики управлінських рішень і являють собою загрози втрати підприємством економічної безпеки [45]. Звідси, діяльність підприємств потребує не лише забезпечення їх ефективного функціонування, а й розробки такої системи управління, за якої зміна чинників навколишнього середовища суттєво не впливала б на економічну діяльність суб'єктів господарювання.

Окрім захисту від негативного впливу зовнішнього середовища, необхідно зважити і на те, що підприємницька діяльність за своєю суттю є дуже різносторонньою, адже вона пов'язана з правовими, економічними, фінансовими, інформаційними, кадровими проблемами, технічним та технологічним аспектом, вирішенням організаційних питань, тощо. Коли ж мова йде про велике виробниче підприємство, яке має широке коло ділових зв'язків і значну кількість постачальників, кредиторів, позичальників, клієнтів, то управління такою складною системою значно ускладнюється.

Таким чином, кожне підприємство, будучи соціально-економічною системою, включає основні елементи і зв'язки між ними. Саме по лініях внутрішніх і зовнішніх зв'язків системи можуть виникати і реалізовуватися загрози для її економічної безпеки. Для гарантування максимального ступеню захисту від цих загроз необхідно здійснювати діяльність, яка повинна носити системний характер.

Зарубіжний і вітчизняний досвід забезпечення безпеки свідчить, що для боротьби з усією сукупністю потенційно можливих загроз необхідна чітка і цілеспрямована організація процесу протидії. Важливо, що у реалізації цього процесу повинні брати участь не тільки працівники безпосередньо відповідальні за цей напрямок, а також: професійні фахівці, керівництво організації, провідні співробітники організації. Для цього необхідно розробляти, із врахуванням специфіки функціонування певного підприємства індивідуальну концепцію безпеки. Проте, теорія і практика таких функціональних дій ще не склалися, зокрема, через недостатнє методологічне і теоретичне вивчення змісту цієї діяльності. Враховуючи дану ситуацію, практика на перший план висуває проблему розробки господарюючими суб'єктами такого основоположного документа, в якому були б зроблені висновки про основні загрози і ризики, сформульовані стратегічні та оперативні завдання, розставлені пріоритети у здійсненні організаційної та виконавчої діяльності у сфері безпеки, відображений вплив особливостей здійснення діяльності на можливість забезпечення безпеки, визначені завдання і способи діяльності структур, які забезпечують економічну безпеку підприємства. Таким основоположним документом є концепція безпеки підприємства, тобто, система поглядів, помислів, що визначають основний напрям, стратегію і тактику реалізації бізнесово-підприємницьких проєктів та програм [136; 100].

Важливість розроблення та реалізації концепції економічної безпеки підприємства обумовлена ще й тим, що з розвитком ринкових відносин в Україні вітчизняні підприємства зіткнулися з істотним зменшенням прямої державної підтримки їх діяльності. Окрім цього, сьогодні фактично держава прямо не здійснює управління діяльністю підприємств, а тільки регулює їхню діяльність за допомогою правових, економічних і соціальних заходів, за допомогою прямого (нормативні акти, положення тощо) і непрямого (податкова система, цінова та фінансово-кредитна політика тощо) регулю-

вання. Попри отриману самостійність, як правильно зазначає проф. О. Ареф'єва, нерозуміння місця управління безпекою для багатьох систем різного рівня ієрархії призвело до того, що наявні ресурси та резерви не використовувались повною мірою [4]. У результаті цього процес адаптації різних системи до нового ринкового середовища виявляється інертним із значною кількістю помилок, що загрожує їх подальшому існуванню.

Попри обгрунтовану у попередніх підрозділах позицію стосовно пріоритетної ролі безпеки, доцільно ще раз підкреслити, що стабільне функціонування, зростання економічного потенціалу будь-якого підприємства в умовах ринкових відносин багато в чому залежить від наявності надійної системи економічної безпеки. Сучасне підприємство знаходиться в умовах безперервної зміни зовнішнього середовища його існування. Ця нестабільність вимагає від господарюючих суб'єктів постійної адаптації, зокрема пошуку нових і вдосконалення вже відомих засобів забезпечення системи економічної безпеки заради досягнення економічної і соціальної мети діяльності підприємства.

Обумовлена важливість розроблення концепції економічної безпеки спонукала до першочергового з'ясування суті самого терміну «концепція». Так, концепція (від лат. *conceptio* – розуміння, система) – це певний спосіб розуміння, трактування будь-якого предмету, явища, процесу, головна точка зору на предмет тощо, керівна ідея для систематичного висвітлення. Термін «концепція» застосовується також для розгляду головного замислу, конструктивного принципу в науковій, технічній, політичній та інших видах діяльності [15].

На думку В. Шликова, концепція економічної безпеки – це система поглядів на проблему безпеки господарюючого суб'єкта на різних етапах і рівнях виробничої і комерційної діяльності, а також основні принципи і напрямки реалізації заходів по забезпеченню економічної безпеки [130].

У трактуванні українських вчених А. Козаченко, В. Пономарьова, А. Ляшенка [67], концепція формування і подальшого функціонування системи економічної безпеки підприємства базується на розумінні авторами сутності економічної безпеки підприємства. Концепцією системи управління економічною безпекою підприємства передбачається, що керівництво підприємства повинне

сформувати систему його пріоритетних інтересів, виявити інтереси взаємодіючих з ним суб'єктів господарювання й обрати такі форми і способи погодження цих інтересів, щоб результати взаємодії підприємства з даними суб'єктами забезпечили його прибуткову роботу.

На нашу думку, спираючись на вище процитоване визначення, зміст концепції економічної безпеки підприємства повинен містити загальні положення, сформовані із врахуванням специфіки функціонування певного підприємства, визначення інституційних та функціональних позицій, механізм забезпечення.

Мета розробки концепції економічної безпеки полягає у розробці вихідного документа достатньо короткого змісту, який би служив основою для досягнення кінцевої мети, а саме регламентував функціонування комплексної системи економічної безпеки для конкретного підприємства та визначив її місце в загальній структурі управління.

Методологічна основа підходу при проектуванні комплексних систем безпеки повинна ґрунтуватися на визначенні, ідентифікації, ранжуванні, аналізі та оцінці загроз і ризиків. При цьому необхідно враховувати множинність об'єктів захисту та величину сукупності, джерело надходження та характер ймовірності дії загроз. Слід також зазначити, що для кожного конкретного підприємства набір загроз має свій індивідуальний характер.

Виходячи з вище зазначеного слідує, що концепцією економічної безпеки підприємства передбачається, що його керівництвом має бути сформульована система пріоритетних інтересів, виявлені інтереси суб'єктів зовнішнього середовища, що взаємодіють з ним, та обрані такі форми і способи гармонізації або узгодження цих інтересів, щоб результати взаємодії підприємства із цими суб'єктами забезпечили його прибуткову роботу [94].

Ключовими позиціями при розробленні концепції економічної безпеки підприємства можна вважати наступні:

– система безпеки підприємницької діяльності не може бути однаковою в різних підприємствах, установах чи організаціях. Її відмінність та унікальність залежить від спеціалізації та структури виробничої діяльності, виробничого потенціалу, місця суб'єкта господарювання на ринку, кваліфікації та дисциплінованості кадрів тощо;

– система безпеки окремого підприємства є відносно самостійною й відособленою, стосовно систем безпеки інших суб'єктів підприємницької діяльності. У той час, якщо виходити, наприклад, з адміністративно-територіального поділу, система безпеки окремого підприємства є складовим елементом системи економічної безпеки міста, району, області, держави;

– система безпеки суб'єкта підприємницької діяльності може бути тільки комплексною. Її забезпечення тісно пов'язано з рівнем забезпечення науково-технічної, кадрової, екологічної, інформаційної, фізичної безпеки та інших. Ядром такої системи має бути комплексна система економічної безпеки підприємництва:

– ефективне забезпечення безпеки підприємства можливе за умов, коли вибір та застосування сил, засобів та охоронних заходів здійснюється на основі детально продуманої концепції, що визначає як стратегію, так і тактику.

– кожне підприємство є системою, що включає різні, пов'язані між собою складові елементи, причому якісні риси якої не властиві її частинам й компонентам. Саме на межі внутрішніх і зовнішніх зв'язків системи (підприємства) можуть утворюватися прогалини, через які реалізуються різні види загроз її економічної безпеки. Для забезпечення належного ступеня захисту від них і необхідно протиставити діяльність, яка б носила системний характер.

Спираючись на зазначені базові умови, нами створено власну концепцію економічної безпеки на мікрорівні (рис. 1.7).

У нашому трактуванні, яке є ключовим підходом до розуміння економічної безпеки підприємства, концепція повинна поєднувати як динамічну, так і статичну складові, органічне поєднання яких обумовлюється такими чинниками: складністю прогнозування змін зовнішнього середовища, неможливістю здійснення абсолютного контролю над внутрішнім середовищем, конфліктністю інтересів, складністю проблеми тощо.

Окремо потрібно підкреслити, що в основі розробленої концепції міститься комплексна система забезпечення, яка умовно розділена на науково-методичну, практичну та організаційно-економічну складові, зміст кожної з яких нами в загальному було розглянуто вище.

Потрібно підкреслити, що значну кількість елементів розробленої концепції нами було розглянуто у попередньому підрозділі, тому зосередимо увагу лише на окремих складових.

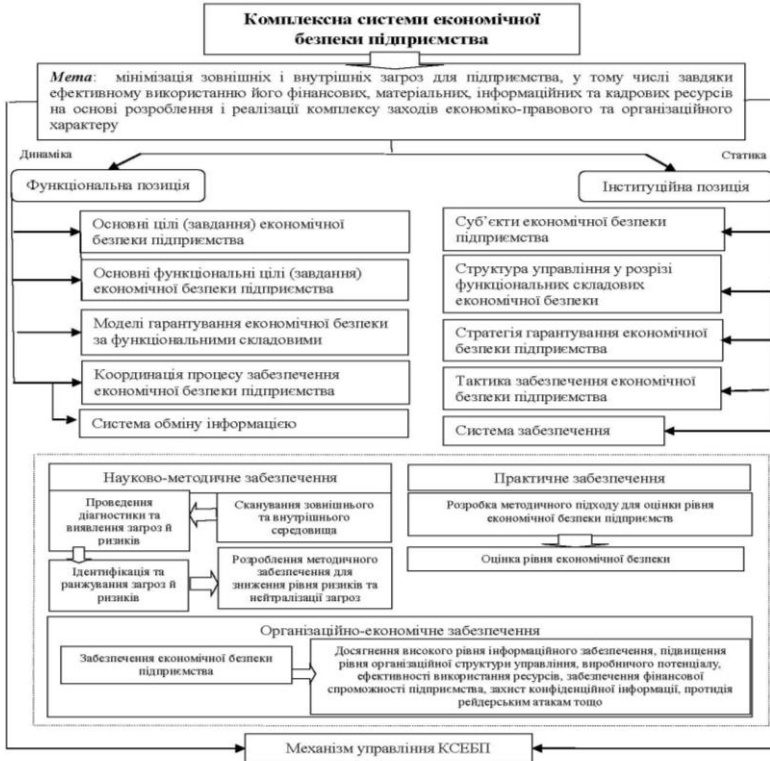


Рис. 1.7. Концепція економічної безпеки підприємства

Перш за все зазначимо, що ефективне управління підприємством в рамках концепції економічної безпеки неможливе без трансформації існуючої системи управління та формування нових комунікаційних зв'язків між структурними підрозділами підприємства. Важливість такого кроку обумовлена тим фактом, що суб'єктом безпеки, як зазначалось вище, виступає як окремий спеціалізований підрозділ, частково будь-який інший функціональний підрозділ та зрештою і опосередковано кожен працівник підприємства. Більш

того, на більшості вітчизняних підприємств функції забезпечення економічної безпеки виконують різні структурні підрозділи. Так, наприклад, фінансову безпеку, як правило, забезпечує фінансовий директор або головний бухгалтер, правовий захист здійснює юридичний відділ, за безпеку кадрів відповідає директор з персоналу і т.д. При цьому невирішеною залишається проблема координації дій усіх спеціалістів підприємства в системі забезпечення економічної безпеки.

Попри зазначене, потрібно визнати, що одним із найбільш оптимальних способів забезпечення ЕБП є створення внутрішньої служби економічної безпеки підприємства, яка координує роботу всіх структурних підрозділів, здійснює «силовий» захист, забезпечує максимальний захист всіх бізнес-процесів підприємства [70].

Стосовно ж інших складових концепції, то оскільки механізм управління КСЕБП нами подано вище, то зазначимо, що в процесі його реалізації важливе місце посідає виконання наступної сукупності завдань:

а) кадрові – система заходів для усунення ризиків у зв'язку з володінням певною частиною персоналу інформацією, що може розцінюватися як комерційна таємниця, недостатнім кваліфікаційно-освітнім рівнем працівників, помилками та зловживаннями (управління кадровими ризиками, вдосконалення кадрових технологій);

б) інформаційно-аналітичні – система заходів, що проводяться з метою прийняття ефективних та дієвих управлінських рішень, які стосуються стратегії і тактики розвитку підприємства; прийняття превентивних заходів і попередження реальних та можливих загроз економічній безпеці;

в) фінансово-економічні – система заходів, до яких належать: забезпечення економічної ефективності господарської діяльності суб'єкта господарювання; забезпечення фінансової стабільності та фінансової незалежності; забезпечення високої конкурентоспроможності продукції, товарів та послуг на основі ефективного менеджменту та маркетингу фірми тощо;

г) правові – дії, спрямовані на відслідковування нових законодавчих актів, що приймаються у сфері економічної безпеки, та активне застосування усіх законів та підзаконних актів України у боротьбі за інтереси конкретного суб'єкта господарювання;

д) техніко-технологічні – заходи, спрямовані на досягнення відповідного рівня освоєння виробничої потужності, інноваційну політику підприємства, своєчасне оновлення основних виробничих фондів тощо;

е) ресурсні – система заходів, що проводяться з метою забезпечення виробництва основними ресурсами: фінансовими, матеріальними, трудовими та ін.

Таким чином, розроблена концепція забезпечення й управління економічною безпекою підприємства, із врахуванням методологічних положень викладених у попередньому та даному підрозділі, заснована на ряді положень, що відображають: склад і структуру об'єктів економічної безпеки; принципи забезпечення економічної безпеки; класифікацію загроз економічної безпеки; основні принципи відбору й оцінювання основних функціональних складових економічної безпеки підприємства; базові підходи до розробки і впровадження механізмів управління економічною безпекою підприємства. Комплексне оцінювання рівня економічної безпеки підприємства дає можливість апарату управління вчасно реагувати на дестабілізуючі впливи внутрішніх і зовнішніх загроз, приймати ефективні управлінські рішення щодо зростання рівня економічної безпеки, що, у свою чергу, забезпечує прогресивний розвиток підприємства.

ЛІТЕРАТУРА ДО ПЕРШОГО РОЗДІЛУ

1. Альгин А. П. Риск и его роль в общественной жизни / А. П. Альгин. – М.: Мысль, 1989. – 187 с.
2. Амитан В. Н. Экономическая безопасность: понятие, концепция / В. Н. Амитан, А. Г. Амитан, А-ндр. Г. Амитан / Промитей: регіональний збірник наукових праць з економіки. – Донецьк: Юго-Восток, 2000. – № 2. – 333 с.
3. Аналітична доповідь Українського центру економічних і політичних досліджень до засідання круглого столу «Актуальні проблеми економічної безпеки України». – К.: УЦЕПД, 1997. – 163 с.
4. Ареф'єва О. В. Наукові основи формування економічної безпеки підприємств / О. В. Ареф'єва // Недержавна система безпеки підприємництва як суб'єкт національної безпеки України: Збірник матеріалів наук.-практ. конф., Київ, 16–17 травня 2001 р. – К.: Вид-во Європейського ун-ту фінансів, інформаційних систем, менеджменту і бізнесу, 2003. – С. 49–53.
5. Ареф'єва О. В. Планування економічної безпеки підприємств / О. В. Ареф'єва, Т. Б. Кузьменко. – К.: Вид-во Європ. ун-ту, 2005. – 170 с.
6. Бабанова Ю. В. Теоретико-методологические основы экономической безопасности хозяйствующих субъектов / Ю.В.Бабанова: Дис... к.э.н.: 08.00.01. – Челябинск, 2004. – 198 с.
7. Базилюк Я. Б. Умови формування і стратегія забезпечення конкурентоспроможності національної економіки: Автореф. дис. канд. екон. наук 21.04.01 / Я. Б. Базилюк; Нац. ін-т стратег. дослідж., Нац. ін-т пробл. міжнар. безпеки. – К., 2001. – 17 с.
8. Безопасность предпринимательской деятельности : учебн. / под общей ред. д.ф.н. Л. Д. Шарый. – М.: ВК, 2005. – 480 с.
9. Белінська Я. В. Теоретичні засади аналізу валютних ризиків / Я. В. Белінська // Актуальні проблеми економіки. – 2002. – № 10. – С. 34–40.
10. Бендиков М. Экономическая безопасность наукоемких производств / М. Бендиков, Е. Хрусталева // Вопросы экономики. – 1999. – № 9. – С. 9.
11. Береза З. В. Суть та складові економічної безпеки підприємства / З. В. Береза // Наука й економіка. – 2009. – № 4 (16). – С. 59–64
12. Берлач А. І. Безпека бізнесу : навч. посіб. / А. І. Берлач. – К.: Університет «Україна», 2007. – 280 с.
13. Берталанфи Л. фон. Общая теория систем. Обзор проблем и результатов / Л. фон Берталанфи // Системные исследования: Ежегодник, 1969. – М. : Наука, 1969. – С. 30–54.

14. Болгова К. В. Організаційно-економічний механізм забезпечення економічної безпеки підприємства [Електронний ресурс] / К. В. Болгова, Л. І. Шилова. – Режим доступу : www.masters.donntu.edu.ua
15. Большая Советская Энциклопедия: В 30 томах. / Гл. ред. А.М. Прохоров. Изд. 3-е. – М.: Советская Энциклопедия, 1973.
16. Бондаренко О. М. Показники, критерії та методи оцінки економічної безпеки авіакомпаній / О. М. Бондаренко // Наукові праці ОНАЗ : періодичний наук. зб. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. – Одеса, 2003. – С. 59–64.
17. Будович Л. С. Управление предприятием на основе совершенствования системы экономической безопасности: дис... к.э.н.: 08.00.05. – М., 2007. – 212 с.
18. Варналій З. С. Економічна безпека України: проблеми та пріоритети зміцнення : моногр. / З. С. Варналій, Д. Д. Буркальцева, О. С. Саєнко. – К. : Знання України, 2011. – 299 с.
19. Васильців Т. Економічна безпека підприємництва України: стратегія та механізми зміцнення : моногр. / Т. Васильців. – Львів: Арал, 2008. – 384 с.
20. Васильчак С. В. Економічна безпека підприємства та її складова в сучасних умовах / С. В. Васильчак, А. І. Веселовський // Науковий вісник НЛТУ України. – 2010. – Вип. 20.15. – С. 98–105.
21. Вишняков Я. Д. Управление обеспечением безопасности предприятий : экономические подходы [Електронний ресурс] / Я. Д. Вишняков, С. А. Марченко // Менеджмент в России и за рубежом. – 2001. – №5. – Режим доступу : www.mevriz.ru.
22. Вітлінський В. В. Аналіз, моделювання та управління економічним ризиком : навч. посіб. / В. В. Вітлінський, П. І. Верченко. – К.: КНЕУ, 2000. – 292 с.
23. Воробьев Е. М. Проблемы экономической безопасности в странах рыночной трансформации / Е. М. Воробьев // Вісник ХДУ. Економічна серія. – 1999. – 3446. – С. 162–166.
24. Гапоненко В. Ф. Экономическая безопасность предприятий / В. Ф. Гапоненко, А. Л. Беспалько, А. С. Власков. – М.: Издательство «Ось-89», 2007. – 208 с.
25. Генеза ринкової економіки (політекономія, мікроекономіка, макроекономіка, економічний аналіз, економіка підприємства, менеджмент, маркетинг, фінанси, банки, інвестиції, біржова діяльність): Терміни, поняття, персоналії. Укладачі: В. С. Іфтемчук, В. А. Григорьев, М. І. Маниліч, Г. Д. Шутак ; за наук. ред. Г. І. Башняніна і В. С. Іфтемчука. – К.: «Магнолія плюс», 2004. – 688 с.
26. Герасимчук З. В. Економічна безпека регіону: діагностика та механізм забезпечення: моногр. / З. В. Герасимчук, Н. С. Вавдіюк. – Луцьк : Надтир'я, 2006. – 243 с.

27. Глущенко В. В. Управление рисками. Страхование / В. В. Глущенко. – М. : ТОО НПЦ «Крылья». – 1999. – С. 11–16.
28. Головченко О. М. Економічна безпека регіону в гарантуванні стабільності національної економіки : моногр. / О. М. Головченко. – Одеса: 2008. – 399 с.
29. Гончаренко Л. П. Управление безопасностью : учеб. пособ. / Л. П. Гончаренко, Е. С. Куценко. – М.: КНОРУС, 2005. – 272 с.
30. Городецкий А. Вопросы безопасности экономики России / А. Городецкий // Экономист. – 1995. – №10. – С. 46–49.
31. Грунин О. А. Экономическая безопасность организаций : учеб. пособ. / О. А. Грунин, С. О. Грунин. – СПб. – 2002. – 256 с.
32. Грунин С. О. Механизм управления экономической безопасностью организации / С. О. Грунин. – СПб, 2001. – 195 с.
33. Губський Б. В. Економічна безпека України : методологія виміру, стан і стратегія забезпечення : моногр / Б. В. Губський. – К.: Укрархбудінформ, 2001. – 121 с.
34. Гунько М. М. Словник банкіра / М. М. Гунько, Т. С. Смовженко. – Львів: Фенікс Лтд., 1992. – 49 с.
35. Дзилиев М. И. Основы обеспечения безопасности жизнедеятельности : курс лекций / М. И. Дзилиев, Н. Н. Потрубач. – М., 1996. – 186 с.
36. Дмітрієв І. А. Визначення переліку складових економічної безпеки підприємства [Електронний ресурс] / І. А. Дмітрієв, А. О. Близьнюк. – Режим доступу: www.nbuv.gov.ua/portal/Soc_Gum/2011_23_1/33DmBl.html.
37. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО «ТИД «ДС», 2001. – 688 с.
38. Донець Л. І. Економічна безпека підприємства : навч. посіб. / Л. І. Донець, Н. В. Ващенко. – К.: ЦУЛ, 2008. – 240 с.
39. Доронин А. Бизнес-разведка / А. Доронин. – М: Ось-89, 2003. – 384 с.
40. Дубецька С. П. Економічна безпека підприємств України / С. П. Дубецька // Недержавна система безпеки підприємництва як суб'єкт національної безпеки України: Збірник матеріалів наук.-практ. конф., Київ, 16-17.05.2001. – К.: Вид-во європейського ун-т фінансів, інформаційних систем, менеджменту і бізнесу, 2003. – С. 146–172.
41. Евдокимов Ф. И. Критерии оценки уровня экономической безопасности предприятия [Электронный ресурс] / Ф. И. Евдокимов, О. А. Бородина. – Режим доступу : www.borodina2002.ukrtop.com
42. Евдокимов Ф. И. Факторы и методы оценки экономической безопасности предприятия [Электронный ресурс] / Ф. И. Евдокимов, В. С. Белозубенко, О. А. Бородина. – Режим доступа : www.borodina2002.ukrtop.com

43. Економіка підприємства: підруч. / за заг. ред. С. Ф. Покропівного. – 2-е вид., перероб. та доп. – К. : КНЕУ, 2000. – 528 с.
44. Економіка підприємства : підруч. / [Посилкіна О.В., Сагайдак Р.В., Козирєва О.В., Латін П.Д.] ; за ред. О.В. Посилкіної. – Х. : Вид-во НФаУ: Золоті сторінки, 2006. – 488 с.
45. Економічна безпека підприємств, організацій та установ : [навч. посібник для студ. вищ. навч. закл.] / В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін. – К. : Правова єдність, 2009. – 544 с.
46. Економічна безпека України: сутність і напрямки забезпечення : моногр. / В. Т. Шлемко, І. Ф. Бінько. – К.: НІСД, 1997. – 144 с.
47. Єрмошенко М. Визначення загрози національним інтересам держави у фінансово-кредитній сфері / М. Єрмошенко // Економіка України. – 1999. – №1. – С.4–12.
48. Єрмошенко М. М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення / М. М. Єрмошенко. – К.: Київ. нац. торг.-екон. ун-т., 2001, – 309 с.
49. Живко З. Б. Філософські, економічні та правові підходи до трактування підприємницької діяльності / З. Б. Живко // Історія народного господарства та економічної думки України: зб. наук. праць. – Вип. 45. – К. : ДУ «Ін-т екон. та прогнозув. НАН України», 2012. – С. 55–66.
50. Забродский В. А. Современные методы организации и управления промышленным производством / В. А. Забродский, Н. А. Кизим, Л. И. Янов. – Харьков : АО «Бизнес-Информ», 1997. – 64 с.
51. Забродский В. Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15–16. – С. 35–37.
52. Иванов А. В. Экономическая безопасность предприятия / А. В. Иванов, В. В. Шлыков. – М.: Вираз-центр. – 1995. – 265 с.
53. Иващенко Г. В. Доктрина информационной безопасности и методологические проблемы теории безопасности / Г. Иващенко // Глобальная информатизация и безопасность России / [общ. ред. проф. В. И. Дебреньков]. – М., 2001. – 398 с.
54. Ильяшенко С. Н. Составляющие экономической безопасности предприятия и подходы к их оценке / С. Н. Ильяшенко // Актуальні проблеми економіки. – 2003. – № 3. – С. 12–19.
55. Кавун С. В. Концептуальная модель системы экономической безопасности предприятия / С. В. Кавун // Економіка розвитку. – 2007. – №3. – С. 97–101.
56. Кавун С. В. Методика построения политики безопасности организации / С. В. Кавун, Г. В. Шубина // Бизнес Информ. – 2005. – №1–2. – С. 96–102.
57. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия / С. В. Кавун // Управління розвитком. – 2008. – № 6. – С. 17–21.

58. Калина А. В. Економіка підприємства : навч. посіб. / А. В. Калина, А. А. Котвицький, О. З. Стожок. – К. : Знання України, 2007. – 324 с.
59. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посібн. / М. І. Камлик. – К.: Атіка, 2005. – 432 с.
60. Капустин Н. Н. Экономика предприятия / Н. Н. Капустин. – М.: Флинта, 2002. – 204 с.
61. Капустин Н. Экономическая безопасность отрасли и фирмы / Н. Капустин // Бизнес-информ. – 1999. – № 11–12. – С. 45–47.
62. Кашин А. В. Экономическая безопасность предприятий: управленческие проблемы / А. В. Кашин // Экономические науки. – 2008. – №1. – С. 171–173.
63. Кириенко А. В. Механізм досягнення і підтримки економічної безпеки підприємства : автореф. дис... канд. екон. наук.: 08.06.01 / Київський національний економічний університет. – К., 2000. – 19 с.
64. Кириленко В. І. Інвестиційна складова економічної безпеки : моногр. / В. І. Кириленко. – К.: КНЕУ, 2005. – 232 с.
65. Кіриченко А. А. Методологічні основи економічної безпеки суб'єктів господарювання в трансформаційній економіці / А. А. Кіриченко, Ю. Г. Кім // Актуальні проблеми економіки. – 2008. – № 12 (90). – С. 53–65.
66. Ковалев Д. Экономическая безопасность предприятия / Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48–51.
67. Козаченко Г. В. Економічна безпека підприємства: сутність та механізм забезпечення : моногр. / Г. В. Козаченко, В. П. Пономарьов, О. М. Ляшенко. – К. : Лібра, 2003. – 280 с.
68. Колобчинський О. Л. Методика формування системи економічної безпеки підприємства / О. Л. Колобчинський // Актуальні проблеми економіки. – 2009. – № 4(94). – С. 41–45.
69. Колпаков П. А. Концептуальные основы экономической безопасности фирмы: [Электронный ресурс] / П. А. Колпаков. – Режим доступа: <http://e-journal.spa.msu.ru/images/File/Awtoreferat-Kolpakov.pdf>
70. Комаха А. Организация службы экономической безопасности на предприятии / А. Комаха // Бизнес и безопасность. – 2002. – № 3. – С. 14–16.
71. Концепція економічної безпеки антикризового управління економікою України. Науково-аналітична доповідь. – К.: «Дорадо-Друк», 2009. – 64 с.
72. Коробчинський О. Л. Методика формування системи економічної безпеки підприємства / О. Л. Коробчинський // Актуальні проблеми економіки. – 2009. – № 4 (94). – С. 41–45.

73. Королев М. И. Принципы организации системы защиты фирмы. [Электронный ресурс] / М. И. Королев. – Режим доступа: http://www.ps.j.ru/saver_magazins/detail.php.

74. Корчевська Л. О. Ітеративний підхід до дослідження економічної безпеки підприємства / Л. О. Корчевська // Актуальні проблеми економіки. – 2012. – №4. – С. 111–119.

75. Корчевська Л. О. Система принципів забезпечення економічної безпеки підприємства / Л. О. Корчевська // Вісник економіки транспорту і промисловості. – 2012. – № 38. – С. 44–49.

76. Крысин А. Безопасность предпринимательской деятельности / А. Крысин. – М., 1996. – 256 с.

77. Кузенко Т. Б. Управління фінансовою безпекою підприємства: методичний аспект / Т. Б. Кузенко, Н. В. Сабліна, О. Ю. Литовченко // Вісник економіки транспорту і промисловості, 2010. – № 29. – С. 119–123.

78. Кузнецов В. Н. Культура безопасности: Социологическое исследование. Серия «За нашу и вашу безопасность». Приложение к журналу «Безопасность Евразии» / В. Н. Кузнецов. – М.: Наука. – 2001. – 320 с.

79. Куркин Н. В. Управление экономической безопасностью развития предприятия : моногр. / Н. В. Куркин. – Днепропетровск: АРТ-ПРЕСС, 2004. – 452 с.

80. Локотецька О. В. Концепція комплексної системи гарантування економічної безпеки підприємства / О. В. Локотецька // БІЗНЕСІН-ФОРМ. – 2012. – № 3. – С. 171–174.

81. Лукасевич И. Я. Анализ финансовых операций / И. Я. Лукасевич. – М.: Финансы, Изд. об-ние «Юнити», 1998. – 400 с.

82. Лысенко Ю. Г. Механизмы управления экономической безопасностью / Ю. Г. Лысенко, С. Г. Мищенко, Р. А. Руденский. – Донецк : ДонНУ, 2002. – 178 с.

83. Мак-Мак В. П. Служба безопасности предприятия / В. П. Мак-Мак. – М.: Школа охраны «Баярд», 2003. – 208 с.

84. Манилов В. Исследование проблем национальной безопасности: вопросы методологии / В. Манилов // Военная мысль. – 1995. – № 5. – С. 9–18.

85. Манів З. О. Економіка підприємства : навч. посібник / З. О. Манів, І. М. Луцький. – [2-е вид., стер.]. – К. : Знання, 2006. – 580 с.

86. Мельник Л. В. Аналіз та оцінка ефективності управління інноваційними процесами на підприємствах / Л. В. Мельник, А. Я. Гончарук, О. Є. Кузьмін // Управление развитием социально-экономических систем: глобализация, предпринимательство, устойчивый экономический рост: Труды пятой международной научной конференции студентов и молодых ученых. Ч 1. – Донецк: ДонНУ, 2004 – С. 315–317.

87. Мертон Р. Социальная теория и социальная структура / Р. Мертон ; [пер.с англ. Е.Н. Егоровой и др.]. – М. : АСТ : Хранитель, 2006. – 873 с.
88. Мехеда Н. Г. Особливості оцінки економічної безпеки за окремими функціональними складовими [Електронний ресурс] / Н. Г. Мехеда, А. Маджула. – Режим доступу: www.rusnauka.com/portal/13_EISN_2012/Economics/10_109523.doc.htm
89. Мищенко С. Н. Система обеспечения экономической безопасности организации: дис. ... канд. экон. наук: 08.00.05. – Ростов-на-Дону, 2004. – 197 с.
90. Могильний А. І. Основи безпеки бізнесу / А. І. Могильний, В. Н. Бесчасний, Ю. О. Винокуров. – Донецьк. – 2000. – 351 с.
91. Моделювання економічної безпеки: держава, регіон, підприємство : моногр. / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. – Х., 2006. – 240 с.
92. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус; за заг. ред. П. В. Мельника, Н. Р. Нижник. – Ірпінь, 2000. – 304 с.
93. Ніколаюк С. І. Безпека суб'єктів підприємницької діяльності / С. І. Ніколаюк, Д. Й. Никифорчук. – К.: КНТ, 2005. – 320 с.
94. Новікова О. Ф. Економічна безпека: концептуальні визначення та механізми забезпечення : моногр. / О. Ф. Новікова, Р. В. Покотиленко. – Донецьк : НАН України, Ін-т економіки промисловості, 2006. – 408 с.
95. Овчаренко Є. І. Система економічної безпеки підприємства: ознаки та принципи функціонування / Є. І. Овчаренко // Економіка Менеджмент Підприємництво. – 2012. – № 24 (II). – 133–143.
96. Ожегов С. Толковый словарь русского языка / С. Ожегов, Н. Шведова. – М., 1992. – 521 с.
97. Ожегов С. И. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова. – Российская академия наук. Институт русского языка им. В. В. Виноградова. – 4-е изд., доп. – М.: Азбуковник, 1999. – 1280 с.
98. Організація управління економічною безпекою підприємства : автореф. дис... канд. экон. наук: 08.06.01 / НАН України; інститут економіки промисловості / Н. О. Подлужна. – Донецьк, 2003. – 20 с.
99. Орлов П. І. Основи економічної безпеки фірми : навч. посіб. / П. І. Орлов, В. Є. Духов. – Х.: ТОВ «Прометей-Прес», 2004. – 284 с.
100. Основи економічної безпеки : підруч. / [О. М. Бандурка, В. Є. Духов, К. Я. Петрова, І. М. Червяков]. – Харків : Вид-во Нац. ун-ту внутр. справ, 2003. – 236 с.
101. Основы экономической безопасности (Государство, регион, предприятие, личность) / [под ред. Е. А. Олейникова]. – М. : Бизнес-школа «Интел-синтез», 1997. – 278 с.

102. Особливості гарантування економічної безпеки підприємницької діяльності в ринкових умовах : моногр. / [Долженков О.Ф., Жуковська Ж.О., Головченко О.М.] ; за ред. О.Ф. Долженкова. – Одеса: ОЮІ ХНУВС, 2007. – 208 с.
103. Парсонс Т. О структуре социального действия / Т. Парсонс. – М.: Акад. проект, 2002. – 878 с.
104. Петрович Й. М. Економіка підприємства : підруч. / [Петрович Й. М., Кіт А. Ф., Семенів О. М. та ін.] ; за заг. ред. Й. М. Петровича. – Львів : «Новий Світ– 2000», 2004. – 680 с.
105. Покропивний С. Ф. Економіка підприємства : підруч. / за заг. ред. С. Ф. Покропивного. – К.: КНЕУ, 2001. – 528 с.
106. Полушкин О. А. Управление безопасностью предприятий в условиях рыночной экономики / О. А. Полушкин // Закон и право. – 2005. – №10. – С. 46–50.
107. Проблеми управління економічною безпекою суб'єктів господарювання : моногр. / О. А. Кіриченко, В. С. Сідак, С. М. Лаптев та ін. – К.: Ун-т економіки та права «КРОК», 2008. – 403 с.
108. Раздина Е. Коммерческая информация и экономическая безопасность предприятия / Е. Раздина // Бизнес-Информ. – 1997. – №24. – С. 63–65.
109. Раздина Е. В. Экономическая безопасность (сущность и тенденции развития) : автореф. дис... канд. экон. наук: 08.00.01 / Е. В. Раздина. – М., 1998. – 20 с.
110. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур / Н. Й. Реверчук. – Львів : ЛБІ НБУ, 2004. – 195 с.
111. Роль маркетинговых исследований в экономической безопасности предприятия [Электронный ресурс] / Ф. И. Евдокимов, О. А. Бородина, Ф. И. Евдокимов, О. А. Бородина. – Режим доступа : www.borodina2002.ukrtop.com
112. Романенко Л. Ф. Ризики у банківській діяльності / Л. Ф. Романенко, А. В. Коротєва // Фінанси України. – 2003. – №5. – С. 121–127.
113. Руда Т. В. Сутність та структуризація економічної безпеки / Т. В. Руда // Митна безпека. – 2012. – № 1 – 2. – С. 51–57.
114. Русин Ю. П. Организационные меры обеспечения экономической безопасности предприятия в условиях конкуренции: Дис... к.э.н.: 05.02.22. – М., 2005. – 210 с.
115. Слободяник Т. М. Запровадження комплексної системи економічної безпеки та оцінка її ефективності на сучасному підприємстві / Т. М. Слободяник // Економічний простір. – 2008. – № 12/2. – С. 22–26.
116. Соколова Л. В. Информационное обеспечение функционирования комплексной системы экономической безопасности предприятия / Л. В. Соколова, К. В. Шутов // Управління розвитком. – 2008. – № 14. – С. 18–19.

117. Соснин А. С. Менеджмент безопасности предпринимательства: учеб. пособ. / А. С. Соснин, П. Я. Прыгунов. – К.: Изд-о Европ. ун-та, 2002. – 357 с.
118. Соціальна політика та економічна безпека / [Головінов О. М. та ін.]; під заг. ред. Є. І. Крихтіна. – Донецьк: Каштан, 2004. – 335 с.
119. Судакова О. І. Стратегія забезпечення належної економічної безпеки підприємства [Електронний ресурс] / О. І. Судакова, А. В. Шкурупій, Д. В. Гречко. – Режим доступу: www.rusnauka.com.
120. Сумець О. М. Стратегії сучасного підприємства та його економічна безпека: навч. посіб. / О. М. Сумець, М. Б. Тумар. – К.: «Хай-Тек Прес», 2008. – 400 с.
121. Тамбовцев В. Л. Экономическая безопасность хозяйственных систем: структура проблемы / В. Л. Тамбовцев // Вестн. Моск. ун-та. – М.: Экономика. – 1995. – №3. – С. 3-5.
122. Тумар М. Б. Основи економічної безпеки підприємства: навч. посіб. / М. Б. Тумар. – К.: «Хай-Тек Прес», 2008. – 232 с.
123. Фінансовий менеджмент: навч. посіб. / за ред. проф. Г. Г. Кірейцева. – Житомир: ЖІТІ, 2001. – 432 с.
124. Финансовый менеджмент: теория и практика: учебн. / под ред. Е. С. Стояновой. – 4-е изд., перераб. и доп. – М.: Перспектива, 1999. – 656 с.
125. Цыпина И. С. Экономическая безопасность (национальный и международный аспект): учебн.-метод. пособ. / И. С. Цыпина, Ю. Ф. Кваша. – М.: ВГНА МНС РФ, 2001. – 108 с.
126. Четвертаков Р. В. Развитие представлений о безопасности России (IX – XVII вв.) / Четвертаков Р. В. // Биосфера. – 2002. – №1. – С. 56–61.
127. Шаваев А. Г. Криминологическая безопасность негосударственных объектов экономики / А. Г. Шаваев. – М.: ИНФРА-М, 1995. – 126 с.
128. Шваб Л. І. Економіка підприємства: навч. посіб. / Л. І. Шваб. – Житомир: ЖДТУ, 2004. – 459 с.
129. Шершньова З. Є. Стратегічне управління: підруч. / З. Є. Шершньова; [2-ге вид., перероб. і доп.]. – К.: КНЕУ, 2004. – 699 с.
130. Шлыков В. В. Комплексное обеспечение экономической безопасности предприятия / В. В. Шлыков. – СПб: Алетей. – 1999. – 318 с.
131. Шнышко А. С. Экономические войны: истоки, формы, цели, проблемы, перспективы / А. С. Шнышко. – К.: Генеза, 2007. – 376 с.
132. Ярочкин В. И. Основы безопасности бизнеса и предпринимательства / В. И. Ярочкин, Я. В. Бузанова. – М., 2005. – 206 с.
133. Ярочкин В. И. Секьюритология – наука о безопасности жизнедеятельности / В. И. Ярочкин. – М.: «Ось-89», 2000. – 400 с.
134. Ярочкин В. И. Система безопасности фирмы / В. И. Ярочкин. – М.: Ось-89, 2003. – 352 с.

135. Экономика предприятия : учебн. пособ. / под ред. д-ра э. н., проф. Л. Г. Мельника. – Сумы: ИТД «Университетская книга», 2002. – 632 с.
136. Экономическая безопасность / А. И. Архипов, Р. А. Белоусов, А. Н. Быков и др. ; под ред. В. К. Сенчагова. – Москва: ЗАО «Финстатинформ», 1998. – 621 с.
137. Экономическая безопасность деятельности предприятия / под ред. В. К. Сенгалова. – М.: Финстатинформ, 1999. – 511 с.
138. Экономическая безопасность коммерческих предприятий и деловая разведка. [Электронный ресурс] / А. А. Митрофанов. – Режим доступа: www.bre.ru/security/22843.html.
139. Экономическая безопасность хозяйственных систем / под общей ред. А. В. Колосова. – М.: Изд-во РАГС, 2001. – 446 с.
140. Экономическая и национальная безопасность : учеб. / [под ред. Е. А. Олейникова]. – М. : Издательство «Экзамен», 2004. – 768 с.
141. Эшби У. Р. Принципы самоорганизации / У. Р. Эшби ; пер. с англ. – М. : Мир, 1966. – 343 с.

Розділ 2

ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Фінансово-економічні результати діяльності підприємства в оцінюванні економічної безпеки

Ключовою умовою гарантування національної безпеки будь-якої країни є високий рівень безпеки первинної ланки її економіки, тобто сукупності підприємств. З іншої сторони, згідно ст. 17 Конституції України забезпечення економічної безпеки, в т. ч. і суб'єктів господарської діяльності, є однією з основних функцій держави. Взаємозв'язок двох рівнів: економічної безпеки держави та безпеки кожного підприємства є беззаперечний, а відтак, внаслідок складності трансформаційних процесів, які мають місце в нашій країні упродовж останніх двох десятиків років, та унікальності ситуації, до якої складно застосувати напрацьовані в розвинутих країнах механізм управління, розв'язання проблеми гарантування економічної безпеки на мікрорівні потребує особливої уваги, і перш за все, науковців.

За часів існування Радянського Союзу, проблема забезпечення економічної безпеки окремого підприємства просто не існувала, адже уся система працювала виключно на гарантування безпеки, в т. ч. в найбільшій мірі військової, мега країни. Зазначене обумовлювалося і тими обставинами, що усі суб'єкти господарювання були виключно державної форми власності, не існувала конкуренція та інститут банкрутства.

Починаючи з 1990 р. у зв'язку з переходом від планової до ринкової економіки докорінно змінилися умови функціонування вітчизняних підприємств. Якщо за радянської системи економічних

відносин понад 90% ВВП формували підприємства з державною формою власності, то здійснення масштабних процесів приватизації та роздержавлення зменшили цю частку майже до 10%. Отож, сьогодні підприємства недержавної форми власності суттєво впливають на ВВП держави, на її добробут та безпечний розвиток. Таким чином, ефективна господарська діяльність та високий рівень економічної безпеки суб'єктів господарювання має розглядатися як гарантія свободи й незалежності всієї України, її економічної могутності, як фундамент міцності держави в цілому.

Треба констатувати, що у зв'язку з розпадом Радянського Союзу та змінами у формах власності наша держава втратила монополію на забезпечення безпеки у сфері економіки, а значна кількість суб'єктів, на захисті інтересів яких раніше стояв увесь державний механізм, сьогодні фактично залишилася незахищеною. Це стосується передусім більшості підприємств малого та середнього бізнесу, які, як відомо, є базисом і забезпечують розвиток економічної системи в будь-якій країні світу. Їх подальший розвиток, входження до наявних регіональних і всесвітніх економічних структур вимагають від вітчизняного бізнесу негайного посилення власних позицій на зовнішніх і внутрішніх ринках, різкого підвищення конкурентоспроможності товарів і послуг, що також обумовлює нагальну необхідність удосконалення системи управління економічною безпекою кожного підприємства.

Передумовою постановки та розв'язання будь-якого завдання є оцінка початкової ситуації чи стану об'єкту уваги. У нашому випадку важливим підґрунтям для удосконалення управління економічною безпекою підприємства є визначення загального рівня безпеки стосовно функціонуючих в Україні суб'єктів господарської діяльності.

Беручи за основу офіційні статистичні дані охарактеризуємо рівень економічної безпеки вітчизняних підприємств, його зміну під впливом фінансової кризи 2008-2009 рр.

Для ринкової економіки характерним є ризик банкрутства, що з однієї сторони стимулює підприємця до зваженого прийняття будь-якого рішення, більш ефективного використання наявних у нього ресурсів та задоволення потреб споживачів, а з іншої – уможливорює систематичну ротацію, коли на місце банкрута приходять новий товаровиробник. Відтак, кількість суб'єктів господарю-

вання систематично змінюється, в т.ч. під впливом загальноекономічних процесів, характерних для національної економіки. Важливо, що відносні показники інтенсивності розвитку підприємництва є ключовими для характеристики рівня безпеки на мікрорівні. Одним з таких показників можна вважати кількість суб'єктів господарювання у розрахунку на 10 тис. осіб населення, динаміку якого у графічному вигляді представлено на рис. 2.1.

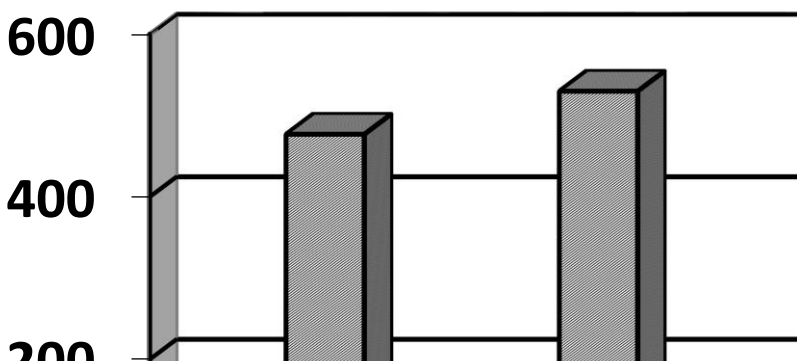


Рис. 2.1. Кількість суб'єктів господарювання на 10 тис. осіб наявного населення

Важливим для характеристики рівня економічної безпеки вітчизняних підприємств є той факт, що у період кризи, який визначається 2008-2009 рр. кількість підприємств та фізичних осіб, які займаються підприємницькою діяльністю, зростала і була вищою у порівнянні із докризовим 2007-м. Водночас, для посткризових – 2010-2011 рр. притаманні суто негативні тенденції, коли кількість підприємств скоротилась у 2011 р. стосовно 2009 р. на 15,91%, а фізичних осіб-підприємців – на 49,91%, що вказує на погіршення умов ведення бізнесу, неможливості забезпечення необхідного для функціонування рівня економічної безпеки.

Окремим важливим параметром функціонування підприємств в Україні є масштаби діяльності, для характеристики якого визначена структура у розрізі груп «великі», «середні» та «малі» стосовно 2011 р. на рис. 2.2.

93,7

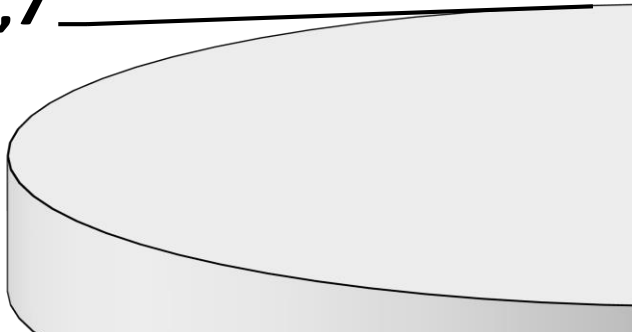


Рис. 2.2. Структура підприємств за масштабами діяльності у 2011 р., %

Приватизація державної форми власності, яка активно здійснювалася в Україні у 90-х роках, у сукупності із стимулюванням розвитку підприємництва суттєво змінили структуру суб'єктів господарювання за масштабами діяльності. Так, домінуючу частку – 93,7% складають малі підприємства і лише 0,6% – великі. Цей аспект є досить важливим, адже сьогодні активно розробляються і впроваджуються у практику інструменти забезпечення економічної безпеки для великого та середнього бізнесу, які не можна застосувати на малих підприємствах, що суттєво впливає на загальний рівень безпеки усієї сукупності підприємницьких структур, не сприяючи його зростанню.

Виявлені тенденції вимагають конкретизації подальшого дослідження стосовно окремих видів діяльності, що дозволить виявити вплив внутрішньоекономічних процесів на економічну безпеку підприємств. Структура суб'єктів ЄДРПОУ, згідно інформації Державного комітету статистики України у 2011 р., представлено на рис. 2.3.

В контексті досліджуваної теми важливо, що найбільшу частку у структурі займають підприємства торгівлі – 24,9%. Зазначене скоріше негативно характеризує структуру національної економіки, адже пріоритетним для її розвитку став не реальний сектор, а посередницька діяльність, яка зокрема сприяє і зростанню частки імпо-

ртних товарів на внутрішньому ринку та спричиняє занепад вітчизняного товаровиробника. Можна зробити висновок, що така структура негативно впливає не лише на рівень національної безпеки, але і опосередковано на економічну безпеку кожного підприємства реального сектору економіки.

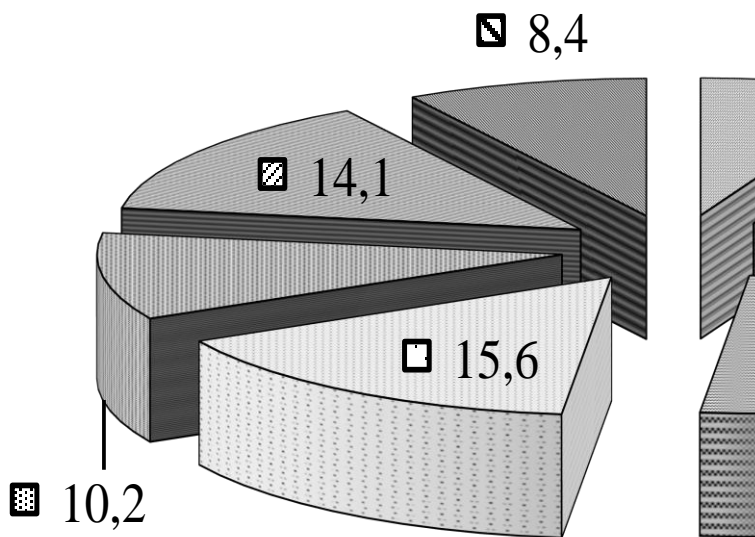


Рис. 2.3. Структура суб'єктів ЄДРПОУ за видами економічної діяльності (на 1 січня 2012 року; відсотків)

В розвинутих країнах світу активно здійснюють кроки щодо формування постіндустріального суспільства, ключова роль в якому належить людині як генератору нових знань. У контексті ж досліджуваної теми, важливо, що саме персонал є найбільш цінним ресурсом підприємства, який виконує найважливішу роль у процесі забезпечення економічної безпеки підприємства в якості суб'єкта безпеки.

Зазначені аргументи доводять необхідність дослідження динаміки кількості найманих працівників як індикатора рівня кадрової безпеки підприємства та можливості забезпечення економічної безпеки на мікрорівні (див. рис. 2.4).



Рис. 2.4. Динаміка кількості найманих працівників

Динаміка кількості найманих працівників у 2007–2011 рр. характеризується суто негативними тенденціями, які визначаються наступними темпами зниження (відносно попереднього року): у 2008-му – (-2,27%), 2009-му – (-7,93%), 2010-му – (-4,76%), 2011-му – (-1,58%), що засвідчує втрату людського капіталу.

Негативні тенденції притаманні як для штатних, так і позаштатних працівників і з точки зору забезпечення безпеки можуть визначатися як чинники, що спричинять виникнення загрози для кадрової безпеки, а відтак і економічної безпеки підприємства.

Наявність негативних тенденцій щодо усієї сукупності найманих працівників визначила необхідність здійснення аналізу структури у розрізі видів економічної діяльності (див. рис. 2.5).

Перш за все зазначимо, що найбільша частка найманих працівників упродовж 2007-2011 рр. була зайнята у промисловості: у 2007-му – 40,4%, 2008-му – 39,5%, 2009-му – 38,7%, 2010-му – 39,1%, 2011-му – 39,2%, хоча і чітко помітна тенденція до її зниження у 2007–2010 рр.

Не менш важливим є факт скорочення частки у 2011 р. у порівнянні із 2007-м, в найбільшій мірі у будівництві – на 2,1 п., сільському та лісовому господарствах й мисливстві на 1,3 п. та промисловості на 1,2 п.

Найбільш суттєве зростання ж було притаманне для торгівлі у розмірі 1,8 п.

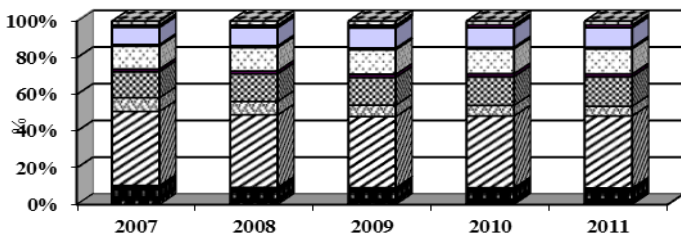


Рис. 2.5. Структура найманих працівників за видами економічної діяльності

Ретельний аналіз абсолютних показників кількості найманих працівників дозволив виявити, що найбільш суттєве зменшення в 2011 р. у порівнянні із 2007 р. було притаманне для промисловості – 666,9 тис. осіб (18,07%) та будівництва – 270,9 тис. осіб (38,89%), що суттєво вплинуло на рівень кадрової безпеки підприємств зазначених видів діяльності.

Беручи до уваги, що найбільша частка працівників зайнята у промисловості (у 2011 р. – 39,2%), то визначимо тенденції стосовно динаміки трудових ресурсів за видами промислової діяльності (рис. 2.6).

Серед видів промислової діяльності найбільша частка найманих працівників зайнята у переробній промисловості, зокрема у 2011 р. – 66,27%, але потрібно звернути увагу на той факт, що ця частка знизилась у порівнянні із 2007 р. на 4,4 п. Іншим важливим моментом є те, що саме стосовно переробної промисловості мало місце найбільше скорочення чисельності працівників в абсолютно-

му виразі на 604,4 тис. осіб, а у відносному – на 23,18%. Серед інших видів промислової діяльності доцільно виділити скорочення кількості працівників у легкій промисловості на 37,3 тис. осіб (25,36%) та машинобудуванні – на 155 тис. осіб (20,3%).

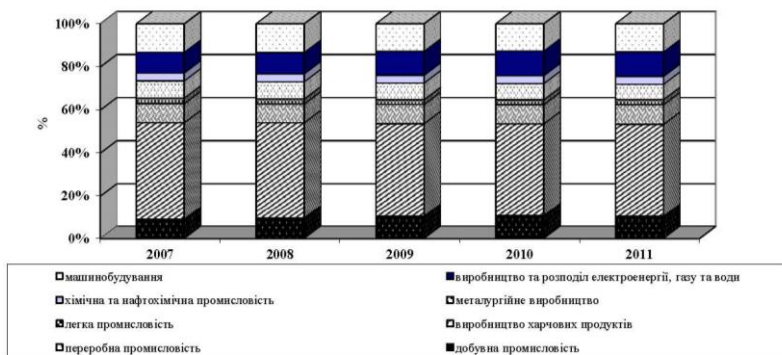


Рис. 2.6. Структура найманих працівників за видами промислової діяльності (вибірково)

Визначені тенденції є підставою стверджувати, що скорочення кількості найманих працівників мало місце як у докризовому, кризовому, так і посткризовому періодах. Внаслідок пріоритетності ефективного використання людського капіталу на сучасному етапі розвитку світової економіки, скорочення працівників є негативним фактом як на мікро, так і макрорівні, оскільки негативно впливає на економічну безпеку на усіх ієрархічних рівнях.

Ефективність використання трудових ресурсів безпосередньо залежить не лише від наявності робочого місця, але і задіяного мотиваційного механізму. В розвинутих країнах світу при високому рівні механізації й автоматизації, найбільш цінною вважається інтелектуальна праця, а система мотивації ґрунтується на необхідності стимулювання саме творчого підходу до вирішення виробничих питань, в т.ч. шляхом матеріального стимулювання через встановлення відповідного рівня оплати праці. Незаперечним є факт, що рівень оплати праці вітчизняних фахівців і закордонних за схожу роботу є суттєво відмінним і не на користь нашої країни. Саме

цим можна пояснити критично високий рівень трудової міграції не лише зорієнтований на заповнення вільних вакансій на закордонних ринках праці у секторі низькооплачуваної фізичної праці, але і стосовно наукових працівників та молоді, яка отримавши освіту та відповідну фахову підготовку на батьківщині, реалізує власний потенціал на користь іноземних держав. Безперечно, що саме такий стан справ на ринку праці негативно впливає на рівень кадрової безпеки підприємств. Для характеристики цього аспекту скористаємося статистичними даними щодо середньомісячної заробітної плати (рис. 2.7).

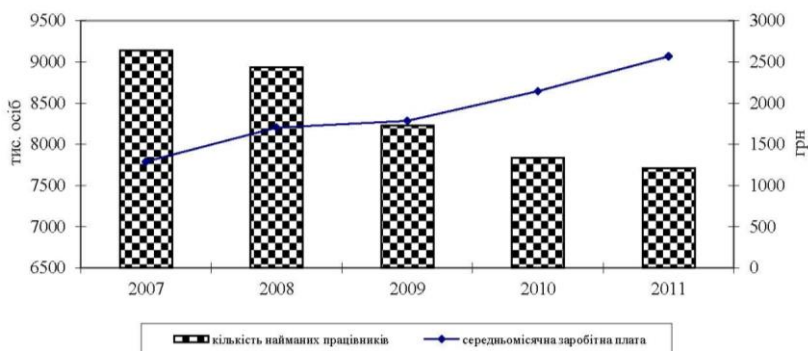


Рис. 2.7. Динаміка кількості та середньомісячної заробітної плати найманих працівників

Якщо порівняти динаміку кількості найманих працівників та середньомісячної заробітної плати, то безперечно, що позитивним і важливим для стимулювання працівників, в т.ч. і до виконання обов'язків в системі економічної безпеки підприємства, є збільшення рівня оплати праці. У 2011 р. у порівнянні із 2007-м величина середньомісячної оплати праці зросла на 1279,8 грн. або майже удвічі. Попри це потрібно взяти до уваги й інші факти, що вплинули на рівень реальної матеріальної винагороди, а це перш за все різке падіння національної валюти – якщо у 2007 р. середньомісячна оплата із врахуванням середньорічного курсу гривні складала 255,04 дол. США, то у 2011-му – 322,28. Зростання лише на 26,36% за п'ять років при фактично високому рівні інфляційних процесів

спричинило знецінення отриманої винагороди за виконану роботу та не стимулювало до продуктивної праці. Окрім зазначеного, необхідно взяти до уваги ще один важливий факт – це відмінність в оплаті праці у різних видах діяльності, оцінку якому можна дати на основі статистичних даних, які в графічному вигляді представлені на рис. 2.8.

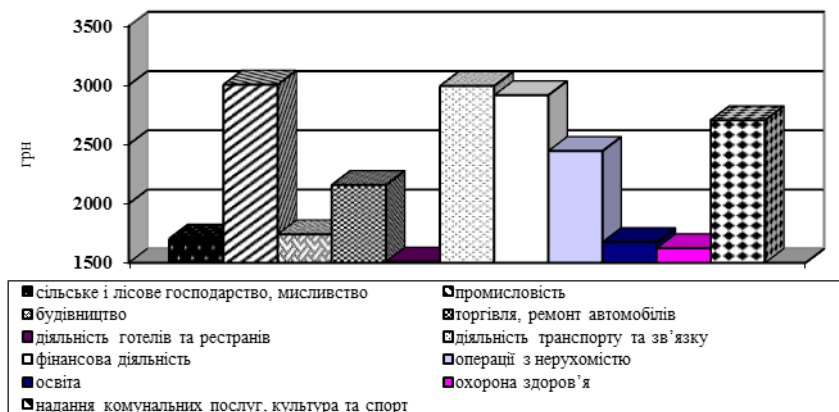


Рис. 2.8. Середньомісячна заробітна плата найманих працівників за видами економічної діяльності у 2011 р.

Якщо попередньо нами були висловлені міркування про недостатньо високий рівень оплати праці, що не сприяє якісному виконанню обов'язків найманими працівниками, зокрема і щодо забезпечення необхідного для існування та розвитку рівня економічної безпеки підприємства, то оцінка середньомісячної заробітної плати у розрізі видів економічної діяльності не лише переконує у вірності зроблених припущень, але дозволяє зробити певні уточнення. За рівнем середньомісячної заробітної плати у 2011 р. лідерами були промислові підприємства – 3003,52 грн., транспорту та зв'язку – 2992,54 грн. та фінансові установи – 2914,69 грн. Більш важливо, що у порівнянні із цими лідерами, майже удвічі нижчою була оплата праці стосовно діяльності готелів та ресторанів – 1510,72 грн., охорона здоров'я та надання соціальної допомоги – 1623,84 грн. та освіти – 1676,07 грн. Суттєва різниця в оплаті праці

негативно впливає на розвиток того чи іншого підприємства та безпосередньо на рівень його кадрової безпеки.

Оскільки нами визначено, що саме в промисловості був найвищий рівень оплати праці, то здійснимо більш ретельний аналіз цього важливого аспекту для забезпечення економічної безпеки кожного підприємства у розрізі видів промислової діяльності (рис. 2.9).

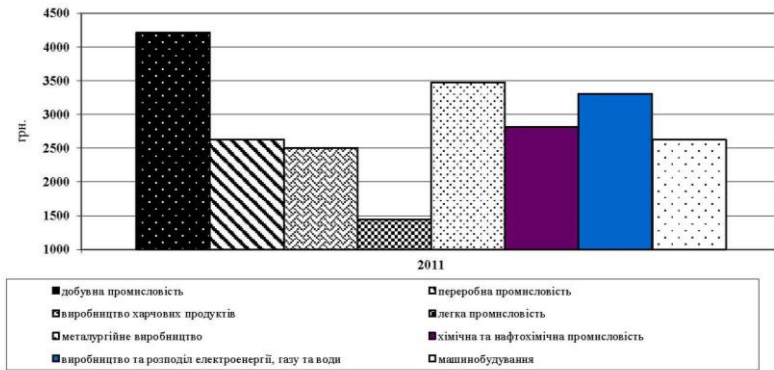


Рис. 2.9. Середньомісячна заробітна плата найманих працівників за видами промислової діяльності у 2011 р. (вибірково)

Отримані результати можна трактувати наступним чином:

- у розвинутих країнах світу, які сьогодні активно стимулюють розвиток високотехнологічних секторів економіки, найвищий рівень оплати праці характерний для машинобудування, зокрема авіаційного та космічного, створення нанотехнологій та розвитку інформаційно-комунікаційних систем;

- абсолютною протилежністю є ситуація, яка склалася сьогодні в нашій країні, адже найвищий рівень оплати праці має місце в добувній промисловості і зокрема – добуванні паливно-енергетичних копалин – 4471,62 грн.;

- таким, що не сприяє інноваційному розвитку і фактично є загрозою для економічної безпеки держави можна вважати той факт, що рівень оплати праці в секторі добування корисних копалин на порядок вищий у порівнянні із машинобудуванням (2626,52 грн.);

– темпи зростання середньомісячної оплати праці в сировинних секторах економіки суттєво вищі у порівнянні з середнім по промисловості та в загальному по економіці, що негативно впливає на процес розвитку та рівень економічної безпеки більшості вітчизняних підприємств.

Поруч із динамікою кількості та ефективністю мотивації найманих працівників про рівень економічної безпеки підприємств свідчать і фінансові результати їх діяльності. На першому етапі розглянемо зміни в обсязі реалізованої продукції та операційних витрат на одиницю реалізованої продукції (рис. 2.10).

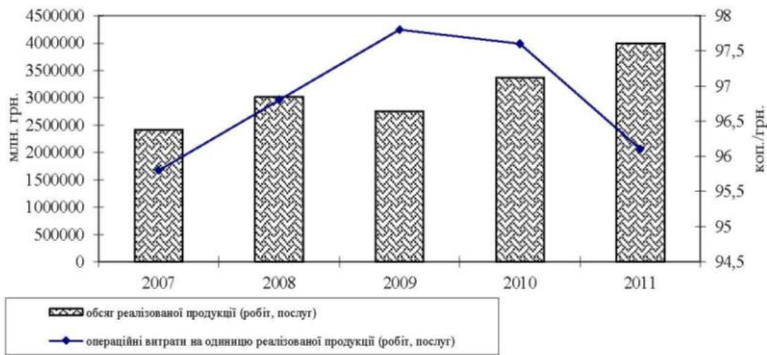


Рис. 2.10. Динаміка обсягу реалізованої продукції (робіт, послуг) та операційних витрат на одиницю реалізованої продукції (робіт, послуг)

Фінансова криза 2008–2009 рр. суттєво вплинула на всі сфери суспільного життя, не оминувши і діяльність підприємств щодо виробництва та реалізації продукції. Саме цим можна пояснити зниження величини реалізації у 2009 р. у порівнянні із 2008-м на 9,05%. Водночас, про поступове відновлення господарської діяльності свідчить приріст реалізованої продукції (відносно попереднього року) у 2010 р. на 22,6% та у 2011-му – на 18,57%. Якщо ж взяти до уваги рівень операційних витрат на одиницю реалізованої продукції, то попередньо зроблені висновки будуть менш оптимістичні. Рівень витрат як 97,8 коп./грн. у 2009 р., так і 96,1 коп./грн. у 2011 р. не можна вважати прийнятним, адже це

свідчить про фактичну відсутність резервів для подальшого зростання. Якщо ж проаналізувати цей показник у розрізі видів економічної діяльності, то фактичною загрозою для фінансової складової економічної безпеки можна вважати рівень операційних витрат для підприємств, які надають комунальні послуги, здійснюють діяльність у сфері культури та спорту: у 2007-му – 102,2 коп. /грн., 2008-му – 105,1 коп. /грн., 2009-му – 128,9 коп. /грн., 2010-му – 122,8 коп. /грн., 2011-му – 126,0 коп. /грн.

Важливість збільшення обсягу реалізованої продукції як передумова зростання рівня економічної безпеки на мікрорівні спонукало до розгляду динаміки цього показника у розрізі видів економічної діяльності (рис. 2.11).

Далекою від такої, що засвідчує пріоритетність інноваційного розвитку національної економіки, можна вважати структуру реалізованої продукції.

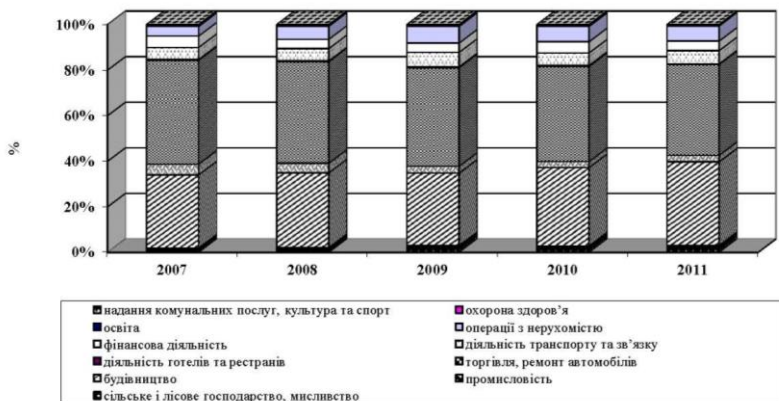


Рис. 2.11. Структура обсягу реалізованої продукції (робіт, послуг) за видами економічної діяльності

Ця теза ґрунтується на тому факті, що найбільш вагому частку у 2011 р. посідала торгівля – 39,9%, коли промисловість – лише 36,7%. Якщо зважити на наявність від’ємного зовнішнього торговельного сальдо та факт засилля внутрішнього ринку офіційно та контрабандою завезеним товаром, то це можна вважати загрозою для економічної безпеки вітчизняного товаровиробника. Попри

це необхідно взяти до уваги і ще один факт, який дещо пом'якшує зроблені нами висновки, а саме наявність позитивної динаміки, так частка торгівлі, хоча і є найбільшою, але поступово зменшується: у 2007-му – 45,6%, 2008-му – 44,6%, 2009-му – 43,3%, 2010-му – 41,8%, 2011-му – 39,9%. У свою чергу, питома вага промисловості в останні три роки поступово зростала: у 2009-му – 31,8%, 2010-му – 34,4%, 2011-му – 36,7%.

Визначена позитивна динаміка стала причиною детального розгляду обсягу реалізації у розрізі промислової продукції за видами економічної діяльності (рис. 2.12).

У структурі обсягу реалізованої промислової продукції найбільша частка припадає на підприємства переробної промисловості у 2007-му – 74,2%, 2008-му – 72,5%, 2009-му – 69,0%, 2010-му – 68,4%, 2011-му – 66,6%.

Вище ми уже наголошували та загрозовували та неприйнятності в добу формування постіндустріального суспільства пріоритетності розвитку в Україні сировинних секторів економіки і в контексті досліджуваного параметра маємо можливість підтвердити наявність даного факту.

Так, поруч із скороченням виробництва на підприємствах переробної промисловості, має місце зростання частки добувної промисловості із 8,6% у 2007 р. до 12,6% у 2011-му та виробництва і розподілу енергоносіїв, газу та води відповідно 17,2% до 20,8%.

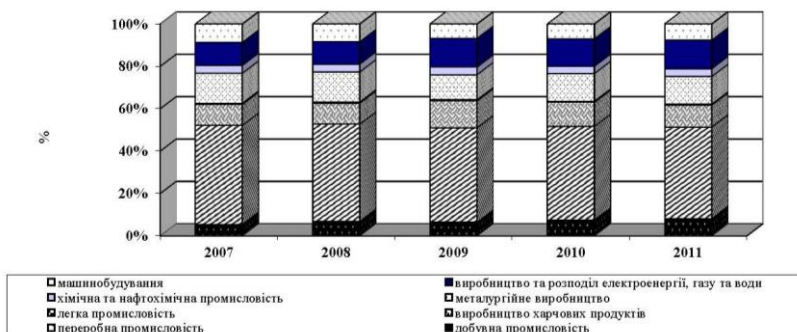


Рис. 2.12. Структура обсягу реалізованої промислової продукції (вибірково)

Дещо негативним можна вважати той факт, що темпи приросту обсягу реалізованої продукції (у 2011 р. в порівнянні із 2007-м) підприємств добувної промисловості (176,06%) і тих, які задіяні у виробництві та розподілі електроенергії, газу та води (128,59%) на порядок вищі за переробної промисловості (69,53%).

Рівень фінансової складової економічної безпеки підприємства значною мірою визначається кінцевим фінансовим результатом господарської діяльності, динаміка якого подана у графічному виразі на рис. 2.13.

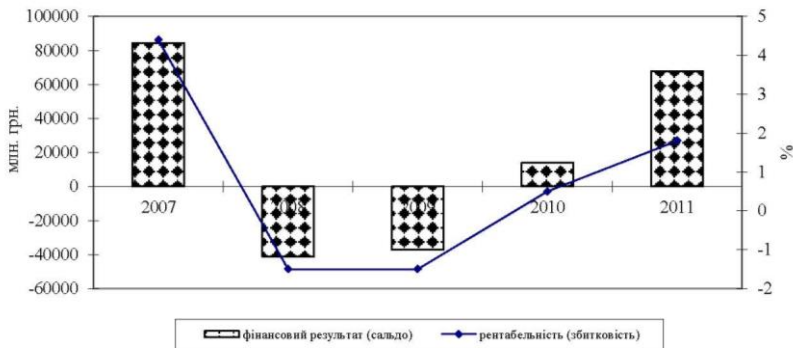


Рис. 2.13. Динаміка чистого прибутку (збитку) та рентабельності усієї діяльності підприємств

Результатом негативного впливу фінансової кризи на діяльність підприємницьких структур став отриманий сукупний збиток у 2008 р. у розмірі 41025,1 млн. грн. та у 2009 р. – 37131,1 млн. грн. У 2010–2011 рр. мало місце значне покращення результатів діяльності, але рівень докризового 2007-го не було досягнуто. У розрізі видів економічної діяльності привертає увагу збитковість будівництва (у 2008-му – 7975,4 млн. грн., 2009-му – 4439,0 млн. грн., 2010-му – 3584,8 млн. грн., 2011-му – 2466,7 млн. грн.), діяльність готелів та ресторанів (у 2007-му – 114,3 млн. грн., 2008-му – 1568,9 млн. грн., 2009-му – 922,5 млн. грн., 2010-му – 633,6 млн. грн., 2011-му – 692,4 млн. грн.), операцій з нерухомістю, оренди і т.д. (у 2008-му – 10928,3 млн. грн., 2009-му – 14219,6 млн. грн., 2010-му – 30676,2 млн. грн., 2011-му – 9325,1 млн. грн.),

охорони здоров'я та подання соціальної допомоги (у 2007-му – 59,1 млн. грн., 2008-му – 187,5 млн. грн., 2009-му – 133,7 млн. грн., 2010-му – 98,8 млн. грн., 2011-му – 215,0 млн. грн.), надання комунальних послуг, діяльність в сфері культури та спорту (у 2007-му – 95,1 млн. грн., 2008-му – 2251,4 млн. грн., 2009-му – 3588,6 млн. грн., 2010-му – 3093,7 млн. грн., 2011-му – 3696,2 млн. грн.). На нашу думку, збитковість у 2010–2011 рр. є важливим індикатором низького рівня фінансової безпеки підприємств певного виду економічної діяльності і потребує удосконалення функціонування їх системи економічної безпеки.

Підтвердження висловленої тези є і визначена нами у графічному виразі динаміка фінансових результатів діяльності підприємств та частки серед них збиткових (рис. 2.14).

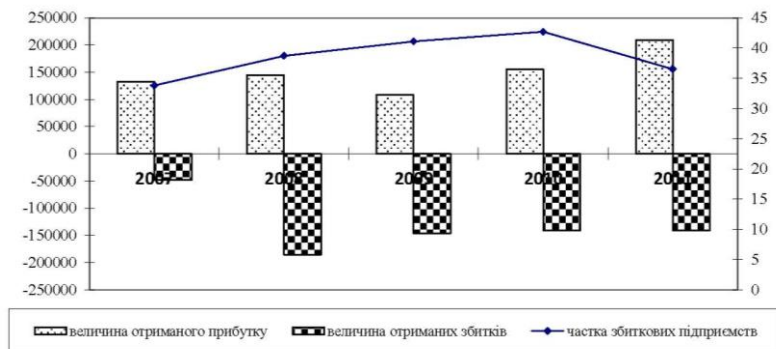


Рис. 2.14. Динаміка фінансового результату та частки збиткових підприємств

На нашу думку, важливим є той факт, що величина сумарних збитків у 2008-2011 рр. як і частка збиткових підприємств суттєво не змінюється, тобто проблема збитковості, а відтак і незадовільного рівня економічної безпеки, має хронічний характер, який потребує особливої уваги на усіх рівнях управління.

Відносним показником ефективності господарської діяльності є рівень рентабельності (збитковості), який як і сальдо фінансового результату підтверджує падіння рівня фінансової безпеки у кризові 2008-2009 рр. та поступове зростання у 2010–2011 рр.

Водночас виявлена збитковість окремих видів діяльності, яка мала місце не лише у кризовому, але в загальному у досліджуваному періоді стимулювала до більш ретельного дослідження рентабельності за видами економічної діяльності (рис. 2.15).

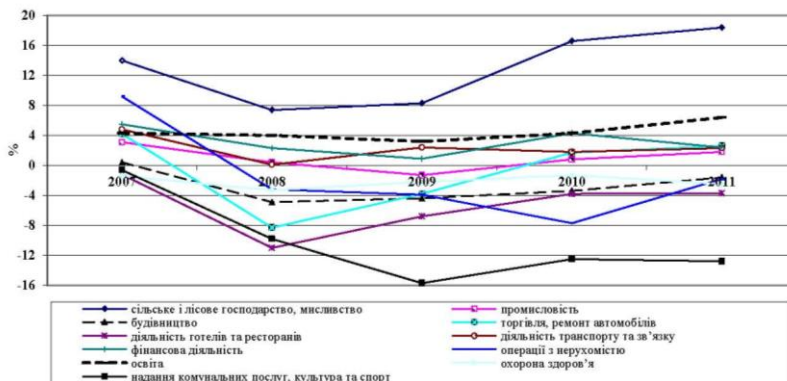


Рис. 2.15. Рентабельність (збитковість) усієї діяльності підприємств за видами економічної діяльності

У розрізі видів економічної діяльності найвищий рівень рентабельності упродовж 2007–2011 рр. мав місце стосовно діяльності підприємств у сфері сільського й лісового господарства та мисливства: у 2007-му – 14,0%, 2008-му – 7,4%, 2009-му – 8,3, 2010-му – 16,6, 2011-му – 18,4. На противагу цьому результату, підприємства, які функціонують в сфері надання комунальних послуг, культури та спорту, для яких були притаманна збитковість: у 2007-му – 0,6%, 2008-му – 9,8%, 2009-му – 15,7%, 2010-му – 12,5%, 2011-му – 12,8%. Безперечно, що рентабельність є визначальним індикатором фінансової безпеки на мікрорівні і в першому випадку вказує на її високий рівень, а в другому – критично низький. Оскільки попередньо ми доволі багато уваги приділили характеристиці рівня економічної безпеки промислових підприємств, то дамо оцінку і цьому індикатору (рис. 2.16).

Найвищий рівень рентабельності господарської діяльності у досліджуваному періоді мали підприємства, які здійснюють добування корисних копалин: у 2007-му – 13,7%, 2008-му – 28,6%,

2009-му – 5,0%, 2010-му – 5,3%, 2011-му – 21,3%. Водночас для більшості підприємств переробної промисловості притаманний низький рівень рентабельності, або ж збитковість. Більш того, якщо загальна рентабельність в 2011 р. досягла рівня 1,8%, то в промисловості в подальшому залишились збитковими суб'єкти господарювання, які здійснюють виробництво коксу та продуктів нафтопереробки (-2,4%), металургійного виробництва (-1,5%), хімічного виробництва (-1,4%) та ін.

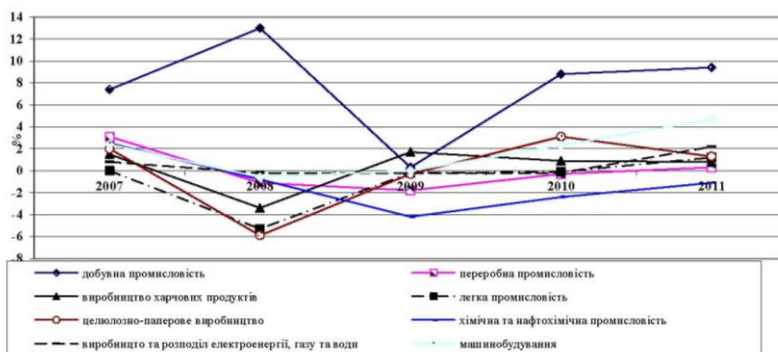


Рис. 2.16. Структура обсягу реалізованої промислової продукції (вибірково)

Проведений аналіз дозволив охарактеризувати тенденції розвитку та визначити окремі параметри рівня економічної безпеки вітчизняних підприємств упродовж 2007–2011 рр. – періоду, який мав ознаки «докризового» (2007 р.), «кризового» (2008–2009 рр.), «посткризового» (2010–2011 рр.). Кожен із визначених періодів суттєво вплинув на рівень економічної безпеки суб'єктів господарювання, дозволив виявити недоліки в системі їх економічної безпеки, що повинно стати базою для подальшого наукового пошуку та удосконалення.

Отримані результати будуть нами використані в наступному розділі для формування переліку ключових загроз, ідентифікація, визначення та ієрархічне впорядкування яких дозволить розробити нові методологічні підходи до управління економічною безпекою на мікрорівні.

2.2. Визначення та ідентифікація ключових загроз економічної безпеки підприємства в Україні

Спираючись на отримані результати дослідження тенденцій розвитку та оцінки рівня економічної безпеки вітчизняних підприємств, висвітлені в попередньому підрозділі, можна стверджувати, що упродовж останніх двох десятиків років в Україні не була створена ефективна високоорганізована система бізнесу, яка б у повній мірі була інтегрована в систему національної безпеки, відповідала міжнародним стандартам і уможливлювала досягнення інтересів кожного суб'єкта підприємницької діяльності. Першопричини виникнення та існування цієї складної проблеми потрібно шукати як на макро-, так і мікрорівні. Сьогодні можна вважати державну політику у сфері організації безпеки господарюючих суб'єктів слабкою, чітко невизначеною, без належно впорядкованого законодавчого поля та із пасивною участю та підтримкою інститутів громадського суспільства. Поруч із цим і значна частина керівників підприємств не вважають безпеку фундаментальною основою для розвитку бізнесу, не приділяючи їй належної уваги, виділяючи на забезпечення мізерні кошти. У цьому контексті як справедливо зауважує В. Щербина, «ситуація в економіці України, що склалася останніми роками, характеризується істотним зниженням безпеки підприємств. Це викликано труднощами тривалого перехідного періоду до системи ринкового господарства та політичною нестабільністю в суспільстві» [26].

На нашу точку зору, враховуючи ту обставину, що сьогодні основою економіки України є недержавний підприємницький сектор, забезпечення необхідного рівня економічної безпеки кожного суб'єкта господарювання є пріоритетним завданням не лише на мікро-, але і на державному рівні, що і повинно стимулювати удосконалення наявного та розроблення нового методологічного забезпечення гарантування економічної безпеки підприємства.

Важливою умовою виконання цього завдання є не лише характеристика рівня економічної безпеки підприємств, але й визначення та ідентифікація ключових загроз, протидія яким формує основу управління економічною безпекою суб'єктів господарювання.

Використовуючи дані Державного комітету статистики України та представлені вище результати проведеної оцінки рівня

економічної безпеки, нами визначена наступна сукупність ключових загроз, суть яких охарактеризовано нижче.

Рівень економічної безпеки будь-якого підприємства у значній мірі залежить від інтенсивності й сприятливості впливу зовнішнього середовища, тобто від умов ведення бізнесу, які в т.ч. створює держава.

Прикро, але сьогодні у світовому рейтингу Doing Business Україна посідає 145 місце з-поміж 183 країн, відчутно поступаючись за критерієм сприятливості ведення бізнесу всім країнам Центрально-Східної Європи (рис. 2.17).

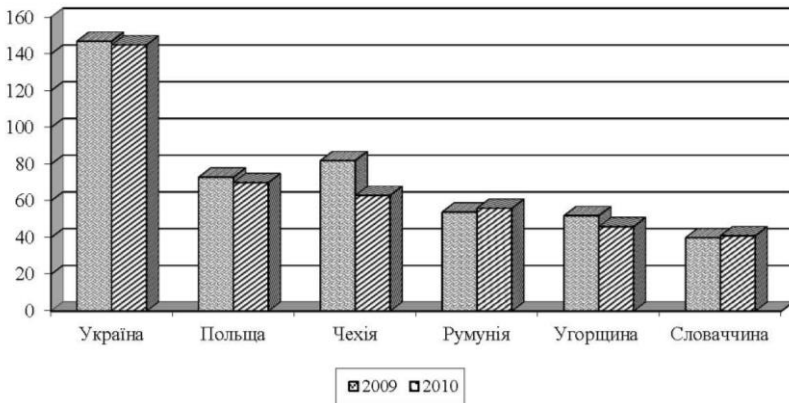


Рис. 2.17. Позиції України та країн ЦСЄ у рейтингу умов ведення бізнесу в 2010 р. [29]

На нашу думку, попри незадовільно низьке місце, яке посідає наша держава стосовно цього важливого параметру, для удосконалення методичного забезпечення гарантування економічної безпеки підприємства доцільно ретельно розглянути та охарактеризувати вплив найбільш суттєвих чинників на формування вітчизняного бізнес-середовища, до числа яких необхідно віднести:

- високий рівень реальної інфляції, значний дефіцит бюджету, негативне торговельне сальдо, залежність від кон'юнктури товарів на світових ринках та низька купівельна спроможність населення, що у сукупності створюють несприятливу ситуацію для розвитку бізнесу;

- відсутність єдиної довгострокової стратегії розвитку та структурної перебудови національної економіки, яка б відповідала сучасним пріоритетам та уможлиблювала зайняття прийнятної конкурентної позиції у світовому економічному просторі;
- непрогнозована зміна та недосконалість нормативно-правового забезпечення процесу функціонування суб'єктів господарювання;
- низька ефективність застосування інструментів державного регулювання економічних процесів;
- безвідповідальність державних чинників за результати реалізації реформ;
- відсутність ефективної системи контролю за забезпеченням виконання норм чинного законодавства;
- незавершеність ринково спрямованих інституційних перетворень і нерозвиненість ринкової інфраструктури;
- складність та нераціональність регуляторної системи, що виражається в обтяжливості дозвільних процедур, надмірній кількості документів, що подаються для одержання дозволів, недосконалості процедур нагляду і контролю та припинення господарської діяльності тощо). Кожен етап підприємницької діяльності від реєстрації підприємства й укладання комерційних угод до ліквідації супроводжується значно більшими часовими витратами (у 2–4 рази) порівняно з розвиненими країнами та країнами-сусідами. Майже за кожним показником легкості ведення бізнесу в Україні кількість процедур, необхідних для цього, перевищує показники розвинених країн і країн-сусідів у 2-3 рази. Саме цим пояснюється значне погіршення значень показників із реєстрації прав власності (з 160 до 164), ліквідації підприємств (з 145 до 150), а також стійкості рейтингу міжнародної торгівлі (139), підтримки виконання контрактів (43) і рівня оподаткування (181) [29];
- незахищеність прав власності. Зазначене ґрунтується на результатах оцінки цього критерію міжнародними аналітичними організаціями. Так, за оцінками Світового економічного форуму у 2009–2010 рр. за рівнем захисту прав власності, включаючи фінансові активи, Україна посідала 135 місце з-поміж 139 країн світу [32], поступаючись всім країнам Центрально-Східної Європи, зокрема за такими критеріями, як незалежність судів, довіра населення до судів, політична стабільність, корупція, захист права власності, захист прав інтелектуальної власності, авторських прав;

- неприпустимо високий рівень корупції, вибіркове виконання норм законодавства, зловживання та протиправні дії чиновників різного рангу. Якщо ж знов звернутися до оцінки, яку дають цьому чиннику закордонні аналітики, то Україна знаходиться на 134 позиції Індексу сприйняття корупції поряд із такими країнами, як Азербайджан, Бангладеш, Гондурас, Нігерія, Філіппіни, Сьєра Леоне та Зімбабве [28];

- надмірне втручання в роботу підприємств державних контролюючих, регулюючих та правоохоронних органів. Як зазначає Н. Тумар, «з органами МВС, СБ України, податковою адміністрацією і прокуратурою нині українські підприємці пов'язують близько 50% усіх проблем по лінії економічної безпеки» [19]. При цьому, як зазначає автор, практика свідчить, що названі державні органи мають можливість і неупереджено (в межах чинного законодавства) втручатися в роботу підприємств у разі порушення ними правових норм.

Усі перелічені вище чинники негативно впливають на процес функціонування підприємницьких структур та рівень їх економічної безпеки, формуючи несприятливий бізнес-клімат, який стримує розвиток перш за все середнього та малого підприємництва, який відіграє важливу соціально-економічну функцію забезпечення громадян країни робочими місцями та поглинання надлишків робочої сили, що вивільняється внаслідок структурних змін в економіці. Розвиток малого й середнього підприємництва – важливий індикатор ефективності ринкових перетворень і передумов прогресивних структурних зрушень у трансформаційних економіках.

Результати впливу перелічених чинників частково нами були визначені у попередньому підрозділі, тому підкреслимо лише окремі ключові аспекти стосовно ідентифікованої загрози для економічної безпеки підприємств:

- у сукупній пропозиції на внутрішньому ринку зберігається тенденція постійного зниження питомої ваги товарів вітчизняного виробництва, особливо товарів кінцевого споживання. Зокрема, у структурі оптового товарообороту питома вага продажу товарів вітчизняного виробництва зменшилася із 70% у 2005 р. до 63,6% у 2010 р., у структурі роздрібного товарообороту – відповідно із 70,5 до 64,3%;

– особливо стрімко зменшується частка вітчизняної непродовольчої продукції, у 2010 р. вона складала 61% в обсязі оптової торгівлі та 50% в обсязі роздрібного товарообороту. За деякими групами товарів легкої промисловості, аудіо- та відеообладнанням, комп'ютерною та обчислювальною технікою Україна забезпечує лише 4–6% потреб за рахунок власного виробництва. Водночас питома вага вітчизняних продовольчих товарів складає 75,1% у структурі оптової та 88,2% у структурі роздрібної торгівлі, маючи тенденцію до поступового зниження;

– упродовж 2007-2011 рр. відбулося скорочення кількості об'єктів інфраструктури підтримки малого підприємництва: бізнес-центрів (у 2010 р. порівняно з 2008 р. їх кількість зменшилася на 27 одиниць, або 5,8%), лізингових компаній (на 30 од., або 3,8%), фондів підтримки підприємництва (на 34 од., або 12,2%), кредитних спілок (на 162 од., або 19,7%), страхових організацій (на 46 од., або 9,1%), інформаційно-консультативних установ (на 65 од., або 2%), аудиторських компаній (на 62 од., або 4%);

Усе вище подане засвідчує суттєвий вплив незадовільних умов ведення бізнесу на економічну безпеку вітчизняних підприємств і дозволяє ідентифікувати їх як першу загрозу.

Вітчизняні та закордонні фахівці дотримуються думки, що Українська економіка характеризується надто високим рівнем енергоємності ВВП. Цей показник в Україні, за оцінками компанії Enerdata, є одним із найвищих серед країн світу, зокрема у 3,8 разу вищим ніж у країнах ЄС-27, у 3,2 разу – ніж у сусідній Польщі, в 1,4 разу – ніж у Росії (рис. 2.18).

Із врахуванням цих обставин, зростання світових цін на нафту при збереженні тенденцій останніх років (2008–2011 рр.) до збільшення обсягів імпорту нафти створює умови для низки негативних макроекономічних ефектів для України.

Підставою для такого твердження є те, що зростання зовнішніх цін на нафту спричинить їх збільшення на внутрішньому ринку та пропорційне збільшення цін на продукти нафтопереробки. За умов відсутності дієвого регулювання цін на продукти нафтопереробки, у певних галузях, зокрема у транспорті, сільському господарстві, харчовій промисловості та будівництві, які є найбільш залежними від цін на нафтопродукти, зросте собівартість виробництва продукції.

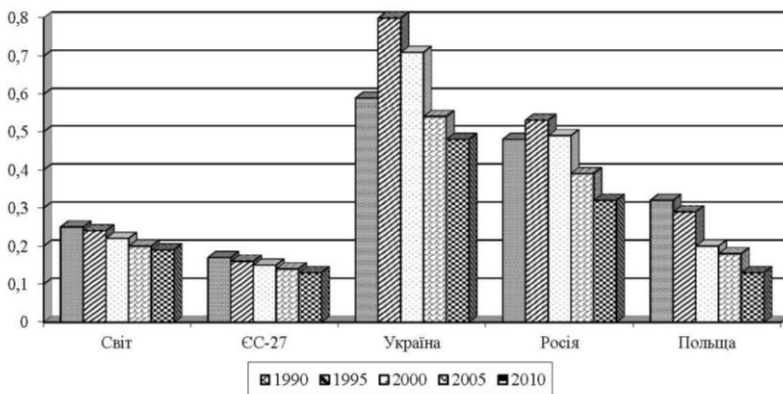


Рис. 2.18. Енергоємність ВВП, кілограмів нафтового еквіваленту на 1 тис. євро [34]

З метою збереження рівня рентабельності, підприємства з вагомою часткою нафти та нафтопродуктів у структурі витрат будуть вимушені підвищувати відпускні ціни, а внаслідок дії міжгалузевих зв'язків це може призвести до наступних негативних макроекономічних ефектів та ризиків.

Коливання цін на чорні метали у порівнянні із нафтою має неоднозначний вплив на економічну безпеку вітчизняних підприємств. При зростанні цін на цей товар буде мати покращення стану платіжного балансу та формування потенційних можливостей для зростання виробництва та доданої вартості у металургії. Це, у свою чергу, створить умови і сприятиме збільшенню податкових надходжень до бюджету, оплати праці та прибутковості галузі, нагромадження коштів на інвестиційні цілі.

Разом з тим слід очікувати певні негативні ефекти, які виникнуть внаслідок міжгалузевих зв'язків. Зростання зовнішніх цін на продукцію металургійної галузі спричинить їх збільшення на внутрішньому ринку. Як наслідок, у певних галузях, зокрема у машинобудуванні та будівництві, які є найбільшими споживачами металургійної продукції, зросте собівартість виробництва продукції.

За таких умов або підприємства будуть вимушені підвищувати відпускні ціни, або їх додана вартість зменшиться, що може

привести до зменшення оплати праці, надходжень до бюджету або згорання інвестиційної активності на цих підприємствах. Підвищення цін на підприємствах машинобудування та будівництва спричинить зростання індексу цін інвестицій в основний капітал, що гальмуватиме виконання інвестиційних планів на вітчизняних підприємствах.

Підсумовуючи, можна стверджувати, що явною загрозою для економічної безпеки вітчизняних підприємств є висока енергомісткість та матеріаломісткість виробництва. Це обумовлено низьким технологічним рівнем виробництва, високими цінами на сировину, матеріали, паливно-енергетичні ресурси, відсутністю ефективних заходів із ресурсозбереження, що частково спричинено пасивністю держави у питаннях стимулювання інноваційних процесів, залучення до вітчизняного виробництва передових енергозберігаючих технологій тощо.

В суспільній свідомості сформоване трактування тіньової економіки як суто негативного явища. Водночас, потрібно визнати, що тіньова складова в умовах трансформаційної економіки є абсолютно очевидним фактом, а її нелегальність обумовлена слабкістю соціально-економічних інститутів. Збільшенню тіньової економіки сприяє скорочення виробництва в основних видах економічної діяльності, низька частка оплати праці у випуску та фонду оплати праці у ВВП, збереження високого рівня бідності працюючого населення, високий рівень оподаткування легального бізнесу, у тому числі внесків до державних соціальних фондів, низький рівень дотримання законів і, як наслідок, втрата довіри до правоохоронної й судової систем держави.

Потрібно взяти до уваги і той факт, що тіньова економіка притаманна не лише для країн, які перебувають на шляху формування ринкової економіки, але і для лідерів світового економічного простору (рис. 2.19), хоча рівень, безперечно, є суттєво відмінним.

Важливо, що частка тіньової економіки в країнах ОЕСР як у докризовому, кризовому та посткризовому періодах мала тенденцію до зниження, коли в Україні – до негативного зростання у 2008–2009 рр., що можна трактувати як реакцію бізнесу на кризові явища в економіці та намаганням продовжити своє існування шляхом переходу із легального становища у тінь.

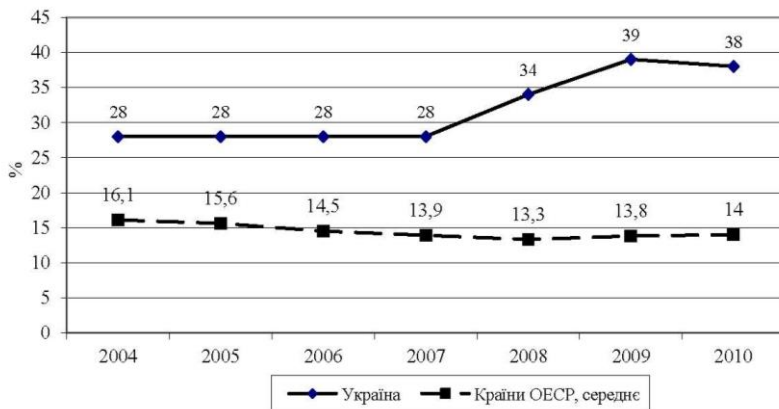


Рис. 2.19. Обсяг тіньової економіки в Україні, % ВВП

*Джерело: Україна – Міністерство економічного розвитку і торгівлі, ОЕСР – оцінки Ф. Шнайдера [33]

При цьому дані, отримані різними методами розрахунку рівня тіньової економіки, яскраво відтворюють поведінку різних агентів на різних етапах економічного циклу (рис. 2.20).

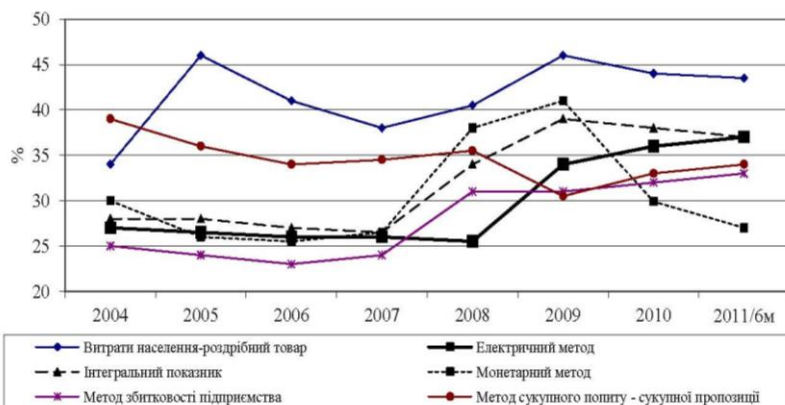


Рис. 2.20. Рівень тіньової економіки України, обчислений за різними методами, % ВВП [23]

Аналітичні оцінки, отримані на основі модельних розрахунків [22], свідчать, що до найістотніших чинників тінізації національної економіки належать наступні.

1. Суперечливість та дублювання законодавчої та нормативно-розпорядчої бази в окремих секторах, що відтворює низький рівень структурних компонентів індексу економічної свободи та зростання тінізації.

2. Недієвість організаційно-інституціональних механізмів антикорупційного законодавства. За даними міжнародної неурядової організації «Transparency International», Індекс сприйняття корупції в Україні у 2010 р. становив 2,4 пункту (у найменш корумпованих країнах Індекс сприйняття корупції становить 9,0–10, у країнах з високим рівнем корупції – менше 3,0.) , що відповідає 134 місцю у рейтингу серед 178 країн світу.

3. Недосконалість судової та правоохоронної системи, що позначається на низьких оцінках експертів Світового економічного форуму незалежності судової влади та довіри до правоохоронних органів [32].

4. Неєфективне адміністрування податків, що підтверджують рейтингові оцінки [29] щодо ефективності оподаткування. За оцінками експертів Світового банку, після запровадження Податкового кодексу система адміністрування податків залишається складною через існування низки податкових пільг.

5. Високий рівень злочинності. Налагоджені кримінальні зв'язки формують умови для поширення економічної злочинності та іншої протиправної діяльності. За експертними оцінками [30], організована злочинність та торгівля незаконними товарами формують близько третини світових тіньових фінансових потоків. Загальна кількість зареєстрованих в Україні злочинів у 2010 р. збільшилася на 14,9%, засуджених – на 15,2%, кількість осіб, притягнутих до адміністративної відповідальності, – на 6,9%.

6. Відсутність історичної практики дотримання норм та моральних стандартів законослухняної поведінки під час провадження господарської діяльності та сплати податків у суб'єктів господарювання та громадян [6].

Підсумовуючи вище викладене, потрібно підкреслити, що критично високий рівень тіньової економіки негативно впливає на економічну безпеку вітчизняних підприємств в т.ч. через нерівність

умов в яких функціонує легальний бізнес та тіньовий сектор економіки, негативний вплив на конкурентне середовище, деградацію системи державного управління та ринкових інституцій, а відтак її потрібно ідентифікувати як загрозу.

Значна частина вітчизняних підприємств залишаються незадоволеними кількістю податків і порядком їх розрахунків, що не стимулює до активного розвитку та негативно впливає на рівень економічної безпеки. Так, за індексом сприятливості податкової системи, який розраховується на основі показників кількості платежів, часу, необхідного для сплати податків і загального розміру податків, Україна посідає 181 місце з-поміж 183 країн світу [31]. Система оподаткування характеризується надмірною кількістю процедур (135), що в 10 разів більше, ніж у розвинених країнах, і в 3,5 разу – ніж у країнах-сусідах.

Поруч із непомірним фіскальним навантаженням на діяльність підприємств, в Україні має місце необґрунтована диференціація податкової політики, яка провокує технологічну деградацію виробничого потенціалу. Загалом високе фіскальне навантаження на промисловість та низьке – на фінансову діяльність і торгівлю впливає на міжгалузевий розподіл економічних ресурсів, насамперед капіталу, призводить до вимивання коштів із промислового виробництва на користь торговельно-фінансової сфери. Таким чином, промисловість, особливо її високо технологічний сегмент, позбавляються власних фінансових ресурсів, чим підриваються можливості їх розширеного відтворення [27]. У свою чергу серед галузей промисловості найбільше податкове навантаження покладено на харчову промисловість (у 2009 р. вона забезпечила 31% усіх надходжень від сплати податків на прибуток та імпорт (у 2008 р. цей показник складав 21,3%), тоді як у вартісній структурі випуску частка галузі складала за підсумком року 8,8%. Машинобудування, формуючи 4,8% випуску продукції, сплатило 9,9% податків.

Водночас найбільша галузь виробничої сфери – металургійне виробництво (7,9% у вартісній структурі випуску) сплачувала лише 1,2% від загального обсягу податкових надходжень.

Недосконалість податкової системи, яка проявляється в надмірному фіскальному тиску на бізнес та хибність диференціації податкового навантаження на реальний сектор економіки, який

зокрема гальмує розвиток високотехнологічного сектору економіки, на нашу думку, потрібно ідентифікувати як загрозу економічній безпеці підприємств.

Динаміку фінансових результатів діяльності вітчизняних підприємств нами було ретельно розглянуто у попередньому підрозділі, але їх вагомий вплив на рівень економічної безпеки змушує коротко повернутися до цього аспекту.

Упродовж 2007–2011 рр. найвищий рівень рентабельності операційної діяльності з поміж видів економічної діяльності мали сільське та лісове господарство й мисливство (19,0% у 2007 р. і 23,6% у 2011 р.), а найнижчий – надання комунальних послуг, діяльність у сфері культури та спорту (відповідно 2,6% та (-13,8%)). Динаміка загального рівня цього показника для промисловості характеризувалася зниженням у 2007-2009 рр.: у 2007-му – 5,8%, 2008-му – 4,9%, 2009-му – 1,8% та зростанням у 2010-му до 3,6% та у 2011-му – 4,7%.

Серед видів промислової діяльності найвищий рівень мала добувна галузь (11,4% у 2007 р. і 17,3% у 2011 р.). Водночас низький рівень рентабельності мали машинобудування (відповідно 4,3% і 8,6%), легка промисловість (0,7% та 4,0%), харчова промисловість (4,7% та 4,2%). Окремо потрібно ще раз підкреслити, що у 2010 р. – 42,7% та у 2011-му – 36,5% підприємств були збитковими.

Беручи до уваги сформовані та опрацьовані аналітичні матеріали, вважаємо за доцільне визначити як загрозу для економічної безпеки вітчизняних підприємств недостатньо високу ефективність їх господарської діяльності, що знаходить відображення у низькому рівні рентабельності та критично високій частці збиткових суб'єктів господарювання.

Важливим чинником, який впливає на рівень техніко-технологічної безпеки, а відтак і економічної безпеки в загальному є стан основних засобів, ступінь зношеності яких невпинно зростає: із 43,7% у 2000 р. до 60% у 2009 р. (рис. 2.21). Особливо різко збільшилося значення цього показника у 2008 р. – на 8,6 п. Найскладнішою є ситуація зі станом основних засобів у транспорті та зв'язку (у 2009 р. ступінь зношеності складав 83,9%), у переробній промисловості (64,9%), виробництві й розподіленні електроенергії, газу та води (62,2%).

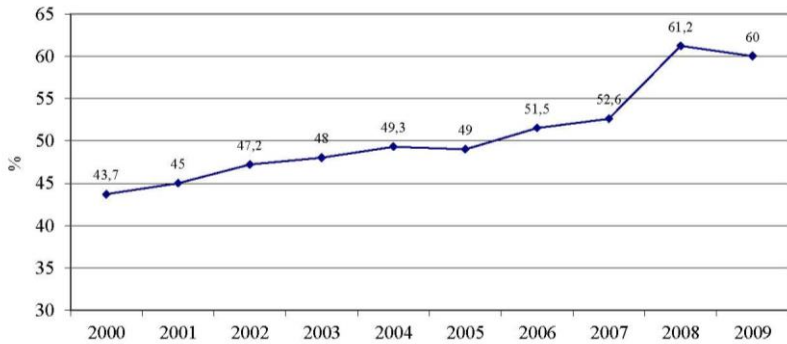


Рис. 2.21. Ступінь зношеності основних засобів в Україні в 2000–2009 рр.

Беручи до уваги ці офіційні статистичні дані, на нашу думку, потрібно зважити і на той факт, що мова йде виключно про знос визначений згідно фінансової звітності. Водночас не враховується моральний знос основних засобів і здатність підприємства на їх основі виготовляти конкурентоспроможну продукцію. З однієї сторони, узагальнити та охарактеризувати цей аспект є неможливим, а з іншої – проблема оновлення основних фондів нами буде розглядатися згодом в контексті оцінки інвестиційно-інноваційної діяльності підприємств.

В контексті досліджуваного аспекту забезпечення економічної безпеки підприємств, на нашу думку, доцільно приділити увагу проблемі нарахування і використання амортизації. Зазначене зумовлено тим фактом, що у більшості розвинених країн амортизація є одним із основних важелів регулювання розширеного відтворення основних фондів, оскільки у загальних інвестиціях на неї припадає 65–70%, а тому вона є вагомим чинником економічного зростання, а відтак і суттєво впливає на рівень економічної безпеки підприємства. Так, у США питома вага амортизаційних відрахувань за 1950–2008 рр. збільшилася з 18 до 74,2%, у результаті чого ефективна податкова ставка з податку на прибуток у корпоративному секторі знизилася за цей період із 34 до 15%. Активне використання прискореної амортизації дозволило США посісти передові позиції в технічному, технологічному, інформаційному й багатьох інших

відношеннях [14]. У свою чергу, в Україні за 9 місяців 2010 р. частка амортизації у структурі операційних витрат складала 3,2%, у т. ч. у промисловості – 4,0%, а частка в загальному обсязі інвестицій – 60,9%. Необхідно наголосити на тому факті, що в нашій країні відсутній дієвий контроль за витрачанням амортизаційних коштів, що дозволяє підприємствам витрачати їх на цілі, не пов'язані з інвестиціями в основні фонди.

Розглянуте дозволяє дійти висновку, що загрозою для економічної безпеки підприємства є високий рівень зносу основних фондів, технологічна відсталість та низька ефективність використання амортизації.

У попередньому підрозділі нами було приділено достатньо багато уваги проблемі забезпечення кадрової безпеки підприємств через характеристику динаміки кількості найманих працівників та ефективності мотивації їх праці. Стосовно ж поставленого завдання щодо ідентифікації загроз для економічної безпеки, то до зроблених вище висновків, доцільно додати, що відповідно до аналітичних даних американських експертів близько 80% збитків матеріальним активам компаній завдає їх власний персонал. Тільки 20% спроб несанкціонованого проникнення в закриті мережі здійснюється ззовні, а решта 80% випадків спровоковані за участі персоналу компаній.

Динаміка вартості зловживань, здійснених посадовими особами та працівниками американських компаній у 1980 р., становила 50 млрд дол. США, у 1990 р. – 250 млрд дол. США, у 1998 р. – 400 млрд дол. США, у 2002 р. – 600 млрд дол. США.

Аналогічна інформація щодо вітчизняних суб'єктів господарювання відсутня, але потрібно зважити, що низький рівень оплати праці та негативні тенденції щодо скорочення кількості найманих працівників не сприяють якісному виконанню обов'язків, у т.ч. стосовно забезпечення економічної безпеки. Окремо потрібно наголосити на неприпустимо низькому рівні менеджменту на вітчизняних підприємствах, який і є однією із причин незадовільних результатів діяльності та низького рівня економічної безпеки. Звідси, на нашу точку зору, одну із загроз для економічної безпеки підприємств доцільно визначити як недостатньо високий якісний рівень, вмотивованість та виконання функції в системі економічної безпеки персоналом підприємства.

За орієнтовними розрахунками аналітиків, щорічний ринок приватизації та поглинань в Україні становить 3 млрд дол. США, з яких 60–70% є недружніми поглинаннями (близько 2 млрд дол. США). Такі обсяги матеріальних ресурсів самі по собі є стимулом для схильних до правопорушень членів суспільства зайнятися такою протиправною діяльністю. Успішність рейдерських атак обумовлюється низкою чинників:

- недосконалістю українського законодавства, особливо в тій його частині, що встановлює відповідальність за рейдерство. Наприклад, за рейдерські атаки протягом 2005-2006 рр. жодна особа або компанія, що брали участь у підготовці чи здійсненні незаконного поглинання, не були притягнуті навіть до адміністративної відповідальності, не кажучи вже про кримінальну;

- фактами корумпованості представників судової влади, контролюючих і правоохоронних органів;

- високою «рентабельністю» рейдерства – нараховується сотнями відсотків прибутку, а рівень ефективності рейдерських атак складає 90%. Це означає, що лише одній із десяти жертв рейдерів вдається захистити себе та відбити рейдерську атаку;

- слабкою мобілізованістю державних органів і громадськості на вирішення цієї проблеми, недостатнім усвідомленням у суспільстві шкоди, що завдається рейдерством, національним інтересам України та її міжнародному іміджу.

Для досягнення своїх цілей поряд із використанням вказаних чинників рейдери застосовують прийоми недобросовісної конкуренції, які зазвичай зводяться до трьох основних напрямів впливу:

- до неправомірного використання ділової репутації суб'єкта господарювання;

- до створення перешкод господарській діяльності та досягнення неправомірних переваг у конкуренції;

- до неправомірного збирання, розкриття та використання комерційної таємниці [11].

За даними експертів, на сьогодні кількість рейдерських атак в Україні нараховує понад 9000 випадків, а число рейдерських груп досягає 30–50. Про масштаб цього явища свідчить той факт, що об'єктами атак з боку рейдерів уже стали великі компанії, а також підприємства, де утримувачем контрольного пакета є держава.

За масштабами здійснення та наслідками впливу в Україні рейдерські захоплення та протиправна діяльність кримінальних структур створюють реальну загрозу не лише окремим підприємствам, а й національній безпеці України.

В попередньому розділі нами було доволі ретельно розглянуто динаміку фінансових результатів діяльності підприємств і зроблені висновки про галузеву диспропорцію національної економіки, що суперечить світовим тенденціям, але в процесі ідентифікації та обґрунтування чергової загрози доцільно наголосити на окремих ключових аспектах. Так, фінансово-економічна криза не тільки призвела до драматичних змін в обсягах промислового виробництва, але й відобразилася на його структурі. Ці зміни обумовлені дією об'єктивних зовнішніх чинників і внутрішніх суперечностей, що накопичилися в економіці [4]. Зокрема, спад обсягів виробництва у промисловості складав 5,4% у 2008 р. і 21,9% у 2009 р. При цьому найбільших втрат зазнала переробна промисловість, скорочення виробництва складало відповідно 6 та 26,5%. Найбільшого спаду зазнали галузі, орієнтовані на виробництво продукції виробничого та інвестиційного призначення: машинобудування, виробництво неметалевої мінеральної продукції, металургійне виробництво й виробництво готових металевих виробів, хімічна промисловість. Найбільш глибоким і затяжним виявився спад у машинобудуванні. Ця галузь промисловості, що є основним джерелом інноваційного розвитку й модернізації економіки, зазнала дуже глибокого падіння у 2009 р. – на 44,9%. Провідним джерелом спаду в машинобудуванні стало виробництво транспортних засобів та устаткування, яке скоротилося на понад 60%. Динаміка металургії та хімічної промисловості була майже синхронною із загальною промисловою динамікою, проте через свою вагомість чорна металургія викликала понад третину загального спаду. Внаслідок цього відбулися суттєві зміни у структурі реалізованої промислової продукції. За період кризи різко знизилася питома вага металургійної продукції – з 26,2 до 19,6% і машинобудування – з 14,0 до 10,6%. Водночас суттєво зросла частка харчової промисловості – з 13,1 до 18,9% і виробництва й розподілу електроенергії, газу й води – з 13,0 до 19,0% [4]. Таким чином, фінансово-економічна криза різко прискорила темпи скорочення реального сектору економіки, особливо у сфері матеріального виробництва. Відновлення економічного зростання розпо-

чалось у 2010 р. і тривало у 2011 р. насамперед завдяки зростанню зовнішнього попиту на продукцію експортоорієнтованих галузей, а також відновленню попиту (зростання доходів населення у 2010 р. складало 23,1% порівняно з 2009 р.) на продукцію галузей, орієнтованих на внутрішній ринок. Проте, через стагнацію інвестиційних процесів посткризове відновлення зростання не супроводжувалося якісними змінами у виробництві ВДВ. Отже, підґрунтям цього відновлення не стали модернізація національної економіки й набуття нею сучасного рівня конкурентоспроможності [7].

Особливе занепокоєння викликають тенденції до поглиблення деформацій у структурі промисловості, більш швидкий розвиток її низькотехнологічних галузей із застосуванням переважно застарілих технологій. Наприклад, у провідній галузі української економіки – чорній металургії – частка мартенівської сталі складає близько 45% (у Росії – 20%, у Китаї – 7%), тоді як у розвинених країнах мартенівські печі вже взагалі не використовують. Низькотехнологічні й екологічно небезпечні види промислової діяльності впродовж останніх років залишалися найбільш значущими галузями виробничої сфери.

Відтворення промислового виробництва в період економічного зростання відбувалося за рахунок середньо-низьких технологій без життєво необхідної модернізації виробничого апарату. Близько 58% виробленої продукції припадає на нижчий – третій – технологічний уклад (виробництво будівельних матеріалів, чорну металургію, суднобудування, оброблення металу, легку, деревообробку, целюлозно-паперову промисловість). Водночас в обсязі випуску продукції вищі технологічні уклади – п'ятий і шостий – складають близько 4%, причому шостий – технологічний – уклад, що визначає перспективи високотехнологічного розвитку країни в майбутньому, в нашій країні майже відсутній (менше 0,1%) [24].

Як підсумок вище поданого, можна стверджувати, що динаміка структури української економіки не відповідає загальним закономірностям структурних зрушень, що відбуваються в розвинених економіках світу на сучасному етапі й полягають у зростанні частки високотехнологічних виробництв обробної промисловості, телекомунікаційних, фінансових і бізнесових послуг, а також соціально орієнтованих видів економічної діяльності, випереджальному розвитку наукоємних, високотехнологічних галузей. Натомість

в Україні сформувалася неефективна структура економіки з високою ресурсо- та енергоємністю виробництва, надмірним екстенсивним розвитком добувної промисловості, відсталістю агропромислового сектору, низьким рівнем інноваційного виробництва, відставанням розвитку інфраструктури, відірваністю фінансового сектору від реальної економіки, неефективним функціонуванням секторів, що забезпечують соціальний розвиток.

Аналіз інвестиційних процесів в Україні свідчить про нестійкий характер їх розвитку внаслідок сукупної дії і зовнішніх, і внутрішніх чинників. Зокрема, доволі динамічне зростання обсягів інвестицій в основний капітал у докризовий період (2000–2008 рр.): у 2006 р. 19,0%, у 2007 р. – 29,8% відносно попереднього року, у кризові роки змінилося різким падінням інвестиційної активності та поступовою стабілізацією інвестиційної діяльності у посткризовий період (рис. 2.22).

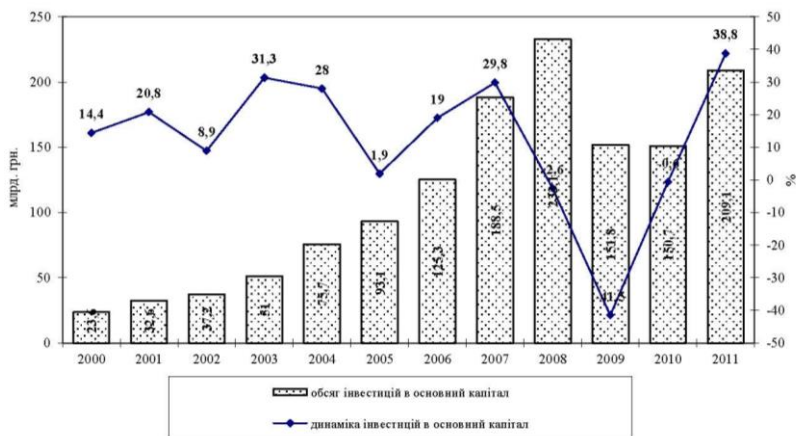


Рис. 2.22. Інвестиції в основний капітал в Україні у 2001–2011 рр.

В докризовому періоді стримуючими чинниками ефективної інвестиційної діяльності були відсутність системної інвестиційної політики, дієвих інституційних засад розвитку інвестиційної діяльності, несприятливий бізнес-клімат, незадовільна ситуація у сфері захисту прав інвесторів. Це обумовило неадекватність стратегічним

цілям розвитку спрямованості інвестиційних потоків. Найвищими темпами зростали капіталовкладення в сектори економіки посередницького характеру: в торгівлю (протягом 2005–2008 рр. – на 126,9%), фінансову діяльність (114,4%), операції з нерухомістю (81,0%). Водночас галузі реальної економіки суттєво поступалися за темпами залучення інвестицій: переробна промисловість за чотири роки збільшила інвестиційний капітал на 62,8%, транспорт і зв'язок – на 11,3%. Ретельний аналіз інвестиційних процесів в промисловості дозволяє зробити висновок, що структурою інвестицій консервувалася низькотехнологічна структура промислового виробництва. Зокрема, у 2007 р. понад 80% усіх інвестицій у переробну промисловість надійшли в низько- та середньо-низькотехнологічні галузі. Натомість стабільно зростала частка вкладень в операції з нерухомістю і торгівлю. За підсумком 2008 р. сумарна частка інвестицій у торгівлю, фінансову діяльність та операції з нерухомістю сягнула 33,6 проти 23,4% у 2004 р., водночас частка промисловості відповідно зменшилася з 37,2 до 32,9%. Таким чином, основною тенденцією докризового періоду стала переорієнтація інвестиційних потоків зі сфери промислового виробництва до сфери фінансових послуг і операцій із нерухомістю, що можна вважати малоефективною та не зорієнтованою на реалізацію стратегічних пріоритетів економічного розвитку [20].

Кризові явища світової та вітчизняної економік не могли не позначитися на розвитку інвестиційних процесів. Характер останніх формувався під дією низки чинників [12], з-поміж яких такі:

- значне падіння обсягів виробництва, спричинене звуженням зовнішнього та внутрішнього попиту;

- погіршення очікувань суб'єктів господарювання щодо найближчих перспектив економічного зростання;

- погіршення фінансового становища підприємств, зменшення їхніх прибутків, а отже, можливостей інвестування;

- погіршення умов кредитування, особливо довгострокового, що ускладнило реалізацію інвестиційних проектів у галузях з високою часткою позичкових ресурсів, передусім у будівництві, машинобудуванні, металургії;

- скорочення державних інвестицій унаслідок перерозподілу фінансових ресурсів на поточні витрати;

різке збільшення витрат на імпортні складники виробництва та на обслуговування боргових зобов'язань в іноземній валюті внаслідок знецінення гривні, що послаблювало стимули до довгострокових інвестиційних проєктів.

Дія цих чинників призвела до згорання інвестиційної активності. У 2009 р. обсяг інвестицій в основний капітал знизився порівняно з 2008 р. на 41,5%. Зміна інвестиційної динаміки тісно корелювала з тенденціями розвитку видів діяльності. Так, з-поміж галузей реального сектору економіки найбільше зниження обсягів інвестицій відбулося в будівництві (на 62,2%), переробній промисловості (на 35,3%), на транспорті (на 33,3%). Суттєво також зменшилося інвестування у посередницьких видах діяльності – сфері нерухомості (на 52,8%), фінансовій діяльності (на 35,4%), торгівлі (на 48,3%). Скоротилися (на 50,2%) інвестиції і в сільському господарстві, яке продовжувало демонструвати позитивну динаміку виробництва. У промисловості найбільш негативна динаміка інвестицій в основний капітал була зафіксована в галузях із тривалим технологічним циклом, що попередніми роками були рушіями інвестиційної активності, зокрема в металургії (обсяги інвестицій зменшилися на 42,6%), машинобудуванні (48%), у виробництві неметалевої мінеральної продукції (39,5%).

Посткризовий період характеризується продовженням низки обмежувальних чинників для інвестиційних процесів, з-помітних такі:

- високі інвестиційні ризики, насамперед через недосконалість інституційного середовища інвестиційної діяльності;

- несприятливий бізнес-клімат (попри здійснені кроки в реформуванні регуляторної системи);

- відсутність адекватної політики залучення іноземних інвестицій в умовах загострення конкуренції на міжнародних ринках капіталів;

- невисока довгострокова дохідність залученого капіталу в галузі реального сектору порівняно з фінансовою діяльністю, торгівлею тощо.

Традиційними для України джерелами формування інвестицій в основний капітал є власні кошти підприємств, частка яких у структурі інвестування у докризовий період коливалася в межах 56–57%, та кредити банків, частка яких збільшувалася (у 2007 р. –

до 16,6%). Проте зростаючі обсяги споживчого кредитування з боку вітчизняних банків у цей період не створювали стимулів для розвитку вітчизняної економіки, підтримуючи імпорт, оскільки значна частина кредитних коштів була спрямована на купівлю товарів тривалого використання іноземного виробництва.

Докризовий період характеризувався також стрімкою динамікою іноземних інвестицій, коли їх обсяг збільшився з 9,1 млрд дол. США станом на 1.01.2005 р. до 29,5 млрд дол. США на 1.01.2008 р. Рекордний обсяг ПІІ було залучено в 2007 р. – 7,9 млрд. дол. США. Водночас використання Україною цього потужного джерела інвестиційних ресурсів знаходиться на дуже низькому рівні. Загалом станом на 1 жовтня 2011 у вітчизняному економіку надійшло 48,5 млрд. дол. США ПІІ (з урахуванням переоцінки, втрат, курсової різниці), що в розрахунку на одну особу становить 1060,8 дол. США. За цим показником ми відстаємо майже від усіх країн Центральної та Східної Європи: від Росії – у 1,8 разу, Польщі – у 4 рази, Чехії – у 10,5 разу тощо.

Кризові явища 2008–2009 рр. зумовили значне звуження доступу до кредитних ресурсів і, як наслідок, скорочення частки кредитів банків та інших позик серед джерел фінансування інвестицій в основний капітал. Значне зростання частки власних коштів до 63,3% у 2009 р. свідчить про відсутність у країні дієвих механізмів зовнішнього фінансування інвестиційних проектів, які могли б стати рушієм технологічного оновлення економіки.

У період кризи суттєво скоротилося державне інвестування економіки. Обсяг капітальних видатків у Зведеному бюджеті України 2009 р. порівняно з попереднім бюджетним періодом зменшився вчетверо – на 30,8 млрд грн. Як результат, частка капітальних видатків зменшилася до 4,3% від загального обсягу видатків бюджету, що є критично низьким показником. Для прикладу, в країнах Центрально-Східної Європи цей показник складає близько 20–25%. Таким чином, бюджет був повністю використаний на задоволення поточних потреб, проте не задіяний для вирішення структурних та інвестиційних проблем економічного зростання [2].

Відновлення економічного зростання 2010 р. сприяло відновленню фактично докризової структури джерел фінансування інвестиційної діяльності в країні. Зміни пов'язані зі зростанням частки державного бюджету внаслідок активних капіталовкладень держа-

ви в інфраструктурні об'єкти для проведення Євро2012, а також значним збільшенням частки коштів населення на індивідуальне житлове будівництво (з 3,6% у 2009 р. до 10,7% у 2010 р.).

У сучасній конкурентоспроможній економіці інноваційний чинник стає вирішальною умовою її стійкого економічного розвитку на середньо строкову і тривалу перспективу. В більшості провідних країн світу інновації є одним з основних чинників, що впливають на структурні перетворення в економіці, дозволяють сформувати нову якість економічної системи і забезпечити конкурентоспроможність економіки. Проте, в Україні інноваційний розвиток не став однією з головних характеристик зростання національної економіки. Внесок високих технологій у вітчизняний економічний розвиток складає лише 0,7% [10].

Інноваційні процеси в Україні мають нестійкий характер за відсутності чітких довгострокових стимулів для інноваційної діяльності. Наявність відносно високого інноваційного потенціалу економіки нівелюється суттєвими вадами в реалізації механізмів інноваційного розвитку економіки, підтвердженням чого є низькі позиції України у світових рейтингах за показниками ефективності інноваційного розвитку.

Так, в рейтингу Світового економічного форуму за критерієм «інноваційні чинники» Україна посідала 63 позицію серед 139 країн [32].

Сучасний стан інноваційної діяльності в Україні характеризується збереженням низького рівня інноваційної активності промислових підприємств.

За часткою підприємств, що займалися інноваційною діяльністю, Україна суттєво поступається розвиненим країнам. Так частка підприємств, що займалися інноваційною діяльністю, у 2008 р. складала в ЄС 51,6%, у Німеччині – 79,9%, Люксембурзі – 64,7%, Бельгії – 58,1%, Португалії – 57,8%, це у 4–6 разів більше, ніж в Україні. Зазначений показник в Україні був удвічі нижчим, ніж у найменш інноваційно активних країнах ЄС: Латвії (24,3%), Польщі (27,9%), Угорщині (28,9%), Литві (30,3%), Болгарії (30,8%).

В Україні інноваціями у 2011 р. займалося кожне шосте (16,2%), а безпосередньо впроваджувало інновації у своїй діяльності лише кожне восьме (12,5%) підприємство (рис. 2.23).

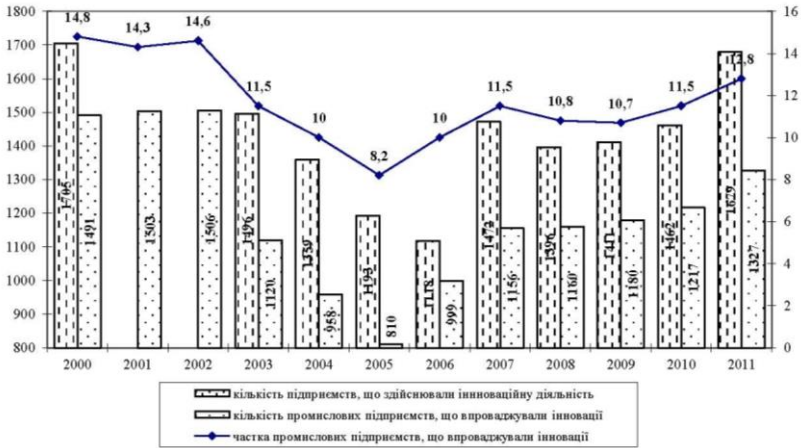


Рис. 2.23. Інноваційна активність промислових підприємств у 2000–2011 рр.

Різке зменшення кількості інноваційно активних підприємств у 2003–2005 рр. є об'єктивним критерієм умов інноваційної діяльності в Україні.

Подальше їх зростання було незначним, залишаючись на рівні, який не дозволяв суттєво впливати на формування основних параметрів конкурентоспроможності економіки країни.

Найбільша частка інноваційно активних підприємств у 2011 р. була сконцентрована у переробній промисловості (17,1%) – у виробництві коксу та продуктів нафтоперероблення (34,9%), машинобудуванні (24,5%), хімічній і нафтохімічній промисловості (24,0%), металургійному виробництві (15,2%), харчовій промисловості (16,1%).

У сфері виробництва та розподілення електроенергії, газу й води у 2011 р. частка таких підприємств складала 13,2%, у добувній промисловості – 8,6%. При цьому частка підприємств, що випускають високотехнологічну продукцію, складає лише 4,5% від загальної кількості підприємств України.

Результативність інноваційного процесу в промисловості України поступово знижується і в частині створення інноваційної продукції, і щодо продукування нових технологічних рішень. Так, у

2011 р. у промисловості було освоєно виробництво 3238 нових видів інноваційної продукції, що втричі нижче за показник навіть 2003 р. (рис. 2.8). Негативна тенденція зменшення частки інноваційної продукції, що чітко прослідковується впродовж кризових років, характерна і посткризовому періоду.

У структурі всього промислового виробництва частка інноваційної продукції в загальному обсязі реалізованої продукції в промисловості протягом 2007–2011 рр. знизилася з 6,7 до 3,8%, досягнувши найнижчого рівня за останні десять років.

Починаючи з 2007 р., відбувається скорочення інноваційного складника у виробництві майже всіх галузей промисловості, причому кризові тенденції 2009–2011 рр. суттєво прискорили цей процес (рис. 2.24).

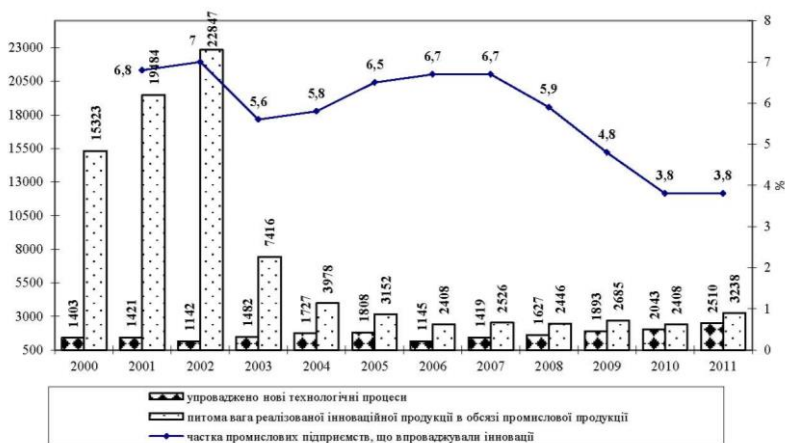


Рис. 2.24. Упровадження інновацій на промислових підприємствах у 2000–2011 рр.

Найбільше знизилася інноваційність виробництва таких галузей як харчова, легка, деревообробна, целюлозно-паперова, хімічна й нафтохімічна, машинобудування, що свідчить про формування підґрунтя для зниження конкурентоспроможності продукції цих галузей на тривалу перспективу, що своєю чергою формує суттєві ризики для стабільності розвитку промисловості України.

Галузева структура реалізованої інноваційної продукції є нестійкою і часто зазнає негативних змін у напрямі погіршення її технологічного складника.

У докризові роки динаміка реалізованої інноваційної продукції характеризувалася негативною тенденцією зменшення питомої ваги машинобудування. Якщо у 2004 р. його частка складала 44,6%, то до 2006 р. вона знизилася більше ніж на третину – до 28,4%.

Водночас у 3,3 рази зросла частка металургійної галузі (із 7,8 до 25,6%).

Надалі ці дві галузі стали основними суб'єктами інноваційного виробництва (їхні частки у структурі виробництва інноваційної промислової продукції 2008 р. склали відповідно 38,9 і 35,5%).

Крім них найбільшими виробниками інноваційної продукції у 2008 р. були також хімічна й нафтохімічна промисловість (5,6%) і харчова промисловість (9,9%). Проте, для відтворення вітчизняної промисловості на інноваційній основі цього недостатньо, оскільки майже дві третини інноваційної продукції в економіці України створюють виробництва третього і четвертого технологічних укладів.

Коротко підсумовуючи, доцільно визначити, що недостатні обсяги інвестицій в основний капітал та пасивну інноваційну політику можна вважати загрозою для економічної безпеки підприємств, адже вони не сприяють зростанню конкурентоспроможності та гальмують розвиток первинної ланки економіки.

2.3. Моделювання загроз економічній безпеці вітчизняних підприємств

Результатом проведеного аналітичного дослідження у двох попередніх підрозділах став перелік загроз економічній безпеці для вітчизняних підприємств.

Нехай визначена сукупність загроз становить деяку множину

$$Z = \{z_1, z_2, \dots, z_n\}.$$

З цієї сукупності виберемо підмножину $Z_1 \in Z_2$ найсуттєвіших загроз.

Для наочності математичного позначення загрози доповнимо її мнемонічною назвою.

Таблиця 2.1

Перелік факторів та їх математичне позначення

Математичне позначення	Назва фактора	Мнемонічна назва
Z_1	несприятливі умови для ведення бізнесу	УВБ
Z_2	висока ресурсомісткість виробництва	ВРВ
Z_3	негативний вплив тіньової економіки	ВТЕ
Z_4	надмірний податковий тиск	НПТ
Z_5	низька ефективність господарської діяльності	НЕВ
Z_6	зношеність основних фондів та технологічне відставання	ЗОФ
Z_7	кадрові проблеми	КП
Z_8	рейдерство та протиправні дії кримінальних структур	РПД
Z_9	галузева диспропорція із пріоритетним розвитком сировинних секторів економіки	ГД
Z_{10}	пасивна інвестиційно-інноваційна діяльність	ІД

Підмножину факторів Z_1 та можливі взаємозв'язки між ними подамо у вигляді орієнтованого графа (рис. 2.25), на вершинах якого розміщено елементи підмножини Z_1 , дуги з'єднують суміжні пари вершин (z_i, z_j) , для котрих визначено зв'язок.

Він вказує на певну залежність одного фактора (початок стрілки) від іншого (кінець стрілки).

Наприклад, низька ефективність господарської діяльності (НЕВ) спричинена: несприятливими умовами ведення бізнесу

(УВБ), високою ресурсомісткістю виробництва (ВРВ), надмірним податковим тиском (НПТ), зношеністю основних засобів та технологічним відставанням (ЗОФ), кадровими проблемами (КП) та пасивною інвестиційно-інноваційною діяльністю (ІД).

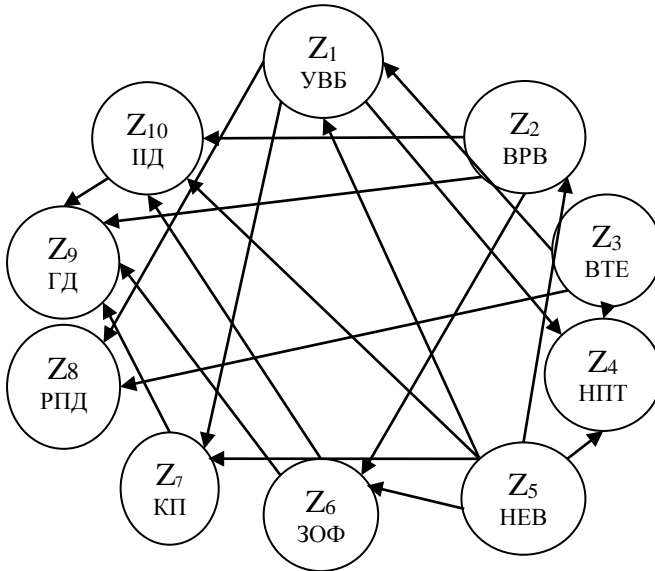


Рис. 2.25. Граф зв'язків між загрозами впливу на економічну безпеку підприємства

На основі поданого графа будемо бінарну матрицю залежності A для множини вершин Z_1 [13]:

$$a_{ij} = \begin{cases} 1, \text{якщо критерій (ввершина) } i \text{ залежить} \\ \text{від критерію (ввершини) } j; \\ 0, \text{якщо критерій (ввершина) } i \text{ не залежить} \\ \text{від критерію (ввершини) } j. \end{cases} \quad (2.1)$$

Для зручності матрицю A розмірності 10×10 елементів помістимо в табл. 2.2, додавши до неї інформаційний рядок і стовпець з назвами загроз.

Таблиця 2.2

Бінарна матриця залежності

		1	2	3	4	5	6	7	8	9	10
		УВБ	ВРВ	ВТЕ	НПТ	НЕВ	ЗОФ	КП	РПД	ГД	ПД
1	УВБ	0	0	0	1	0	0	1	1	0	0
2	ВРВ	0	0	0	0	0	1	0	0	1	1
3	ВТЕ	1	0	0	1	0	0	0	1	0	0
4	НПТ	0	0	0	0	0	0	0	0	0	0
5	НЕВ	1	1	0	1	0	1	1	0	0	1
6	ЗОФ	0	0	0	0	0	0	0	0	1	1
7	КП	0	0	0	0	0	0	0	0	1	0
8	РПД	0	0	0	0	0	0	0	0	0	0
9	ГД	0	0	0	0	0	0	0	0	0	0
10	ПД	0	0	0	0	0	0	0	0	1	0

Використовуючи матрицю A , будемо матрицю досяжності таким чином. Формуємо бінарну матрицю $(I+A)$, де I – одинична матриця.

У результаті матриця досяжності повинна задовольняти умову

$$(I + A)^{k-1} \leq (I + A)^k = (I + A)^{k+1} \quad (2.2)$$

Практично її побудова зводиться до заповнення таблиці, подібної до наведеної вище, бінарні елементи якої визначаються за таким правилом:

$$b_{ij} = \begin{cases} 1, & \text{якщо з } i \text{ можна потрапити в } j \\ 0, & \text{в іншому випадку.} \end{cases} \quad (2.3)$$

Таблиця 2.3

Матриця досяжності

		1	2	3	4	5	6	7	8	9	10
		УВБ	ВРВ	ВТЕ	НПТ	НЕВ	ЗОФ	КП	РПД	ГД	ПД
1	УВБ	1	0	0	1	0	0	1	1	0	0
2	ВРВ	0	1	0	0	0	1	0	0	1	1
3	ВТЕ	1	0	1	1	0	0	0	1	0	0
4	НПТ	0	0	0	1	0	0	0	0	0	0
5	НЕВ	1	1	0	1	1	1	1	0	0	1
6	ЗОФ	0	0	0	0	0	1	0	0	1	1
7	КП	0	0	0	0	0	0	1	0	1	0
8	РПД	0	0	0	0	0	0	0	1	0	0
9	ГД	0	0	0	0	0	0	0	0	1	0
10	ПД	0	0	0	0	0	0	0	0	1	1

Вершина z_j досягається з вершиною z_i , якщо в графі (рис. 2.25) існує шлях, який приводить з вершини z_i до вершини z_j .

Така вершина називається досяжною.

Позначимо підмножину подібних вершин через $S(z_i)$.

Аналогічно вершина z_i є попередницею вершини z_j , якщо вона досягає її вершини.

Нехай сукупність вершин-попередниць утворює підмножину $P(z_i)$.

Остаточню перетин підмножин вершин досяжних і вершин-попередниць, тобто підмножина

$$R(z_i) = S(z_i) \cap P(z_i), \quad (2.4)$$

вершин якої не досягаються з будь-якої з вершин множини Z_1 , що залишилися, визначає певний рівень ієрархії пріоритетності дій загроз, віднесених до цих вершин.

Додатковою умовою при цьому є забезпечення рівності

$$P(z_i) = R(z_i) \quad (2.5)$$

Виконання сукупності вищезазначених дій дає перший рівень (найнижчий з точки зору важливості впливу на досліджуваний процес) ієрархії загроз. Для визначення його з урахуванням попередньої матриці створюємо табл. 2.4.

Таблиця 2.4

Розрахункова таблиця

i	$S(z_i)$	$P(z_i)$	$S(z_i) \cap P(z_i)$
1	1, 4, 7, 8	1, 3, 5	1
2	2, 6, 9, 10	2, 5	2
3	1, 3, 4, 8	3	3
4	4	1, 3, 4, 5	4
5	1, 2, 4, 5, 6, 7, 10	5	5
6	6, 9, 10	2, 5, 6	6
7	7, 9	1, 5, 7	7
8	8	1, 3, 8	8
9	9	2, 6, 7, 9, 10	9
10	9, 10	2, 5, 6, 10	10

Другий стовпець цієї таблиці – номери одиничних елементів відповідних рядків матриці досяжності, третій – номери одиничних елементів стовпців даної матриці.

Рівність (2.5) виконується для 3-ої – негативний вплив тіньової економіки (ВТЕ) та 5-ої – низька ефективність виробництва (НЕВ) загроз.

Згідно з методом аналізу ієрархій [5], ці загрози належать до найнижчого рівня пріоритетності впливу на економічну безпеку.

Далі з табл. 2.4 вилючаємо рядки 3 та 5, а в i -му стовпцях викреслиємо цифри 3 і 5.

Одержимо табл. 2.5, яка є основою для обчислення другої ітерації знаходження номерів загроз, що визначають наступний рівень ієрархії.

Таблиця 2.5

Розрахункова таблиця

i	$S(z_i)$	$P(z_i)$	$S(z_i) \cap P(z_i)$
1	1, 4, 7, 8	1	1
2	2, 6, 9, 10	2	2
4	4	1, 4	4
6	6, 9, 10	2, 6	6
7	7, 9	1, 7	7
8	8	1, 8	8
9	9	2, 6, 7, 9, 10	9
10	9, 10	2, 6, 10	10

У другій ітерації рівність (2.5) виконується для 1-ї – несприятливі умови для ведення бізнесу (УВБ) та 2-ї – висока ресурсомісткість виробництва (ВРВ) загрози, які в визначають наступний рівень ієрархії.

Відтак з табл. 2.5 видаляємо рядки 1 та 2, а в 2-му і 3-му стовпцях – цифр 1 та 2.

Одержимо табл. 2.6.

Розрахункова таблиця

i	$S(z_i)$	$P(z_i)$	$S(z_i) \cap P(z_i)$
4	4	4	4
6	6, 9, 10	6	6
7	7, 9	7	7
8	8	8	8
9	9	6, 7, 9, 10	9
10	9, 10	6, 10	10

Черговий рівень утворюють загрози: 4-а – надмірний податковий тиск (НПТ), 6-а – зношеність основних фондів та технологічне відставання, 7-а – кадрові проблеми, 8-а – рейдерство та протиправні дії кримінальних структур (РПД). Відповідний рядок і цифру в стовпцях вилучаємо з табл. 2.6.

Без додаткових розрахунків, можна стверджувати, що останній рівень ієрархії посядуть 9-а – галузева диспропорція із пріоритетним розвитком сировинних секторів економіки та 10-а – пасивна інвестиційно-інноваційна діяльність.

Розташувавши загрози за визначеними рівнями, одержимо ієрархічно структуровану модель (рис. 2.26), що імітує пріоритетність їх впливу на економічну безпеку вітчизняних підприємств.

Визначена ієрархія загроз стала підґрунтям для побудови моделі ключових загроз для вітчизняних підприємств (рис. 2.27).

Оскільки суть кожної загрози нами були ретельно визначено у попередніх підрозділах, тому приділимо увагу виключно результатам здійсненого ієрархічного впорядкування.

Найвищий рівень важливості, який зайнятий загрозами пов'язаними із галузевою диспропорцією та пасивною інвестиційно-інноваційною діяльністю, на нашу точку зору, доцільно трактувати як стратегічний. Зазначене спричинено тим фактом, що процеси пов'язані із реалізацією визначених загроз найбільш суттєві

негативні наслідки будуть мати в довгостроковій перспективі, коли вітчизняний товаровиробник не зможе конкурувати не лише на зовнішньому, але і внутрішньому ринку, для нього вільними залишаться лише окремі ніші пов'язані із добуванням природних ресурсів та їх примітивною й низько вартісною обробкою. На реальність розвитку подій у цьому напрямку вказують результати господарської діяльності підприємств високотехнологічного сектору економіки, які суттєво поступаються за темпами розвитку та ефективністю суб'єктам господарювання сировинних секторів.

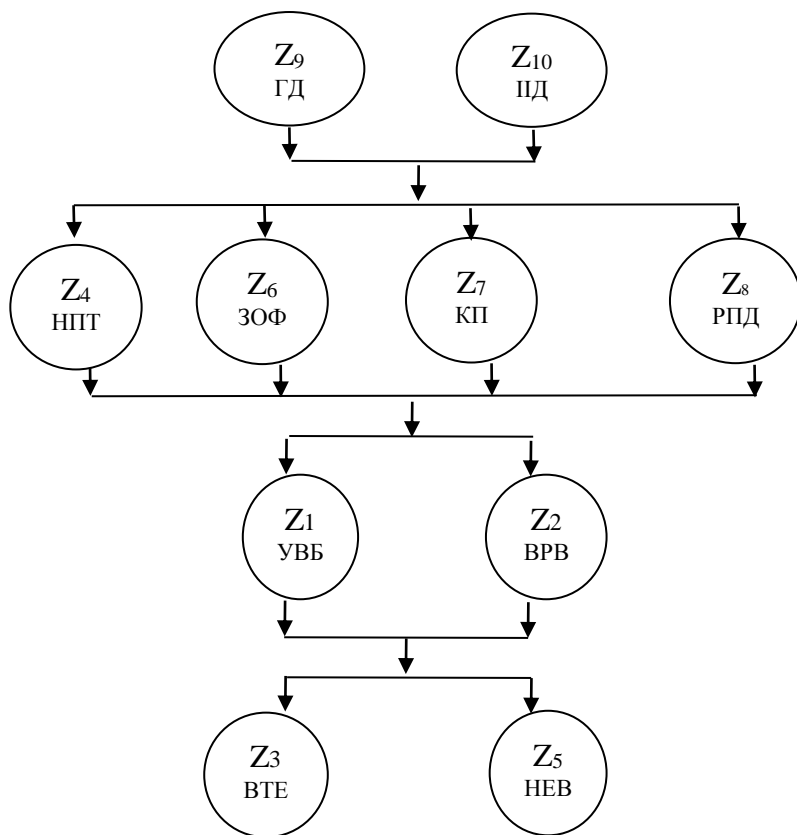


Рис. 2.26. Модель ієрархії загроз впливу на економічну безпеку підприємств

Наступний рівень ієрархії об'єднав одночасно чотири загрози, які пов'язані із надмірним податковим тиском, зношеністю основних засобів та технологічним відставанням, кадровими проблемами, рейдерством та протиправними діями кримінальних структур. На нашу точку зору, ці загрози стосовно різних аспектів діяльності, але схожі за інтенсивністю впливу на економічну безпеку підприємства. Якщо попередній рівень ієрархії нами трактувався як стратегічний, то цей – тактичний. Усі перелічені загрози є реальністю сьогодення і за ефективно організованої системи економічної безпеки підприємства їм можна протистояти.

Третій рівень сформували дві загрози: несприятливі умови для ведення бізнесу та висока ресурсомісткість виробництва. Першу – можна визначити як зовнішню, адже вона пов'язана із сприятливістю та інтенсивністю впливу зовнішнього середовища на підприємство, а друга – внутрішня, яка є об'єктом техніко-технологічної складової економічної безпеки. Звідси слідує висновок, що система економічної безпеки підприємства – повинна бути готовою чітко ідентифікувати, визначити та мінімізувати вплив як зовнішніх, так і внутрішніх загроз.

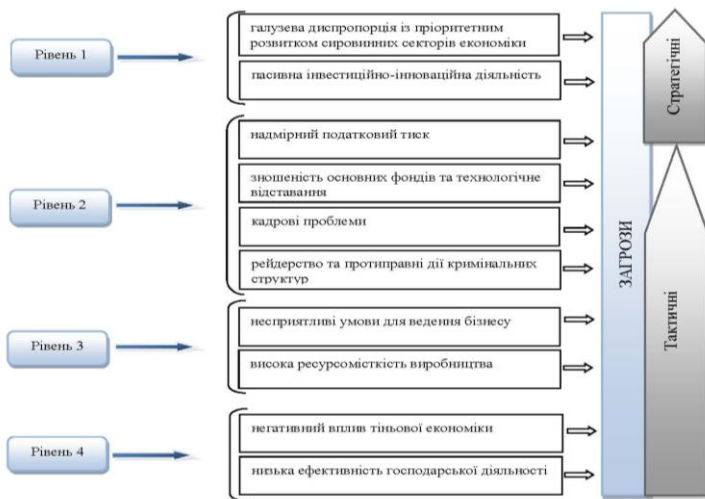


Рис. 2.27. Модель рейтингу ключових загроз для вітчизняних підприємств

Останній рівень представлений також двома загрозами пов'язаними із негативним впливом тіньової економіки та низькою ефективністю господарської діяльності. Як і на попередньому рівні, перша – зовнішня, а друга – внутрішня. Вплив тіньової економіки підприємство може лише контролювати та реалізовувати захисні дії. Стосовно ж результатів діяльності, то тут завданням системи безпеки є активний вплив на об'єкти безпеки з метою забезпечення необхідного для розвитку рівня безпеки.

Підсумовуючи потрібно ще раз наголосити, що визначена сукупність загроз є усереднена, яка не враховує специфіки функціонування якогось окремого суб'єкта підприємницької діяльності, але за суттю більшість із них притаманна для вітчизняних підприємств, а відтак і актуалізує важливість забезпечення високого рівня економічної безпеки на мікрорівні.

ЛІТЕРАТУРА ДО ДРУГОГО РОЗДІЛУ

1. Діяльність суб'єктів господарювання : стат. зб. / [за ред. І. М. Жук]; Держкомстат України. – К. : Держаналітінформ, 2012. – 447 с.
2. Економіка України на шляху від депресії до зростання: джерела, важелі, інструменти / Я. А. Жаліло, Д. С. Покришка, Я. В. Белінська [та ін.]. – К. : НІСД, 2010. – 418 с.
3. Економіка України: стратегія і політика довгострокового розвитку / [за ред. акад. НАН України В.М. Гейця]. – Ін-т екон. прогноз. ; К. : Фенікс, 2003. – 1008 с.
4. Жаліло Я. А. Структурні трансформації промисловості України в період фінансово-економічної кризи / Я. А. Жаліло, Д. С. Покришка // Вісник Інституту економіки та прогнозування. – 2010. – С. 30–36.
5. Лямец В. И. Системный анализ : вступит. курс / В. И. Лямец, А. Д. Тевяшев. – 2-е изд., перераб. и доп. – Х. : ХНУРЕ, 2004. – 448 с.
6. Мазур І. Детінізація економіки України: теорія та практика : моногр. / І. Мазур. – К. : Видавничо-поліграфічний центр «Київський університет», 2006. – 239 с.
7. Модернізація України – наш стратегічний вибір: Щорічне Послання Президента України до Верховної Ради України. – К., 2011. – 269 с.
8. Наукова та інноваційна діяльність в Україні : стат. зб. / Держкомстат України. – К. : Техніка, 2011. – 457 с.
9. Новий курс: реформи в Україні. 2010-2015 : Нац. доп. / за заг. ред. В. М. Гейця [та ін.]. – К. : НВЦ НБУВ, 2010. – 232 с.
10. Огляд актуальної наукової дискусії про перспективи розвитку світу в цілому та України як його частини / Інститут демографічних та соціальних досліджень НАН України, Києво-Могилянська Бізнес-Школа, Український інститут соціальних досліджень імені Олександра Яременка. – К., 2008. – 328 с.
11. Підприємницьке право. Кн. 2 / за ред. О. В. Старцев. – К. : Істина, 2005. – 352 с.
12. Ризики економічної депресії та потенціал післякризового відновлення економіки України / Я. А. Жаліло, Д. С. Покришка, Я. В. Белінська [та ін.]. – К. : НІСД, 2009. – 317 с.
13. Сеньківський В. М. Модель ієрархії критеріїв якості книжкових видань / В. М. Сеньківський // Наук. зап. (Укр. акад. друкарства). – 2007. – Вип. 11. – С. 73–80.
14. Соколов М. Амортизационная политика и диверсификация экономики / М. Соколов // Экономист. – 2010. – № 10. – С. 20.

15. Соціально-економічний стан України: наслідки для народу та держави : нац. доп. / за заг. ред. В. М. Гейця [та ін.]. – К. : НВЦ НБУВ, 2009. – 687 с.
16. Статистичний щорічник України за 2011 рік / за ред. О. Г. Осауленка ; Держкомстат України. – К. : Техніка, 2012. – 566 с.
17. Стратегічні виклики XXI ст. суспільства та економіці України : [в 3 т.] / за ред. В. М. Гейця, В. П. Семиноженка, Б. Є. Кваснюка. – Т. 1 : Економіка знань – Модернізаційний проєкт України / за ред. В. М. Гейця, В. П. Семиноженка, Б. Є. Кваснюка. – К. : Фенікс, 2007. – 544 с.
18. Стратегічні виклики XXI століття суспільства та економіці України : [в 3 т.] / за ред. акад. НАН України В. М. Гейця, акад. НАН України В. П. Семиноженка, чл.-кор. НАН України Б. Є. Кваснюка. – Т. 3 : Конкурентоспроможність української економіки / – К. : Фенікс, 2007. – 556 с.
19. Тумар Н. Б. Экономическая безопасность предприятия / Н. Б. Тумар. – Харьков, 2006. – 346.
20. Україна в 2005–2009 рр.: стратегічні оцінки суспільно-політичного та соціально-економічного розвитку : монографія / за заг. ред. Ю. Г. Рубана. – К. : НІСД, 2009. – 655 с.
21. Україна в 2008 році: щорічні оцінки суспільно-політичного та соціально-економічного розвитку : моногр. / [за заг. ред. Ю. Г. Рубана]. – К. : НІСД, 2008. – 744 с.
22. Флейчук М. І. Легалізація економіки та протидія корупції у системі економічної безпеки: теоретичні основи та стратегічні пріоритети в умовах глобалізації / М. І. Флейчук. – Львів: Ахілл, 2008. – 660 с.
23. Харазішвілі Ю. М. Вимірювання тіньового ВВП за допомогою функцій сукупного попиту та сукупної пропозиції / Ю. М. Харазішвілі // Економіка України. – 2007. – № 1. – С. 57–63.
24. Чумаченко М. Г. Перспективи неоіндустріальної трансформації економіки України та Донбасу // М. Г. Чумаченко, О. І. Амоша, В. І. Ляшенко // Структурні реформи і трансформації в промисловості: перспективи і пріоритети : тези доп. і повідом. Міжнар. наук.-практ. конф. (Донецьк, 17.12.2010 р.) / НАН України, Ін-т економіки пром-сті; редкол. : О. І. Амоша (відп. ред.) [та ін.]. – Донецьк, 2010. – С. 3–6.
25. Чухно А. А. Твори : [у 3 т.] / А. А. Чухно : НАН України, Київ. нац. ун-т ім. Тараса Шевченка, Наук.-дослід. фін. ін-т при М-ві фін. України. – Т. 2: Інформаційна постіндустріальна економіка : теорія і практика. – К., 2006. – 512 с.
26. Шовкун І. Податкові фактори технологічного розвитку економіки / І. Шовкун // Економіка України. – 2011. – № 5. – С. 52–56.
27. Corruption perceptions index 2010. – Berlin : Transparency International, 2011. – P. 5–8.

28. Doing Business 2011: Making a Difference for Entrepreneurs / The World Bank, International Finance Corporation [Электронный ресурс]. – Режим доступа : <http://www.doingbusiness.org/Documents/Annual-Reports/English/DB11-FullReport.pdf>
29. Global Financial Integrity Program [Электронный ресурс]. – Режим доступа : <http://www.gfintegrity.org/>
30. Paying Taxes 2011. The Global Picture / International Finance Corporation, PricewaterhouseCoopers, 2011 [Электронный ресурс]. – Режим доступа : <http://www.pwc.com>.
31. The Global Competitiveness Report 2010-2011. – Geneva : World Economic Forum, 2012. – P. 335 [Электронный ресурс]. – Режим доступа : http://www.weforum.org/docs/WEF_GlobalCompetitivenessReport_2010-2011.pdf
32. The Influence of the economic crisis on the underground economy in Germany and the other OECD-countries in 2010: a (further) increase [Электронный ресурс]. – Режим доступа : <http://www.econ.jku.at>
33. Yearbook Statistical Energy Review 2010 [Электронный ресурс]. – Режим доступа : <http://yearbook/enerdata/net>

Розділ 3

УДОСКОНАЛЕННЯ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

3.1. Кадрова безпека в економічній безпеці підприємства

Сучасне підприємство потрібно розглядати, як складну систему, у якій взаємодіють матеріально-речовинна, інтелектуально-інноваційна та людська складова розвитку власної діяльності. Ефективне використання цих складових та досягнення пріоритетних інтересів уможливлується завдяки режиму економічної безпеки – стабільного функціонування підприємства, його динамічного науково-технічного і соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам.

На поточному етапі еволюції методів управління в організаціях на перший план все чіткіше виступає персонал, як найвища цінність та найголовніший інструмент здійснення ефективної діяльності підприємства. Персонал впливає на всі аспекти життєдіяльності організації, а також невід’ємно пов’язаний з її економічною безпекою. Окрім цього, для персоналу організації притаманний високий динамізм розвитку. Він проявляється не тільки в прискоренні процесу оновлення професійних знань, умінь і навичок, але й в неухильному підвищенні ролі професійно важливих і ділових якостей працівників. Освіта, кваліфікація і рівень розвитку професійно важливих якостей виступають сьогодні основними якісними характеристиками персоналу.

Зважаючи на подане, сучасні системи керування націлені на розвиток різноманітних здібностей працівників для того, щоб останні максимально ефективно були задіяні в процесі виробництва. Зростання ролі соціальної складової виробництва обумовлює

якісні зміни систем керування організаціями, знаходить своє вираження в нових формах, методах і змісті кадрового менеджменту. Тому для збалансованого формування кадрового потенціалу необхідно створити діючу систему керування персоналом, що забезпечувала б економічну безпеку підприємства.

Економічна безпека підприємства являє собою достатньо широке поняття, яке включає в себе фінансову, силову, інформаційну, техніко-технологічну, правову а також кадрову безпеку. Одною з найголовніших складових економічної безпеки підприємства, установи, організації вважається кадрова безпека. Співробітники впливають на всі аспекти життєдіяльності фірми, вони невід'ємно пов'язані з її ефективною діяльністю. Таким чином, серед систем економічної безпеки підприємства та управління персоналом знаходиться кадрова безпека як підсистема систем, яка гарантуватиме стабільне та максимально ефективне функціонування підприємства і високий потенціал розвитку в майбутньому, а визначення місця і рівня впливу кадрової складової у загальній системі економічної безпеки організації потребує значних досліджень.

Перш за все зазначимо, що успішне функціонування підприємства в умовах ринкової економіки передбачає забезпечення ефективної системи заходів безпеки. Як правило, основні ризики організації генеруються її власним персоналом. За даними статистичних досліджень, близько 51% випадків економічних злочинів здійснюють співробітники компаній (рис 3.1) [37], а ефективна організація роботи щодо забезпечення кадрової безпеки може майже на 60% знизити прямі та передбачити непрямі збитки фірми, пов'язані з людським фактором [14].

Згідно з даними порталу Content Security, наявні у світі внутрішні та зовнішні загрози розподіляються таким чином: розголошення (зайва балакучість працівників) – 32%; несанкціонований доступ шляхом підкупу і шхилення до співпраці з боку конкурентів і злочинних угруповань – 24%; відсутність у компанії належного нагляду і жорстких умов забезпечення конфіденційності інформації – 14%; традиційний обмін виробничим досвідом – 12%; безконтрольне використання інформаційних систем – 10%; наявність передумов виникнення серед персоналу конфліктних ситуацій, пов'язаних з відсутністю високої трудової дисципліни, психологічною несумісністю, випадковим підбором кадрів, слабкою роботою кадрів зі згуртування колективу – 8%.

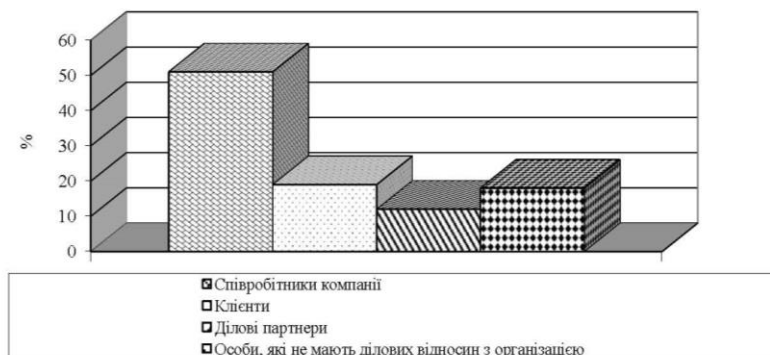


Рис. 3.1. Суб'єкти скоєння економічних злочинів

У відповідності до наведених фактів, у структурі економічних злочинів превалює людський фактор, що актуалізує проблему гарантування кадрової безпеки на мікрорівні. Підтвердженням цієї тези є і те, що за даними дослідження Ernst & Young, рівень зафіксованого в Україні корпоративного шахрайства трохи вищий за середній у розвинених країнах (13%), але кращий за показник країн, що розвиваються (20%).

Так, французька компанія Kroll Ontrack серед десяти основних тенденцій у сфері захисту інформаційних даних 2011 р. називає крадіжки за сприяння т. зв. інсайдерів: сьогодні прогресивні організації роблять ставку на посилення безпеки за допомогою технологій, в той час як злочинці йдуть легшим шляхом – знаходять співників серед персоналу.

На жаль, українські реалії такі, що підприємство окрім негативного впливу зовнішнього середовища потерпають і від внутрішніх злочинів, джерелом яких є власний персонал.

Окрім крадіжок інформації, можна зіштовхнутися і з чорним піаром з боку колишніх підлеглих, і з судовими позовами, що впливають на репутацію підприємства, і з некомпетентністю «випадкового» працівника, і з помилками у кадрових документах.

Показовим є той факт, що розмір збитків від реалізації загроз кадровій безпеці, таких як шахрайство та внутрішньокорпоративні крадіжки, в США складає 4,2 млрд дол. В середньому на кожну компанію припадає до 2,4 млн дол. збитків [29; 41].

При цьому 45% компаній по всьому світу активно займаються питаннями забезпечення кадрової безпеки підприємств. Встановлено, що в 33 країнах світу серед 7800 компаній найактивнішу політику управління кадрової безпеки ведуть у Північноамериканській зоні вільної торгівлі (NAFTA; Канада, США, Мексика), та пасивну – у Східній Азії. У свою чергу, Україна не увійшла у жоден зі світових рейтингів з внутрішньокорпоративного шахрайства і боротьбі з ним.

Однак, визначено, що в 2008 р. на середнє вітчизняне держпідприємство щороку зазнавали збитків від порушень персоналу на 10 млн грн. [29].

Крім економічного збитку від реалізації загроз кадровій безпеці існують і нематеріальні втрати, що обумовлюються зниженням морального духу підприємства, зіпсованою репутацією, зниженням вартості її акцій і порушенням ділових відносин з партнерами. Таким чином, підприємства відчують зростання дій загроз зі сторони власного персоналу, які пов'язані зі збільшенням ризиків в управлінні персоналом.

Негативні наслідки таких ризиків можуть привести до зменшення ефективності менеджменту підприємства та до повної втрати його власником.

Тому визначення загроз кадровій безпеці дає можливість зменшити ризики у виробничо-комерційній діяльності підприємств, що обумовлює актуальність дослідження.

В контексті поданого, визначимо, що до найпоширеніших видів порушень зі сторони персоналу належать:

- афери з боку провідних спеціалістів (менеджерів і керівників середньої ланки, відповідальних за конкретний напрям бізнесу підприємства), в основному «за стінами» своєї фірми, зокрема у міжнародних організаціях;

- «відкат». Фальсифікація сум «живих грошей» («готівки») у касі й сум на банківських рахунках, підробка чеків підприємства. Несанкціонований продаж і використання майна (власності) підприємства із корисливою метою;

- оплата роботи підставних («фіктивних осіб»), так званих «пролісків»;

- фальсифікація документації підприємства за допомогою електронної техніки й Інтернету (наприклад, перерахування коштів

підприємства на свій особистий рахунок, внесення «потрібних» змін у звітні документи);

- несанкціоновані операції із цінними паперами, матеріальними й нематеріальними активами підприємства. Фальсифікація звітів про використання коштів, виділених на відрядження, «представницькі видатки», на інші потреби підприємства;

Причини, тобто мотиви здійснення перелічених вище злочинів можна класифікувати наступним чином:

- особисті фінансові труднощі, неможливість задоволення життєвих потреб своїх та сім'ї;

- наявність слабких місць («дір») у системі управління діяльністю фірми (зокрема в системі бухгалтерського обігу);

- низька кваліфікація керівництва підприємства;

- нездоровий діловий клімат у колективі підприємства (наявність «скривджених»);

- психологічна готовність (схильність) працівника до зловживання службовим становищем;

- порочні зв'язки, вчинки, захоплення;

- відсутність налагодженого контролю з боку керівництва за діяльністю персоналу;

- слабкий кадровий менеджмент, що дає змогу займати відповідальні посади співробітникам-аферистам, неефективна персональна робота з кадрами.

Суттєвий вплив злочинів зі сторони персоналу, тобто реалізація внутрішніх загроз спонукає до ретельного вивчення та формування методологічних засад гарантування кадрової безпеки.

У відповідності до результатів вивчення доробку вітчизняних та закордонних науковців [1–48], можна чітко визначити, що кадрова безпека є синтетичною категорією: економічної теорії, теорії управління персоналом, економіки праці, соціології, політології, але, водночас, є і уніфікованою категорією, яка існує на всіх рівнях від окремо взятого підприємства до національної економіки.

Окрім цього, кадрова безпека є комбінацією складових, пов'язаних між собою складними і часто завуальованими зв'язками (табл. 3.1).

Таблиця 3.1

Складові кадрової безпеки підприємства

Складова	Зміст
Життє-діяльності	здоров'я – створення певних умов праці працівникам із запобігання травматизму, захворюванням на підприємстві; фізична – виконання комплексу заходів щодо запобігання порушенням правил безпеки
Професійна	праці – система принципів, підходів, дій, спрямована на створення певних умов праці (рівень оплати праці, посада, обладнання робочого місця) з урахуванням новітнього, передового досвіду на ринку праці; інформаційна – прогнозування структури персоналу, визначення потреби в кадрах, планування, залучення та розміщення персоналу, оцінювання результатів праці для виявлення потенціалу кожного працівника; пенсійно-страхова – соціальний захист працівників (страхування, медичне обслуговування); володіння сучасними знаннями – впровадження новітніх технологій у розвиток персоналу, удосконалення рівня професійних знань, навичок, умінь, здібностей у зв'язку з розвитком науково-технічного прогресу
Соціально-мотиваційна	фінансова – фінансова, грошово-кредитна платоспроможність працівників; упевненість у своєму робочому місці; оплата праці, яка враховує обсяг, кваліфікацію, професіоналізм і якість виконаної роботи; кар'єрна – професійно-кваліфікаційне та посадове просування працівників, заохочення в пристосуванні своєї кваліфікації до вимог робочого місця, в гарантіях виробничого зростання (планування кар'єри); підвищення особистої мобільності на ринку робочого сили; отримання шансів для самореалізації на робочому місці; етична – проведення загальноосвітніх семінарів, конференцій, групових дискусій; мотивація задоволення персоналу своєю роботою; поліпшення власного іміджу кожного працівника; адміністративно-незалежна – позбавлення можливості призначати не підготовлених і некомпетентних кадрів, які перебувають у родинних стосунках з власниками, акціонерами підприємства, на керівні посади
Анти-конфліктна	патріотична – створення психологічного клімату в колективі на основі позитивного ставлення до підприємства, що характеризується психологічними показниками об'єднаності працівників, забезпечує узгодженість, безконфліктність спілкування, відповідальність та обов'язок, товариську допомогу, вимогливість до себе та іншого в інтересах виробництва; психологічно-комунікаційна – сприяння міжособистісним комунікаціям і створення сприятливого мікроклімату, врахування інтересів і побажань працівників, його особистого потенціалу, задоволеність міжособистісними стосунками по вертикалі (керівник-підлеглий) та горизонталі (виконавці)

Змістом категорії « кадрова безпека » є характеристика стану економічної системи при якому відбувається ефективне функціонування всіх її функціональних складових, забезпечення захищеності та здатність протистояти внутрішнім і зовнішнім впливам і загрозам, пов'язаним з персоналом, змістовний та структурний аналіз, діагностика та прогнозування впливу діяльності персоналу на внутрішні та зовнішні показники вказаної економічної системи.

Кадрова безпека, як уже зазначалось вище, є поняттям складним і багатогранним, тому вітчизняні та зарубіжні автори виокремлюють різні підходи до його трактування. Складність процесу управління кадровою безпекою на підприємстві обумовлюється не лише недостатнім розвитком теоретичної бази дослідження, але й комплексністю даної проблеми та значною кількістю складових безпеки. Отже, кадрову безпеку підприємства слід розглядати як проблему комплексну і при її дослідженні потрібно застосовувати системний підхід.

Аналіз показав, що серед більшості авторів немає однаковості у визначенні даного поняття. За результатами проведеного теоретичного дослідження, нами було виділено три ключові підходи до трактування цього поняття. Перший підхід, який передбачає захист персоналу від зовнішніх і внутрішніх загроз, чітко прослідковується у роботах наступних науковців.

Так, О. Лашенко подає кадрову безпеку як стан економічної системи, при якому проводиться ефективна робота всіх її функціональних складових, забезпечується її захищеність та здатність протистояти внутрішнім і зовнішнім впливам і загрозам, пов'язаним з персоналом, і передбачає змістовний і структурний аналіз, діагностику та прогнозування впливу діяльності персоналу на внутрішні та зовнішні показники вказаної економічної системи. А. Мітрофанов дотримується думки, що кадрова безпека – це таке становище організації як соціальної спільноти й індивіда в ній, за якого на них із боку природного, економічного й соціального середовища, а також внутрішнього середовища самої людини не здатні заподіяти шкоди. А. Шаваєв визначає кадрову безпеку як стан захищеності суспільно-прогресивних інтересів організації з розвитку й удосконалення її людського капіталу, підтримки ефективної системи управління людськими ресурсами й мінімізації ризиків компанії, пов'язаних із її складовою. Н. Логінова доводить необхідність трактувати цю

категорію як найбільш важливу складову економічної безпеки підприємства, яка має на меті виявлення, знешкодження, запобігання, відтворення та попередження загроз, небезпек і ризиків, які спрямовані на персонал та його інтелектуальний потенціал, і ті, які йдуть безпосередньо від нього, що повинно проявлятися в системі управління трудовими ресурсами та в кадровій політиці підприємства. Згідно наукових напрацювань М. Петрового, кадрова безпека – це таке положення організації як соціальної спільності й індивіда в ній, при якому вплив на них з боку природного, економічного й соціального середовища, а також внутрішнього середовища самої людини не здатні заподіяти шкоди.

У другому підході увагу зосереджено на необхідності здійснення попереджувальних, запобіжних дій для збереження найбільш цінного ресурсу будь-якого підприємства – персоналу. Саме такої думки дотримується А. Джобава, у трактуванні якого кадрова безпека – сукупність заходів, спрямованих на запобігання протиправним діям або сприяння їм із боку персоналу підприємства. Н. Швець розглядає кадрову безпеку як процес запобігання негативним впливам на економічну безпеку підприємства через ризики і погрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами загалом. І. Воробйов дотримується думки, що кадрова безпека – це процес запобігання негативним впливам на економічну безпеку через ризики і погрози, що пов'язані з його інтелектуальним потенціалом і трудовими відносинами [6]. Г. Козаченко, В. Пономарьов та О. Ляшенко доводять, що під цієї складовою економічної безпеки потрібно розуміти процес запобігання негативним діям на безпеку підприємства за рахунок усунення ризиків та загроз, пов'язаних з інтелектуальним потенціалом та трудовими відносинами в цілому [15]. О. І. Черняк трактує кадрову безпеку як «...сукупність заходів спрямованих на запобігання протиправних дій або сприяння їм з боку персоналу підприємства».

Третій підхід нами визначено як такий, згідно з яким кадрову безпеку визначають як сукупність управлінських заходів спрямованих на найбільш ефективне формування та використання кадрового потенціалу підприємства. Такої точки зору дотримується О. Ареф'єва та О. Литовченко, трактуючи кадрову безпеку як сукупність управлінських заходів, пов'язаних з ефективним формуванням та використанням кадрового потенціалу підприємства з метою

забезпечення та підтримки економічної стійкості та результативності господарської діяльності підприємства [2]. О. Кириченко подає кадрову безпеку як правове та інформаційне забезпечення процесу управління персоналом: вирішення правових питань трудових відносин, підготовка нормативних документів, що їх регулюють, забезпечення необхідною інформацією всіх підрозділів управління персоналом [13]. В. Кібанов доводить необхідність визначення кадрової безпеки як генерального напрямку кадрової роботи, сукупності принципів, методів, форм організаційного механізму з опрацювання цілей, завдань, спрямованих на збереження, зміцнення й розвиток кадрового потенціалу, на створення відповідального і високопродуктивного згуртованого колективу, здатного вчасно реагувати на постійно мінливі вимоги ринку з урахуванням стратегії розвитку організації [12].

На нашу думку, визначення кадрової безпеки потрібно трактувати з врахуванням процесу розвитку думки стосовно цієї категорії і, водночас, багатогранності самої кадрової безпеки, що потребує комплексного та системного підходу для досягнення її високого рівня в умовах певного підприємства.

Завдяки зусиллям багатьох вчених були досліджені та оприлюднені основні принципи та напрями вдосконалення системи економічної безпеки, але поза увагою більшості вчених робіт і досі залишається методологія впровадження організаційно-економічних заходів забезпечення кадрової безпеки підприємства. Викладене вище обумовлює актуальність подальшого дослідження даної проблеми.

В науковій праці В. Ортинського, І. Керницького, З. Живко та ін. [8] доведено, що безпеку можуть забезпечувати дві групи суб'єктів: Перша група: займаються цією діяльністю безпосередньо на підприємстві і підпорядковані його керівництву. Серед них виокремлюють три підгрупи:

1) спеціалізовані суб'єкти, основним призначенням яких є постійна діяльність із забезпечення безпеки підприємства (в рамках своєї компетенції відділу тощо);

2) напівспеціалізовані суб'єкти, частина функцій у яких полягає в забезпеченні безпеки підприємства (маркетингова служба, юридичний підрозділ тощо);

3) решта персоналу та підрозділи підприємства, які в межах своїх посадових інструкцій та положень про підрозділи зобов'язані вживати заходів щодо забезпечення безпеки підприємства.

Друга група: зовнішні органи та організації, які функціонують самостійно і не підпорядковуються керівництву підприємства, але при цьому їх діяльність істотно впливає на безпеку підприємства. Суб'єктами цієї групи є:

- законодавчі органи;
- органи виконавчої влади;
- суди;
- правоохоронні органи;
- науково-освітні заклади;
- промислові шпигуни;
- конкуренти;
- іноземні компанії;
- кримінальні структури;
- фірми-розвідники

Формування такої чисельності суб'єктів кадрової безпеки є не випадковим, а скоріше виправданим кроком, адже перед підсистемою кадрової безпеки ставиться доволі значна кількість різнопланових завдань, які нами узагальнено і в графічному вигляді представлено на рис. 3.2.

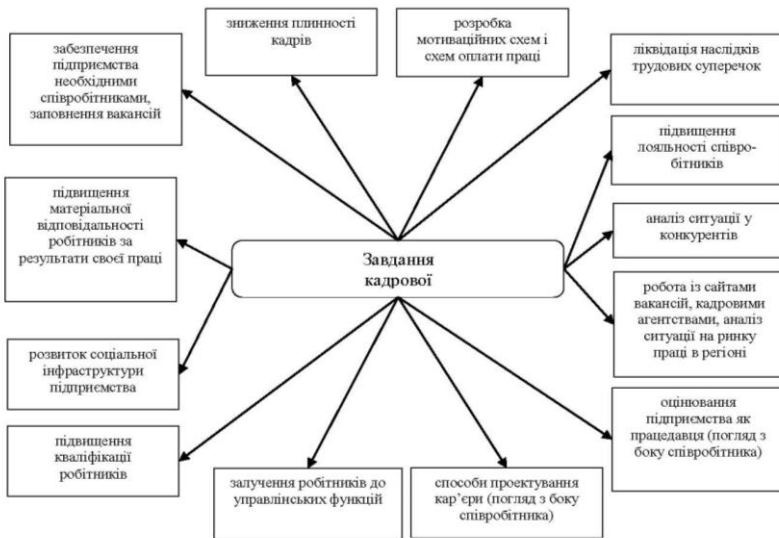


Рис. 3.2. Завдання підсистеми кадрової безпеки

У сучасних ринкових умовах складовою частиною комплексу заходів кожного підприємства повинна стати програма конкретних дій, спрямована на забезпечення високого рівня кадрової безпеки як складової економічної безпеки.

Таким чином, кадрова безпека як домінуючий елемент системи економічної безпеки організації побудована на трудових та етичних відносинах інтелектуального потенціалу, які забезпечують стабільну і прибуткову роботу підприємства, запобігаючи як внутрішнім, так і зовнішнім загрозам, що сприяє розвитку людського та соціального потенціалу, підвищення рівня і якості життя населення, що притаманні цивілізованому суспільству.

3.2. Загрози зі сторони персоналу та можливі шляхи їхньої нейтралізації

Ефективність функціонування підприємства, особливо в період становлення ринкової економіки, значною мірою залежить від надійності систем захисту від внутрішніх і зовнішніх загроз. За статистикою на мікрорівні в структурі загроз співвідношення між зовнішніми та внутрішніми складає як 20 до 80. Тобто 4/5 всіх проблем виникають у внутрішньому середовищі серед своїх співробітників [38–43].

Підприємство стає банкрутом та ліквідується, у кінцевому підсумку, внаслідок неефективного керівництва і невміння створити команду однодумців. Водночас, потрібно пам'ятати, що вагомим чинником стабільності та розвитку управління економічною безпекою підприємства є кадри, або персонал.

Практика свідчить, що саме людський ресурс є вирішальним чинником конкурентної боротьби. Він включає в себе природні здібності і талант, освіту і набуту кваліфікацію, стан здоров'я і здатність до виживання тощо.

Тому важливим є попередження і зменшення загроз негативного впливу на кадрову безпеку підприємства, зі сторони недостатньо кваліфікованих співробітників та неефективного управління персоналом. Усе це надає проблемі управління кадровою безпекою підвищеної значущості і актуальності.

Однією із суттєвих причин виникнення кризових ситуацій на більшості українських підприємств є відсутність на надійної підсистеми кадрової безпеки та неефективного управління нею. У свою чергу одним із найбільш важливих завдань цієї підсистеми є оцінка рівня безпеки цієї сфери підприємства, яка дозволяє точно виявити больові точки в його діяльності, визначити основні напрями і найбільш дієві способи підвищення ефективності роботи підприємства.

Для створення надійної підсистеми кадрової безпеки підприємства необхідно об'єктивно оцінити вплив навколишнього середовища на його господарську діяльність. Від результатів цієї роботи залежить ефективність гарантування безпеки бізнесу. Навколишнє мікро- і макросередовище може бути сприятливим або створювати небезпеку, загрозу для суб'єктів господарювання. При цьому необхідно врахувати зміну ситуації на ринку праці, безробіття, зміну законодавства в галузі охорони праці, появу нових технологій, недобросовісну конкуренцію тощо.

Оцінку рівня кадрової складової економічної безпеки підприємства необхідно здійснювати на основі аналізу показників, які характеризують якість управління і роботу персоналу, розвиток інтелектуального потенціалу.

В цьому контексті нами узагальнені напрацювання вітчизняних та закордонних науковців, таких як Н. Реверчук [27], В. Ортинського, І. Керницького, З. Живко та ін. [8], І. Чумаріна [38–43] та сформовано перелік ключових показників, які доцільно використати як базу для здійснення оцінки рівня кадрової безпеки в умовах певного підприємства.

Інформаційна база для аналізу показників ґрунтується на використанні таких звітів: «Звіт з праці» (річний і щомісячний), «Звіт з використання робочого часу», «Звіт про стан заборгованості із заробітної плати», «Чисельність окремих категорій працівників та підготовка кадрів» тощо. Готують ці матеріали відповідні служби підприємства: відділи праці і зарплати, кадрів, планово-економічний, бухгалтерія.

Середньоспискова чисельність характеризує загальну кількість працівників, потрібних підприємству з урахуванням відпусток, хвороб та інших невиходів на роботу з поважних причин. На основі планового розрахунку чисельності на підприємстві форму-

ється штатний розпис, обчислюється показник укомплектованості кадрами ($K_{ук}$):

$$K_{ук} = \frac{Ч_{шт}}{Ч_{ф}}, \quad (3.1.)$$

де $Ч_{шт}$ – чисельність працівників згідно зі штатним розписом, чол.;
 $Ч_{ф}$ – фактична чисельність працівників, чол.

Оптимальне (допустиме) значення показника дорівнює 1, що відповідає пороговому значенню показника кадрової безпеки. Якщо значення показника більше ніж 1 або менше від одиниці, то це вказує на додаткову потребу або надлишок персоналу і свідчить про незадовільне значення показника кадрової безпеки.

Показник плинності кадрів ($K_{плин}$) характеризує стабільність трудового колективу:

$$K_{плин} = \frac{Ч_{зв}}{Ч_{с.с}} \quad (3.2)$$

де $Ч_{зв}$ – кількість звільнених з усіх причин працівників, чол.;
 $Ч_{с.с}$ – середньоспискова чисельність працівників, чол.

Що менший показник плинності, то ефективніше працює підприємство, вища його кадрова безпека.

Збільшення показника плинності свідчить про незадовільне управління трудовими ресурсами. Показник плинності аналізується в динаміці.

Оптимальне значення показника дорівнює нулю, однак таке значення буває лише теоретично, бо частина працівників звільняється у зв'язку зі вступом до навчальних закладів, виходом на пенсію, призовом до армії, переїздом в іншу місцевість. Звільнення працівників завжди таїть у собі загрозу втрати комерційної таємниці підприємства.

За віком на підприємствах доцільно виділити працівників віком до 30 років, від 30 до 60 років, понад 60 років.

На нашу думку, найбільшу віддачу можна отримати від працівників віком від 30 до 60 років, коли уже накопичений певний досвід і ефективність роботи – максимальна. Показник вікової

структури персоналу ($K_{\text{вік}}$) характеризує питому вагу працівників від 30 до 60 років у загальній кількості працівників:

$$K_{\text{вік}} = \frac{Ч'}{Ч_{c.c}}, \quad (3.3)$$

де $Ч'$ – чисельність працівників від 30 до 60 років, чол.; $Ч_{c.c}$ – середньоспискова чисельність працівників, чол.

Оптимальне значення показника прямує до максимуму.

Залежно від характеру трудових відносин працівників підприємства поділимо на постійних і тимчасових. До складу постійних працівників належать працівники, для яких праця на підприємстві є основним місцем роботи, та працівників, що працюють за сумісництвом, тобто поєднують роботу на даному підприємстві з роботою в інших місцях. Як показує досвід практичної роботи, суміщення основної діяльності з роботою в іншій організації пов'язано з низькою віддачею працівника і можливим витоком конфіденційної інформації. Що вище значення показника постійності ($K_{\text{пост.}}$), який характеризує частку постійних працівників в їх загальній кількості, то вищий рівень кадрової безпеки:

$$K_{\text{пост.}} = \frac{Ч_n}{Ч_{c.c}}, \quad (3.4)$$

де $Ч_n$ – чисельність постійних працівників, чол.; $Ч_{c.c}$ – середньоспискова чисельність працівників, чол.

Показник стабільності або «відданості» персоналу (середній стаж роботи на підприємстві) (K_c):

$$K_c = \frac{P_p}{Ч_{c.c}}, \quad (3.5)$$

де P_p – загальна сума років роботи на підприємстві всього персоналу, роки; $Ч_{c.c}$ – середньоспискова чисельність працівників, чол.

Оптимальне значення показника прямує до максимуму.

Показник продуктивності праці ($П$) є найпоширенішим показником рівня використання трудових ресурсів:

$$П = \frac{П_n}{Ч_{c.c}}, \quad (3.6)$$

де $П_n$ – обсяг промислової продукції, тис. грн; $Ч_{c.c}$ – середньоспискова чисельність працівників, чол.;

Більше значення цього показника відповідає вищому рівню кадрової безпеки підприємства.

Співвідношення темпів росту заробітної плати та продуктивності праці ($K_{zn/nn}$):

$$K_{zn/nn} = \frac{T_p ЗП}{T_p ПП}, \quad (3.7)$$

де $T_p ЗП$ – темп росту заробітної плати; $T_p ПП$ – темп росту продуктивності праці;

Значення показника повинно бути більшим за 1,01.

Для аналізу стану трудової дисципліни на підприємстві доцільно обчислювати показник рівня трудової дисципліни (K_ϕ):

$$K_\phi = \frac{T_\phi - T_n}{T_\phi}, \quad (3.8)$$

де T_n – неявки на роботу без поважних причин, людино-днів; T_ϕ – фактично відпрацьований фонд робочого часу, людино-днів.

Оптимальне значення цього показника дорівнює 1.

Коефіцієнт мотивації зарплати ($K_{м.з}$), який відображає співвідношення середньої зарплати на підприємстві із середньогалузевою або ринковою:

$$K_{м.з} = \frac{З_\phi}{З_{рин}}, \quad (3.9)$$

де $З_\phi$ – фактична середня зарплата по підприємству, грн; $З_{рин}$ – середньогалузева, середньоринкова зарплата, грн.

Оптимальне значення цього показника дорівнює одиниці. Якщо рівень оплати праці на даному підприємстві відповідає сере-

дньоринковому рівню (ціні праці на ринку), то це забезпечує закріплення кадрів на підприємстві, сприяє підвищенню продуктивності праці і рівня кадрової безпеки.

Рівень забезпечення соціально-культурних потреб працюючих відображає коефіцієнт соціальної захищеності ($K_{c.z}$):

$$K_{c.z} = \frac{B_{on}}{Ч_{c.c}}, \quad (3.10)$$

де B_{on} – вартість наданих соціальних послуг, грн; $Ч_{c.c}$ – середньоспискова чисельність працівників, чол.

Значення цього показника визначається в динаміці і що він більший, то вища ефективність стимулювання персоналу підприємства.

Коефіцієнт освітнього рівня працівників ($K_{o.p}$) обчислюється за формулою:

$$K_{o.p} = \frac{Ч_{в.о}}{Ч_{c.c}}, \quad (3.11)$$

де $Ч_{в.о}$ – чисельність працівників з вищою освітою, чол.; $Ч_{c.c}$ – середньоспискова чисельність працівників, чол.

Коефіцієнт відповідності кваліфікації працівників ступеню складності виконуваних ними робіт (K_{κ})

$$K_{\kappa} = \frac{C_m}{C_{m.p}}, \quad (3.12)$$

де C_m – середній тарифний розряд групи робітників; $C_{m.p}$ – середній тарифний розряд робіт, які вони виконують.

Інтелектуальний рівень працівників підприємства характеризується показником інтелектуального рівня і винахідництва ($K_{инт.п}$). Для виконання наукоємних видів робіт підприємці наймають висококваліфікованих робітників. Їх частка в загальній кількості робітників постійно зростає. Що більше значення коефіцієнта інтелектуального рівня робітників, то вищий рівень інтелектуальної складової безпеки підприємства:

$$K_{\text{інт.р.}} = \frac{Ч_{\text{р.в.к.}}}{Ч_{\text{с.с}}}, \quad (3.13)$$

де $Ч_{\text{р.в.к.}}$ – чисельність висококваліфікованих працівників, чол.; $Ч_{\text{с.с}}$ – середньоспискова чисельність працівників, чол.

За результатами проведеного аналізу визначається рівень кадрової безпеки, здійснюється порівняння з рекомендованими значеннями в динаміці за ряд періодів та у порівнянні з основними конкурентами, що стає підґрунтям як для ідентифікації ключових загроз, так і для удосконалення управління цією підсистемою економічної безпеки.

Виявлені, за результатами проведеного оцінювання, загрози для кадрової безпеки можна впорядкувати за кількома параметрами. Наприклад, О. Ареф'єва та О. Литовченко наводять класифікацію за сферою їх виникнення – внутрішні та зовнішні [2]. І. Швець за етапами взаємодії працівника і підприємства поділяє загрози на ті, які виникають при прийомі на роботу, під час трудової діяльності працівника на підприємстві і при звільненні [44]. Також можна навести класифікацію за видами деструктивної поведінки персоналу, яку пропонує І. Чумарін: порушення техніки безпеки, крадіжки і шахрайство, руйнування згуртованого морального клімату [38–43]. За видами прикладів неефективної роботи відділу по роботі з персоналом Е. Жаріков визначає наступні види загроз: за відсутності моніторингу, хибності будь-яких висновків, відсутності системи контролю [9].

Окрім зазначеного, Л. Лапіцкая пропонує декілька класифікаційних ознак [18]: перша – за характером загроз, що утворюються групами ризику (рис. 3.3); друга – за величиною ризику: допустимого ризику, критичного ризику і катастрофічного ризику; третя – за можливістю страхування: ті, що страхуються і не страхуються.

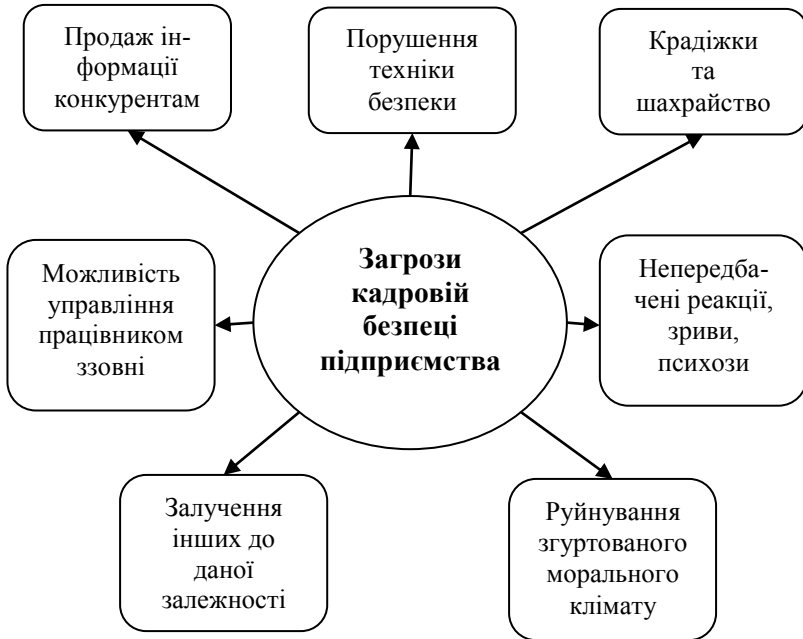


Рис. 3.3. Класифікація загроз кадровій безпеці за характером їх впливу

Іншими дослідниками обґрунтовано, що існує декілька інших класифікаційних ознак:

- за часом виникнення: нерегулярні і постійні;
- за можливими наслідками: прості і альтернативні;
- за можливістю прогнозування: прогнозовані і непрогнозовані;
- за часом реагування: попереджувані, поточні і запізнені.

Кожна із поданих вище класифікацій загроз для кадрової безпеки на мікрорівні є важливою і потрібною для цілей управління, але найбільш придатною для планування певних дій в межах системи підсистеми є все таки поділ на зовнішні та внутрішні.

Зовнішні загрози – це дії, явища або процеси, які не залежать від свідомості співробітників і задають збитки. До внутрішніх належать навмисні дії або дії, які склалися внаслідок необережності або недбальства персоналу (рис. 3.4).

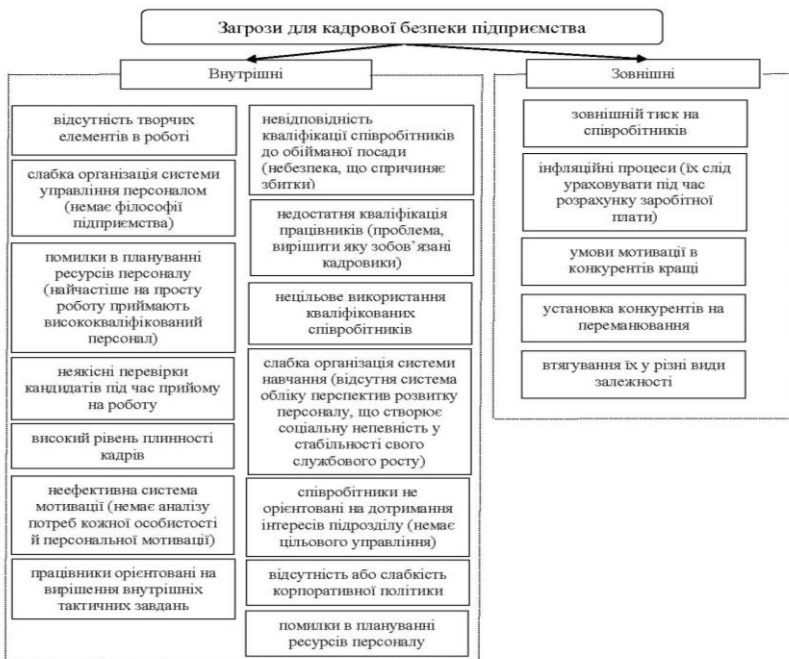


Рис. 3.4. Характеристики внутрішніх і зовнішніх загроз кадровій безпеці підприємства

Безперечно, що в умовах кожного конкретного підприємства можна визначити та ідентифікувати іншу сукупність загроз, але сформована вище є усереднена і характерна для більшості вітчизняних підприємств.

Охарактеризувати вплив кожної із визначених загроз є складно, тому зосередимо увагу лише на окремих. Перш за все приділимо увагу загрозі, яка спричинена неефективною системою мотивації праці. Можна констатувати той факт, що в Україні основною формою матеріальної винагороди за працю є зарплата. Це означає, що гроші є головним мотиватором, хоч їхня роль є не однаковою для різних суспільних груп. Особливо важливу роль відіграє заробітна плата в суспільствах із низьким рівнем економічного розвитку. В міру зростання матеріального добробуту в суспільстві значення матеріальної винагороди за працю зменшується і набирають

ваги інші види винагород. Однак у будь-якому суспільстві зацікавленість працівників лише оплатою праці означає малу привабливість, престижність праці або відсутність інших видів винагород. У сучасній економіці штучне заниження зарплати є могутнім дестабілізуючим чинником безпеки підприємницької діяльності та управління нею.

До складу заробітної плати працівників в Україні входять основна заробітна плата, додаткова і заохочувальні та компенсаційні виплати. При цьому додаткова заробітна плата складає більшу частину загального розміру оплати праці. Посадовий оклад, тобто основна заробітна плата, складає в середньому 30–35% від загальної суми оплати праці. Це породжує нестабільність розміру заробітної плати працівників, а також їх демотивацію до праці через невпевненість в отриманні гідної винагороди за нею.

Непоодинокими є випадки, коли система нарахування додаткових виплат, яка існує в організації, недостатньо ефективно стимулює працівників, тому що до них належать фіксовані доплати, які носять систематичний характер (за кваліфікацію) або компенсаційні виплати (матеріальна допомога), що не сприяє мотивації працівників краще, скоріше, ефективніше виконувати свої обов'язки і приносити більше користі підприємству.

Вагомим індикатором кадрової безпеки підприємства є відповідність мінімальної заробітної плати прожитковому мінімуму. Відповідно до стандартів Європейської соціальної хартії, мінімальна зарплата повинна становити не менше ніж 2,5 прожиткового мінімуму [30]. Якщо взяти до уваги реалії нашої країни, то лише в останні кілька років мінімальна заробітна плата наблизилась до прожиткового мінімуму, але більш важливим є той факт, що з метою зменшення навантаження на фонд заробітної плати масовим є явище виплати саме мінімальної заробітної плати. Окрім цього, через недосконалість тарифної системи, яка тривалий час не змінювалась, знизилась престижність висококваліфікованої праці. Низький рівень заробітної плати використовується для приховування фонду оплати праці. Не секрет, що сьогодні частина зарплати виплачується «у конвертах», унаслідок чого працівник позбавляється відповідного соціального захисту і приречений, у майбутньому, на отримання мізерної пенсії. Отже, мінімальна зарплата не виконує властивих їй функцій, не забезпечує працездатне населен-

ня потрібними коштами для відтворення робочої сили і є стримувальним чинником ефективної організації системи кадрової безпеки підприємства.

Для більшості вітчизняних підприємств є характерна невисока диференціація розміру доходів працівників, що виконують різні функції. Тобто головні виконавці функцій організації отримують заробітну плату, що за розміром не дуже відрізняється від заробітної плати працівників непромислового персоналу (прибиральників приміщень, водіїв та ін.). Звідси недостатня диференціація заробітної плати негативно впливає на рівень кадрової безпеки.

Окремо потрібно наголосити на тому факті, що при розрахунку заробітної плати і прогнозуванні її динаміки не враховуються інфляційні процеси, що спричиняє виникнення зовнішніх загроз для кадрової безпеки підприємства.

Низька мотивація і недостатність кваліфікованих кадрів є внутрішньою загрозою кадровій безпеці організації. Це спричиняє високу плінність кадрів, що сприяє нестабільності колективу, росту потреби в пошуку і навчанні нових якісних кадрів, підвищенні ймовірності втечі конфіденційної інформації.

Звільнення висококваліфікованих працівників породжує потребу в заміщенні вакансій, що утворюються, але пошук кандидатів з потрібним рівнем знань і навичок потребує багато зусиль і часу.

Практична діяльність підприємств свідчить, що значення людського потенціалу усвідомлені власниками ще недостатньо. Добір кадрів відбувається спонтанно, інколи з кола близьких чи знайомих людей. Дружні стосунки, глибока спеціалізація персоналу спочатку позитивно впливає на становлення фірми. Проте, ситуація суттєво змінюється, коли підприємство досягає певного успіху, розширяється.

Перш за все виникає проблема з дотриманням дисципліни, без якої не може ефективно функціонувати підприємство. По-друге, в умовах гострої конкуренції зростає вимога до підвищення професіоналізму працівників, виникають юридичні проблеми із звільненням. Демократизація суспільних процесів призвела до того, що на переважній більшості вітчизняних підприємств немає посадових інструкцій. Проте, саме вони дозволяють вирішити низку важливих проблем: виокремити коло питань, за які працівник несе особисту відповідальність; чітко сформулювати вимоги до знань

і вміння працівників, визначити критерії ефективності їх роботи, що дозволяє юридично чітко розв'язати проблему відносин між найманим працівником і роботодавцем, обґрунтувати розмір заробітної плати; сформувати в керівника уявлення про фактичну організаційну структуру підприємства, виявити «вузькі» місця.

Необхідно наголосити, що відсутність посадових інструкцій не дає можливості роботодавцеві визначити оптимальну кількість працівників, розв'язати конфлікти, пов'язані з розміром заробітної плати, незаконним звільненням. КЗпП України передбачає звільнення працівника у трьох основних випадках: порушення дисципліни, скорочення штатів і службова некомпетентність. Проте довести останню без чітко вписаних у посадових інструкціях вимог до знань, переліку виконуваних робіт, критеріїв ефективності досить складно.

Загроза для деяких підприємств та організацій виникає тоді, коли вони залежать від діяльності декількох ключових співробітників. Частина співробітників може зловживати при виконанні своїх функцій – це бухгалтери, касири, торговельні представники, експедитори. Інколи на стан справ у фірмі може сильно вплинути звільнення, хвороба провідних спеціалістів.

Різноманітні загрози для підприємства можуть надходити від кожного працівника, але існують певні групи ризику, які об'єднують типові сукупності осіб за спільними ознаками. Тобто група ризику серед персоналу – це сукупність працівників, що потенційно мають схильність своїми діями або поведінкою нанести ушкодження підприємству [19].

Така поведінка пов'язана з бажанням людини піти від реальності шляхом зміни стану своєї свідомості. Відхід від реальності завжди супроводжується сильними емоційними переживаннями. Людина фактично залежить не від самого предмета, а від емоцій. Емоції є складовою частиною залежності. Посадивши людину на «емоційний гачок», їм дуже легко керувати [44].

Ризик для кадрової безпеки в цьому контексті полягає в наступному:

– можливість управління працівником, що входить до групи ризику, ззовні, що може бути спрямоване на дестабілізацію організації (одержання секретів, відведення клієнтів і т.д.);

- постійні спроби залежного поширити вплив своїх згубних пристрастей, звичок на оточуючих, пошук або формування їм кола однодумців, тобто збільшення кількості представників групи ризику в організації;

- задоволення своїх залежностей індивідом за рахунок часових і матеріальних ресурсів роботодавця;

- руйнування стабільного працездатного колективу (команди);

- схильність до злочинних дій і порушень або ради, або внаслідок задоволення своїх залежностей [38–43].

Групи ризику можуть належати до будь-якого рівня управління підприємством і характеризуватися як девіантною, так і недобросовісною поведінкою.

Наприклад, до тих, що мають девіантну поведінку, належать алкоголіки, наркомани, гравці, члени релігійних новоутворень і носії інших залежностей. До «недобросовісних» належать: шахраї, члени фінансових пірамід і саме недобросовісні працівники підприємства. Особливу шкоду можуть завдати ті з них, що працюють у топ-менеджменті підприємства.

Для ідентифікації працівників на предмет їх приналежності до однієї із груп ризиків потрібно взяти до уваги деякі ознаки правопорушення в поведінці співробітника і його неправомірні дії:

- незвичне поводження працівника (нервозність, дратівливість, занепокоєння, перепади настрою, підозріла покірність тощо);

- поява нестандартних даних і відхилення від звичайних (середніх) показників у бухгалтерських й/або інших документах;

- зникнення окремих форм обліку та звітності (зокрема бланків) у бухгалтерській або іншій документації;

- проведення сторонніх фінансових документів;

- поява підроблених підписів і підчищень (виправлень) даних у звітній документації. 6) Надання ксерокопій документів замість оригіналів;

- різке поліпшення матеріальних можливостей співробітника, необґрунтоване його легальною діяльністю [27].

Недобросовісній поведінці рядових працівників можна запобігти за допомогою безпосереднього спостереження, використання технічних засобів контролю (наприклад, відеокамер і спеціального

програмного забезпечення комп'ютерів, що дозволяє перевіряти, чим займаються співробітники на робочому місці) і на основі вимірювання результатів праці (наприклад, кількості вироблених деталей). Що стосується керівників, то безпосередній моніторинг їхньої поведінки малоефективний, а оцінити результати їхньої роботи досить важко.

Окрім зазначеного, на нашу думку, доцільно особливу увагу приділити профілактиці правопорушень зі сторони персоналу яку уможлиблюють:

1. Висококваліфікований кадровий менеджмент, використання сучасних технологій, персональна робота з кадрами й управління поведінкою персоналу.

2. Здійснення зовнішнього й внутрішнього аудиту діяльності керівних кадрів, розподіл їхніх функцій.

3. Періодичне відновлення повноважень (анулювання дозволень, переділ функціональних обов'язків тощо).

4. Доручення комерційних справ не одному фахівцеві, а декільком – на конкурентній основі.

5. Розробка й дотримання сучасних методів охорони власності (майна) підприємства, зокрема коштів, інформаційних комунікацій.

6. Оптимізація системи фінансового обліку та звітності.

7. Обмежити доступ (допуск) співробітників до документів фінансової та бухгалтерської звітності.

Беручи до уваги подану вище класифікацію загроз за часом їх виникнення, авторства І. Швець, доцільно сконцентрувати увагу підсистеми кадрової безпеки на таких моментах [3].

- при прийомі рекомендовано вживати заходів для розпізнання девіантних прихильностей кандидата; проводити перевірку його попередньої діяльності для виявлення схильностей, що потенційно можуть завдати шкоду підприємству; перевіряти документацію щодо кваліфікації та акредитації працівника; перевіряти рекомендації і відгуки від попередніх роботодавців; під час анкетування і інтерв'ю ретельно спостерігати за даними та реакціями кандидата та ін.;

- під час роботи рекомендовано проводити постійний моніторинг діяльності персоналу – аналізувати не тільки внутрішні показники діяльності підприємства, але й ті, що характеризують

його в ситуації на ринку (рентабельність, вартість акцій та ін.). Також необхідно уважно спостерігати за відносинами в колективі для виявлення можливості негативного впливу. Відповідальність за процеси діяльності в підприємстві і рівень влади рекомендується розподіляти між декількома працівниками для зменшення можливості маніпуляцій;

– щоб запобігти негативним наслідкам у вигляді загроз кадровій безпеці підприємства після звільнення працівника, треба заздалегідь попіклуватися про заходи, що забезпечать «безболісне» звільнення. До таких заходів можна віднести ті, що спрямовані на «пом'якшення» переживання факту звільнення для працівника, і заходи переважно адміністративного характеру, що безпосередньо забезпечують економічний захист підприємства в цьому випадку. До першої групи належать як адміністративні, так і психологічні заходи, які допомагають створити у працівника, що звільняється, якомога більш лояльне відношення до підприємства, до ситуації звільнення і т.д. До другої групи заходів належать підписання документів (при укладенні трудового договору), що містять інформацію про узгодження працівника з обов'язком зберігати конфіденційну інформацію.

Діапазон конкретних методів та процедур попередження загроз кадровій безпеці дорівнює діапазону всіх тих загроз, що виникають. Найбільш поширені, «загальні», це – чітке ведення бухгалтерського та фінансового обліку діяльності, аудит документації, ретельна увага до відбору персоналу та його стану, аналіз показників рентабельності та прибутковості діяльності підприємства.

З метою уникнення такої загрози як «дестабілізація організації, руйнування стабільного працездатного колективу (команди)» доцільним є проведення ретельного відбору персоналу, нагляд за відносинами в колективі, за комунікаціями на підприємстві, перевірка всіх працівників, які викликають підозру, на належність до будь-якої групи ризику, статистичний нагляд та аналіз руху персоналу.

Загрозу «погіршення дисципліни в колективі, порушення техніки безпеки та правил внутрішнього трудового розпорядку» можна нейтралізувати через нагляд за взаєминами в колективі, комунікаціями на підприємстві, перевірку всіх працівників, які викликають підозру, на належність до будь-якої групи ризику, запобіган-

ня та розв'язання будь-яких конфліктів у колективі, чітку регламентацію субординації і трудового розпорядку.

Для протидії загрози здійснення таємної протизаконної діяльності на підприємстві доцільно активізувати контроль за всіма комунікаціями на підприємстві, увагу сконцентрувати на взаєминах у колективі, вимогах щодо обов'язкової звітності про будь-які ділові операції в межах підприємства, провести аудит документації.

З метою унеможливлення утворенню конфліктів необхідно здійснювати нагляд за взаєминами в колективі, за діяльністю колективу й окремих працівників, чітко регламентувати взаємини останніх, використовувати послуги медіаторів, сприяти згуртованості колективу та підвищенню лояльності персоналу.

Як зазначалось вище, кадрову безпеку послаблює неефективна система мотивації персоналу підприємства. В Україні часто стимулювання зводиться до примітивної концепції «батога і пряника». Водночас, потрібно взяти на озброєння інші методи. Так, якщо працівники роблять те, що від них вимагає керівник, то вони повинні заохочуватися бажаними для них стимулами, які спрямовані на задоволення духовних і моральних потреб: почесними грамотами, значками, визнанням, більш цікавою роботою, просуванням по службі, наданням можливості поліпшити житлові умови, наданням чергової відпустки у зручний для них час, стажуванням за кордоном тощо. І навпаки, у разі небажаної діяльності підлеглих, керівники повинні вдаватися до різних форм покарань: попередження, догани, переведення на нижчу посаду, звільнення тощо. Ефективність мотивації залежить від того, наскільки моральне стимулювання підкріплене матеріальним і чи величина винагороди відповідає особистому досягненню працівника, кількості докладених зусиль.

Окрім зазначеного вище, методи мотивації можна поділити: на прямі економічні, непрямі економічні і негрошові [4]. Суть прямих економічних методів мотивації полягає в тому, щоб шляхом впливу на працівника або колектив працівників – оплатою праці, дивідендами, преміями, участю в прибутках, створювати ефективний механізм підвищення продуктивності праці, а відповідно – безпеки підприємства. До непрямих економічних методів належать пільгове харчування, пільгове користування транспортом, доплати за стаж роботи та інші фінансові важелі.

Негрошові – це методи, які шляхом застосування гнучких робочих графіків, створенням належних умов для захисту здоров'я і безпеки праці, наданням відпустки у зручний час, забезпеченням можливостей для зростання професійної майстерності та реалізації здібностей працівників, які в сукупності підвищують ефективність управління трудовими ресурсами і відповідно рівень кадрової безпеки підприємства.

Важливою рекомендацією для забезпечення високого рівня кадрової безпеки є приділяти більше уваги розвитку прихильності персоналу. Дослідження показали, що лояльні люди мають більш високий рівень поваги до себе і інших, готові приймати нове без паніки та опору, вони враховують інтереси інших людей і менше піддаються впливу пропаганди, умовностей і маніпуляції [46].

Поруч із необхідністю реалізації заходів щодо нейтралізації загроз, окремі ризики, що пов'язані з кадровою безпекою, доцільно страхувати. До таких ризиків належать:

- імовірні втрати в результаті помилок і прорахунків співробітників підприємства;
- імовірні втрати в результаті передачі нелояльними співробітниками підприємства комерційної інформації конкурентам;
- імовірні втрати в результаті невиконання обов'язків субпідрядниками, поставниками, партнерами;
- імовірні втрати в результаті можливої смерті або хвороби керівника або провідного співробітника підприємства.

Реалізація методів попередження загроз та зниження рівня ризиків для кадрової безпеки повинна забезпечити високу ефективність системи менеджменту персоналу та сприяти підвищенню фінансових результатів виробничо-комерційної діяльності підприємств.

3.3. Концептуальні основи управління кадровою безпекою підприємства

Управління кадровою безпекою пов'язано з нейтралізацією ризиків, попередженням виникнення загроз та кризових явищ, а також у забезпеченні ефективності управління персоналом за рахунок формування у персоналу властивостей й характеристик, що

створюють умови для досягнення інтересів власників та самого персоналу, їх захист від внутрішніх і зовнішніх загроз.

Щоб сформувавши концептуальні основи управління кадровою безпекою на мікрорівні потрібно взяти до уваги ті положення, які були нами викладені у попередніх підрозділах, які коротко можна викласти наступним чином:

- кадрова безпека є однією із функціонального складових економічної безпеки підприємства, тобто підсистемою в комплексній системі економічної безпеки підприємства;
- мету кадрової безпеки можна визначити як створення умов для забезпечення конкурентоспроможності підприємства, ефективне використання трудового потенціалу, зниження ризиків, нейтралізація зовнішніх та внутрішніх загроз;
- на рівень кадрової безпеки впливають різноманітні фактори, джерелом походження яких є внутрішнє і зовнішнє середовище;
- об'єктом підсистеми кадрової безпеки на підприємстві є працівник як індивідуум, колектив, людський капітал, система управління персоналом;
- суб'єкти кадрової безпеки поділяються на зовнішні та внутрішні.

Спираючись на вище подані позиції, нами сформовано концепцію управління кадровою безпекою підприємства (рис. 3.5), інші складові якої будуть охарактеризовані нижче.

Завдання кадрової безпеки визначаються, по-перше, залежно від рівнів управління організацією, по-друге, залежно від типів загроз, і, по-третє, залежно від груп ризику. При формуванні завдань важливо врахувати, що кадрова безпека є комбінацією складових, пов'язаних між собою складними і часто завуальованими зв'язками.

Основні загальні завдання кадрової безпеки підприємств можна окреслити наступним чином:

- участь у формуванні кадрової стратегії підприємства, процесах планування людських ресурсів, інформаційній, фінансовій політиці, розвитку і оцінці персоналу;
- формування вимог до співробітників підприємства щодо безпеки;
- складання відповідної нормативної документації для співробітників служби управління кадрами;

- складання нормативної документації для інших співробітників підприємства з метою дотримання кадрової безпеки;
- проведення інформаційно-роз'яснювальної роботи серед співробітників підприємства;
- виявлення, попередження і припинення небажаних дій з боку співробітників підприємства, що можуть спричинити завдання шкоди його інтересам;
- проведення заходів, спрямованих на унеможливлення заняття певними особами посад, зловживаючи якими, вони можуть завдати своїми діями шкоди підприємству;
- моніторинг напрямків забезпечення кадрової безпеки.



Рис. 3.5. Концепція управління кадровою безпекою підприємства

Досягнення кожного із вище поданих завдань є можливим лише за умови дій відповідно до чітко визначених принципів. Поруч із загальною сукупністю принципів, які застосовуються стосовно процесу гарантування економічної безпеки і були нами розглянуті у першому розділі, кадрова безпека має деякі відмінні, притаманні виключно для цієї функціональної складової [21]:

1. Взаємозалежність та взаємообумовленість між функціональною стратегією кадрової безпеки та загальною стратегією розвитку підприємства. У такому контексті політика кадрової безпеки спрямована на кадрове забезпечення реалізації загальної стратегії.

2. Стабільність та гнучкість. Політика кадрової безпеки повинна поєднувати в собі дві протилежні засади – бути досить стабільною (оскільки саме зі стабільністю пов'язані певні очікування працівника) та водночас бути досить динамічною або гнучкою (змінюватися відповідно до зміни стратегії підприємства, політичної й економічної ситуації). Стабільними мають бути цінності, переконання й норми, що визначають поведінку працівників, а також установки поведінки роботодавців стосовно забезпечення стабільної зайнятості персоналу, а це саме ті сторони, які орієнтовані на врахування інтересів персоналу й мають відношення до організаційної культури підприємства. З огляду на цю вимогу політика кадрової безпеки має бути зваженою та заснованою на врахуванні того, як її реалізація позначиться на поведінці працівників, до яких соціально-психологічних втрат вона може призвести. У протилежному випадку, якщо політика кадрової безпеки не буде відповідати названій вимозі, вона може бути занадто рішучою, можливо, навіть на початку негуманною до працівників з використанням формального підходу, з чітким вираженням лише інтересів підприємства.

3. Економічна обґрунтованість. Формування політики менеджменту кадрової безпеки має спиратися на економічні розрахунки, які виходять з реальних можливостей певного підприємства [33].

4. Індивідуальний підхід до кожного зі своїх працівників та значимість ролі людських ресурсів підприємства.

5. Орієнтація на довготривале планування забезпечення безпеки підприємства.

6. Соціальна спрямованість. Політика кадрової безпеки має орієнтуватися на одержання не тільки економічного, але й соціального ефекту та забезпечувати належний соціальний захист працівників.

7. Активність. Політика менеджменту кадрової безпеки сучасної організації має бути спрямована на активний вплив на робочу силу в усіх фазах її відтворення [16]. Наприклад, у фазі формування робочої сили будь-яка організація не може обмежуватися

роллю пасивного споживача робочої сили, а має розширювати межі власної діяльності в напрямі пошуку й залучення кваліфікованих працівників, забезпечувати подальший їхній розвиток у межах організації, а також закріплення на робочих місцях для тривалої зайнятості тощо.

Перелік показників для оцінки поточного рівня кадрової безпеки нами був сформований і охарактеризований у попередньому підрозділі, але їх можна об'єднати у певні головні групи критеріїв кадрової безпеки:

- 1) показники чисельного складу персоналу і його динаміки;
- 2) показники кваліфікації та інтелектуального потенціалу;
- 3) показники ефективності використання персоналу;
- 4) показники якості мотиваційної системи.

У Кодексі законів про працю України зазначено ряд документів, що безпосередньо впливають на безпеку підприємства, і служба персоналу зобов'язана забезпечити їх наявність, правильність, працездатність і відсутність негативних юридичних наслідків. До таких документів, в першу чергу, належать:

- трудовий договір;
- правила внутрішнього трудового розпорядку;
- договір про повну індивідуальну (колективну) матеріальну відповідальність;
- документація з охорони праці та ін. [38-43].

Відповідно до розглянутих і охарактеризованих у попередньому розділі видів загроз, пропонуємо визначити такі основні заходи забезпечення кадрової безпеки підприємства: економічні, технологічні, організаційні, соціально-психологічні, адміністративні та дисциплінарні (рис. 3.6) [38–43].

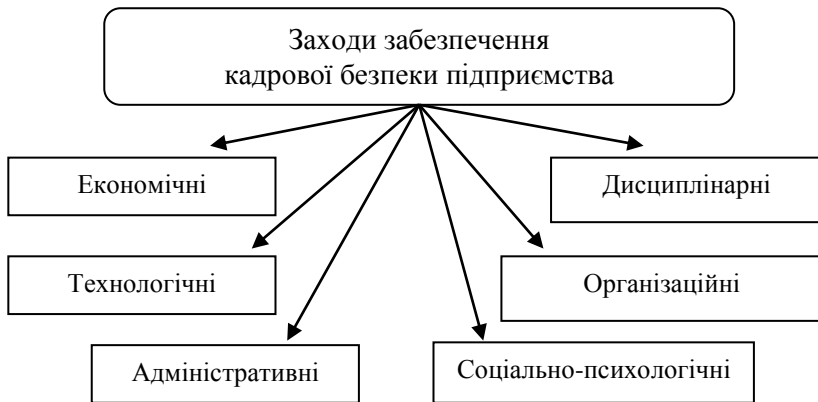


Рис. 3.6. Перелік заходів для забезпечення кадрової безпеки підприємства

Під економічними заходами забезпечення кадрової безпеки слід, в першу чергу, розглядати такі, які створюють сприятливе матеріально-мотиваційне поле для співробітників організації та не спонукатимуть їх до переходу до підприємств-конкурентів зокрема у випадку більш привабливих умов оплати праці. Відповідно як превентивні заходи на підприємстві слід регулярно здійснювати перерахунок заробітної плати та забезпечувати її співрозмірність до роботи, що виконується.

Соціально-психологічні заходи становлять собою сукупність специфічних способів впливу на міжособистісні стосунки і зв'язки, соціальні процеси, що виникають у трудових колективах. З позиції забезпечення кадрової безпеки такі заходи повинні ґрунтуватися на створенні сприятливого соціально-психологічного клімату, формуванні стабільного колективу, персональній роботі з кадрами й управління поведінкою персоналу, вирішенні індивідуальних проблем кожного співробітника з метою гуртування персоналу та відчуття колективізму.

В таких колективах, як правило, співробітники цінують свою роботу, прагнуть продовжувати працювати й надалі, інколи навіть не зважаючи на привабливіші умови праці у конкурентів.

Суть технологічних заходів полягає у розробці чітких правил роботи із секретною інформацією і документами. Дані правила

роботи повинні бути доведені до відома усіх працівників, які мають доступ до конфіденційного характеру інформації. В деяких випадках дана норма правил роботи, а особливо зобов'язання щодо дотримання принципу нерозголошення інформації, може бути обговорена та прописана в трудовому контракті, що укладається при прийомі на роботу.

До технологічних методів належить також розробка й впровадження сучасних форм охорони власності (майна, інформації) підприємства, зокрема баз даних, програм і т.д.

Адміністративні заходи з позиції забезпечення кадрової безпеки підприємства пропонуємо трактувати як сукупність заходів з перевірки персоналу на етапі прийому на роботу, здійснення періодичного внутрішнього і зовнішнього аудиту діяльності персоналу та дотримання низки вимог у випадку звільнення персоналу.

Організаційні заходи забезпечують необхідні умови функціонування організації, а також створюють межі, в яких вона функціонує та розвивається. До них, зокрема, можна віднести розподіл функцій керівних кадрів, періодичне відновлення повноважень (анулювання доручень, переділ функціональних обов'язків тощо), доручення справ не одному фахівцеві, а декільком – на конкурентній основі.

Сферою застосування дисциплінарних заходів є передбачення юридичних та дисциплінарних зобов'язань і відповідальності щодо роботи з окремою категорією інформації. Застосування дисциплінарних заходів матиме місце у разі недотримання зазначених вимог шляхом стягнення, зауваження, висловлення догани, переміщення посадових осіб, звільнення тощо.

Запропонований поділ заходів на означені групи є досить умовним, оскільки всі вони тісно взаємопов'язані. Без сумніву, менеджери із персоналу можуть продовжити даний перелік, що й треба зробити після аналізу стану кадрової роботи з погляду безпеки щодо забезпечення ефективності трудових відносин на підприємстві.

Поруч із розробленими варіантами застосування того чи іншого виду заходів, важливим є встановлення чіткої послідовності реалізації кроків для підтримки необхідної для досягнення мети рівня кадрової безпеки (рис. 3.7).



Рис. 3.7. Алгоритм реалізації заходів гарантування кадрової безпеки на підприємстві

На перших стадіях процесу забезпечення кадрової безпеки здійснюється аналіз джерел негативних факторів впливу та оцінка можливої шкоди від таких дій. З-поміж основних негативних впливів на кадрову безпеку підприємства виокремлюють недостатню кваліфікацію працівників тих чи інших структурних підрозділів, їхнє небажання або нездатність забезпечити реалізацію інтересів власників, персоналу та суб'єктів зовнішнього середовища. Це може бути зумовлене низьким рівнем управління персоналом, браком коштів на оплату праці окремих категорій персоналу чи нерациональним їх витрачанням тощо.

Процес планування та управління персоналом, спрямований на гарантування належного рівня кадрової безпеки, має охоплювати організацію системи підбору, найму, навчання й мотивації праці необхідних працівників, включаючи матеріальні та моральні стимули, престижність професії, волю до творчості, забезпечення соціальними благами та політику звільнення.

Важливим етапом в процесі гарантування кадрової безпеки підприємства є набір кадрів. Зазначимо, що набір кадрів розглядають як процес запобігання негативним впливам на кадрову безпеку підприємства через ризики і загрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами загалом.

В найбільш загальному випадку набір кадрів – процес пошуку потенційних працівників і формування бази даних про них для наступного залучення на вакантні або на ті, що стануть вакантними, посади і робочі місця.

Основою оптимального набору кадрів повинно бути: з одного боку наявність формальних вимог до вакантної посади, а з іншого – об'єктивної інформації про кандидатури на цю посаду.

При дослідженні придатності кандидатів до роботи в організації використовують: аналіз документів, біографічних даних, кваліфікаційні співбесіди, практичне випробування вмінь кандидата, тестові випробування, графологічні експертизи, перевірки на «детекторі брехні», центри оцінювання. Вибір конкретних методів залежить від прийнятої в організації процедури, а також від особливостей робочих місць, на які добирають кандидатів.

Етапи і процедури відбору персоналу охоплюють: перевірку рекомендацій; психологічне тестування; взаємодію зі службою безпеки.

Порядок перевірки кандидата включає в себе:

- збір і перевірку офіційної інформації;
- отримання інформації з баз даних;
- отримання інформації по лінії МВС (знаходження у розшуку і наявність судимостей);
- отримання відгуків з попередніх місць роботи по офіційних каналах;
- проведення співбесіди;
- перевірка на поліграфі (детекторі брехні);
- спостереження за поведінкою.

При перевірці кандидата збирається наступна інформація:

- адресні, анкетні та паспортні дані;
- про злочини та адміністративні проступки, вчинені ним у минулому;
- судові процеси, в яких брав участь;
- раніше взяті фінансові зобов'язання;

- зв'язок з криміналом;
- характеристика ділових контактів і впливових родинних зв'язків;
- інформація про людські слабкості, згубні пристрасті, шкідливі звички;
- дані про друзів, місця проведення дозвілля.

Однією з ефективних процедур відбору є вивчення рекомендацій з минулих місць роботи кандидата, а також перевірка цих відомостей.

Існують різні форми отримання характеристик від зовнішніх суб'єктів. Іноді кандидат з власної ініціативи приносить «рекомендацію» або менеджер з персоналу сам звертається до попереднього працедавця з певними запитаннями щодо претендента на посаду. Варто почати з того, що попросити кандидата на посаду описати три чотири останні реальні (не за трудовою книжкою) місця роботи із зазначенням імен керівників, адрес і контактних телефонів. Доцільно, щоб менеджери з персоналу отримали усну характеристику на колишнього працівника від різних посадових осіб за рівнями. При цьому менеджер з персоналу зв'язується за місцем колишньої роботи зі своїм колегою і просить стисло описати позитивні й негативні якості претендента. Таким чином, характеристики чи рекомендації, компетентна зовнішня і незалежна думка про кандидата є вагомими для ухвалення рішення про його працевлаштування, і нехтувати ними не варто.

Окрім психологічних тестів професійного відбору, застосовують також певні методи відбору з огляду на претендентів, особливо коли потрібно з'ясувати: залежність їх від наркотиків і алкоголю, пристрасть до азартних ігор, схильність кандидата до здійснення протиправних дій, зухвалих і необдуманих вчинків у разі виникнення певних обставин, інші ознаки, що свідчать про морально-психологічну нестійкість кандидата.

Перевірити вміння претендента можливо лише організувавши випробовування. Практичне випробування вмінь кандидата полягає у наданні йому певних завдань і оцінюванні якості їх виконання.

Застосування графологічних експертиз у процесі дослідження придатності кандидата до роботи в організації полягає в аналізі зразків його почерку і визначенні на цій основі якостей особистості.

Метод центрів оцінювання – це оцінювання експертами претендентів із комплексним використанням системи спеціальних методик. Застосовують їх як при відборі працівників в організацію, так і у процесі їх трудової діяльності.

1. Правило відносної більшості. Кожний експерт видає свій голос найкращому, на свою думку, претенденту. Кандидати ранжуються за кількістю відданих їм голосів. Посаду отримує кандидат, який набрав найбільшу кількість голосів. Такий спосіб можна використовувати при невеликій кількості претендентів (до чотирьох). Уже при наявності трьох кандидатів рішення може суперечити думці більшості.

2. Процес вибору працівника відбувається у декілька етапів (турів). За результатами першого туру, проведеного за першим правилом, виключають претендента(ів) з найменшою сумою голосів. Операцію повторюють доти, поки не залишиться декілька претендентів, для яких можна без застережень застосувати правило відносної більшості.

3. За правилом Борда, кожен член експертної групи оцінює всю множину з p претендентів і формує список від найкращого до найгіршого. Претенденти отримують $p-1$ очок за перше місце, $p-2$ – за друге, і так далі, а останній не отримує нічого. Перемагає претендент, який отримав найвищу оцінку. Таке правило допомагає більш якісно оцінити безпосередньо професійні якості.

Метод аналізу ієрархій (МАІ) передбачає структурування проблеми у вигляді ієрархії або мережі. Процес побудови ієрархії базується на способі мислення людини – складні задачі розбивати на простіші підзадачі. Перевагами цього методу є простота, надійність і наочність. При використанні МАІ кількісні та якісні оцінки розглядаються в сукупності, а проблема суб'єктивних суджень розв'язується завдяки використанню попарних порівнянь і визначенню їх ваг на основі спеціальної шкали. Цей метод використовують для відбору персоналу високої кваліфікації.

При відборі претендентів на вакантні посади ймовірність недопущення помилок становить: при застосуванні тестів – 45%. лише анкетних даних – 38%. поведінкового інтерв'ю – 61%, неструктурованого інтерв'ю – 9%, центри оцінювання – 87%.

Узагальнюючи вище подане, можна стверджувати, що процес захисту підприємства від небезпеки починається на етапі під-

бору працівників на існуючі вакансії. І цей процес захисту існує безперервно у весь період функціонування підприємства. Ефективність цього процесу забезпечується використанням різних методів набору персоналу.

Наступним напрямком роботи підсистеми кадрової безпеки є «адаптація» персоналу. Помилка багатьох служб управління персоналом полягає в тому, що зазначену кадрову технологію досліджують тільки на професійному й побутовому рівнях. Час адаптації – це не два місяці випробувального терміну – вони індивідуальні для кожної особистості й кожної соціальної групи працівників.

Контроль як елемент кадрової безпеки – це комплекс засобів, установлений для персоналу (зокрема й для адміністрації), регламент, обмеження, режими, технологічні процеси, оцінювальні, контрольні та інші операції. Цей комплекс безпосередньо спрямований на ліквідацію можливостей заподіяти збитки [38–43]. Служба безпеки у даному напрямі повинна організувати демократичну й прозору систему атестації персоналу, пов'язуючи її з діючою системою оплати праці. Саме справедливість в оплаті праці – основна домінанта формування патріотизму, причому важливо не скільки платять, а наскільки це обґрунтовано й справедливо всередині колективу.

Одним з традиційних способів оцінки персоналу є регулярна атестація персоналу, яка є процесом оцінки ефективності виконання співробітником своїх посадових обов'язків. Фактично на вітчизняних підприємствах, атестація персоналу проводиться так званою атестаційною комісією, в яку входить безпосередній керівник працівника, що атестується, співробітник кадрової служби, один із керівників підприємства і представник профспілки. Атестація повинна проводитися плановірно [17].

Розрізняють наступні види атестації:

- регулярна;
- основна;
- розгорнута (раз у 3-5 років);
- регулярна проміжна;
- спрощена;
- орієнтована на оцінку підсумків поточної роботи

(для керівників і спеціалістів 1 раз на рік, а для деяких категорій – 2 рази на рік і частіше);

- нерегулярна;
- спричинена надзвичайними обставинами (несподівана вакансія, незапланована можливість пройти курс підвищення кваліфікації);
- при введенні нових умов оплати праці.

Проведенню атестації повинна передувати підготовча й організаційна робота. Кадрова служба підприємств, організацій чи установи готує пропозиції щодо складу атестаційної комісії, термінів і графіків проведення атестації, визначає кількість і складає списки працівників, котрі підлягають атестації, роз'яснює мету і порядок проведення атестації, здійснює підготовку необхідних для атестації документів [17].

Атестації підлягають особи, які пропрацювали на підприємстві, в установі або організації понад один рік. Не підлягають атестації працівники, які працюють на підприємстві, в установі чи організації або на посаді менше року, вагітні жінки, керівники державних підприємств, яких призначає на посаду Кабінет Міністрів України, а також особи передпенсійного віку.

Особливо важливо залучати до атестації службу безпеки на підприємствах фінансової сфери діяльності (банки, страхові компанії і тому подібне), на підприємствах, діяльність яких пов'язана з державною таємницею.

При атестації персоналу для забезпечення кадрової безпеки необхідно приділити увагу наступним питанням:

- перевірки знань і умінь працівників в області забезпечення безпеки на підприємстві і на своєму робочому місці;
- перевірки лояльності працівників;
- додатковому інформуванню керівництва компанії про зміни в анкетних даних за період, минулий з прийому на роботу або попередньої атестації;
- оцінці довіри. Оцінка довіри до працівника – контрольний блок атестації.

Атестація працівників з точки зору кадрової безпеки здійснюється в індивідуальному порядку. На кожного з них складається відгук-характеристика, яку підписує безпосередній керівник, і заповнюється атестаційний лист.

У США використовуються різні методи атестації персоналу. Один з найбільш поширених методів складається з оцінки держав-

них службовців за 15 критеріями з комбінацією цифрових та текстових шкал. Кожний з використовуваних п'ятнадцяти елементів має п'ять ступенів.

Доцільним застосуванням системи атестації є те, що на 80,2% компаній атестація поліпшує виконання роботи. Систематична атестація дозволяє визначати і виправляти погані звички в роботі; 66% компаній використовували її як основу для просування по службі і переведень; на понад 63% фірм вона дає докладні відомості про послужний список співробітників і їх досягнення для визначення розміру збільшення заробітної плати; більше, ніж на 61% компаній атестація поліпшує моральний стан; майже 53% компаній використовують її для визначення кандидатів на посади керівників і створення групи потенційних керівників [31]. Отже, процес атестації є важливим елементом забезпечення кадрової безпеки підприємства, адже за допомогою такого виду проведення робіт визначається особисті якості працівника та відповідність вимогам даної посади.

Для підприємств, що дбають про довгострокову перспективу розвитку, важливим є формування лояльності персоналу. Лояльність – задоволеність співробітника умовами, винагородою, перспективами, колективом, захистом від зовнішніх загроз, тобто фактично забезпечення лояльності – це комплекс заходів щодо встановлення позитивних відносин працівників з роботодавцем. Традиційно в цій складовій роботи щодо запобігання загроз кадровій безпеці приділяється недостатньо уваги.

Лояльність персоналу розглядають як універсальну за направленістю складову кадрової безпеки, тому що ставлення працівника до власної організації є фактором, який або зміцнює, або руйнує систему кадрової безпеки підприємства.

Важливість лояльності для бізнесу підтверджується як західними, так і вітчизняними дослідниками. За даними американського щорічного довідника WORKUSA Survey, організації з високолояльними співробітниками за три роки принесли своїм акціонерам 112% прибутку, організації з середнім рівнем лояльності співробітників – 90%, а з низькими показниками лояльності – 76% [7].

Незважаючи на важливість лояльності в процесі гарантування кадрової безпеки, не існує єдиного визначення поняття «лояльність персоналу». Т. Чистякова і Н. Мойсеєнко трактують лояль-

ність персоналу як готовність працівника відповідати корпоративним очікуванням та формувати способи поведінки в межах, заданих організацією або керівництвом; стійкість до провокуючої дії ззовні; дотримання раніше прийнятих домовленостей; внутрішнє схвалення цілей компанії і цінностей, некритичне ставлення до життя в організації.

Л. Почебут розглядає лояльне ставлення працівників до організації, з одного боку, як установку, а з другого – як мотивацію людини працювати на користь організації, відстоювати її інтереси в різних сферах бізнесу [26].

У широкому розумінні лояльність персоналу можна розглядати як вірність працівника своїй організації. Високий рівень лояльності персоналу є важливим фактором зміцнення кадрової безпеки, оскільки лояльний працівник цінує власне робоче місце саме в цій компанії, проявляє бажання працювати на благо організації, є ініціативним та активним у вирішенні поставлених завдань, сприяє розвитку і підтримці корпоративної культури та відданому ставленню до організації.

Працівники з лояльним ставленням до компанії є набагато стійкішими до «спокусу»: їх складно переманити в іншу організацію, схилити до співпраці з конкурентами, шахрайства та зловживання повноваженнями. Лояльні співробітники критично ставляться до колег, які порушують правила організації, тим самим попереджують виникнення внутрішніх загроз кадровій безпеці.

Формування лояльного колективу можливе за рахунок розроблення та впровадження в організації системи заходів управління лояльністю. Під управлінням лояльністю персоналу слід розуміти усвідомлений вплив на чинники, що її формують, з метою забезпечення її подальшого розвитку і зміцнення [14].

Система заходів з управління лояльністю персоналу повинна бути зорієнтована на забезпечення сприятливих умов праці, позитивного психологічного клімату в колективі, розвиненої корпоративної культури та ефективної системи мотивації. Необхідно залучати працівників до вирішення проблем фірми, це сприятиме тому, що співробітник відчуватиме свою цінність та значимість для організації. Важливо, щоб працівники могли простежити й переконатися, як відсоток їх особистого внеску в життя компанії оцінюється й винагороджується.

Зміцнення лояльного ставлення працівників до організації сприятиме зростанню якості і продуктивності праці, відповідальності співробітників, рівня згуртованості та дисциплінованості трудового колективу, підвищенню трудової мотивації працівників, рівня активності та ініціативи, а також забезпеченню творчого підходу працівників та адекватної оцінки роботи.

За допомогою розробки і реалізації заходів щодо управління лояльністю персоналу на підприємстві вирішується низка важливих завдань, які не лише сприяють зміцненню кадрової безпеки організації, а й підвищують ефективність господарської діяльності компанії в цілому.

До важливих заходів управління кадровою безпекою належить і мотивація. Насамперед, це матеріальне заохочення. Ефективна фінансова політика щодо співробітників – важлива умова безпеки підприємства. Загрозою можна вважати як низький, так і високий рівень заробітної плати, адже в обох випадках матеріальна винагорода не виконує стимулюючої функції та знижує продуктивність праці. Обґрунтований рівень основної заробітної плати плюс премія за кожний вдалий крок або за стабільну роботу – найоптимальніше рішення. Як зазначав експерт Д. Староверов: «Гроші – ще не все». У людини виникають різні потреби [31]. Це відомі з теорії мотивації положення, які можна узагальнити.

Соціальні потреби:

- доручення роботи, яка дає змогу співробітникам спілкуватися;
- створення особливої атмосфери, духу єдиної команди;
- проведення періодичних нарад із підлеглими не тільки для прийняття стратегічних рішень, а й для обговорення поточних питань;
- підтримка неформальних відносин, якщо вони не завдають збитків роботі;
- створення умов для активного життя працівників поза організацією.

Потреба в повазі:

- підвищення змістовності роботи співробітників;
- організація зворотного зв'язку за результатами роботи (реакція керівництва);
- оцінювання й заохочення досягнутих результатів;

- залучення підлеглих до формулювання цілей і розробки рішень;
- просування підлеглих по службових сходах;
- забезпечення навчання та перепідготовки співробітників, що підвищує рівень їхньої компетентності.

Потреба в самовираженні:

- визначення та використання потенціалу кожного співробітника;
- доручення складних і важливих завдань, що вимагають повної віддачі;
- заохочення та розвиток творчих здібностей працівників.

Компенсація. Співробітники зазнають стресу, фрустрації, професійних відхилень у психіці через специфіку їхньої діяльності. Емоційне й психологічне розвантаження співробітників, компенсування всіх незручностей захистить організацію від неадекватних учинків персоналу. Для цього можна:

- створити кімнати відпочинку;
- створити затишну обстановку в робочих приміщеннях;
- організувати дозвілля;
- урізноманітнити роботу;
- звільняти від рутини;
- стежити за здоров'ям співробітників;
- увести в штат психолога, який знає специфіку роботи, або запрошувати його зі спеціалізованих фірм для моніторингу ситуації за допомогою тренінгів.

Вирішення особистих проблем. Іноді особисті проблеми співробітника перестають бути винятково його справою. Часто саме проблеми в родині або загроза близьким стає причиною нелояльності. Допомогти співробітникові можна тоді, коли керівник має на це моральне право, тобто коли працівник розуміє необхідність втручання у своє особисте життя. Для цього необхідно зробити хоча б кілька кроків:

- створення атмосфери, що сприяє відкритому вирішенню всіх конфліктів;
- боротьба з байдужістю як з боку колективу, так і з боку начальства;
- залучення психолога, який займається проблемами співробітників;

– культивування певних моральних цінностей, які допоможуть співробітникам встановити для себе певні принципи поведінки.

Пропаганда корпоративності. Зміцненню корпоративного патріотизму службовців сприяють:

- знання історії створення й розвитку компанії;
- постійне нагадування про конкуренцію. Інформація про результати діяльності компанії. Порівняння з конкурентами, як правило, є потужним імпульсом виховання лояльності;
- установа «неформальних» відносин усередині колективу, нормальних міжособистісних взаємин.

Інформаційна політика. Недостача інформації призводить до виникнення чуток, службових інтриг, пліток і доміслів. Запобігти або зменшити загрозу негативних тенденцій треба за допомогою:

- чіткої інформаційної політики;
- коректного ведення справ;
- чіткого окреслення компетенції й посадових обов'язків;
- профілактичних бесід із тими, кого можна вважати «інтригаторами».

І останнє – розумна політика «звільнення». Не можна допустити того, щоб працівник йшов з підприємства ображеним, адже як уже зазначалось вище – це може спричинити реалізацію загрози втрати конфіденційної інформації.

Важливим етапом в гарантуванні кадрової безпеки є оцінка ефективності заходів, яка здійснюється через зіставлення загальної величини витрат на запобіжні заходи і витрат, яких міг би зазнати суб'єкт підприємницької діяльності. Таким чином, кадрова безпека передбачає встановлення таких трудових і етичних відносин, які можна було б визначити як «беззбиткові». Важливо, що процес забезпечення кадрової безпеки здійснюється як безпосередньо фахівцями підрозділу безпеки, так і опосередковано кожним працівником підприємства.

Як об'єкт управління кадрова безпека підприємства володіє специфічними, властивими тільки їй особливостями. Її забезпечення і постійна підтримка є достатньо складним процесом в управлінні підприємством. Проте, не зважаючи на складність забезпечення кадрової безпеки, на новизну даного чинника для більшості українських підприємств, кадрова безпека підприємств є тим новим

елементом сучасного менеджменту підприємств, без реалізації якого не можна забезпечити надійність персоналу та стійкий розвиток підприємств. Тому необхідним є індивідуальний підхід до оцінювання кадрової безпеки, зважаючи на видові особливості, а також для формування найбільш повної інформації про кадрову безпеку підприємства слід дотримуватися комплексних комбінованих рішень, стосується це і критерію кадрової безпеки, що може розглядатися і як показник рівня реалізації трудового потенціалу.

ЛІТЕРАТУРА ДО ТРЕТЬОГО РОЗДІЛУ

1. Андрущенко М. П. Економічна безпека підприємства в аспекті ресурсного підходу / М. П. Андрущенко, О. В. Озаріна. [Електронний ресурс]. – Режим доступу : www.rusnauka.com.
2. Ареф'єва О. В. Кадрова складова в системі економічної машинобудівних підприємств / О. В. Ареф'єва, О. Ю. Литовченко // Актуальні проблеми економіки. – 2008. – № 11. – С. 95–100.
3. Беляева М. Как защититься от недобросовестных топ-менеджеров / М. Беляева // Управление персоналом. – 2008. – № 7. – С. 38–41.
4. Бойчик І. М. Економіка підприємства : навч. посіб. / І. М. Бойчик. – К.: Атіка, 2002. – 480 с.
5. Васильчак С. В. Кадрова безпека підприємства – основа економічного розвитку / С. В. Васильчак, І. Р. Мацюняк // Науковий вісник НЛТУ України. – 2009. – Вип. 19. – С. 122–128.
6. Воробйов І. Боротьба чи співробітництво / І. Воробйов, А. Кузнецов // Управління компанією. – 2007. – № 9. – С. 36–42.
7. Доминяк В. Организационная лояльность: основные подходы / В. Доминяк // Менеджер по персоналу. – 2006. – №4. – С. 34–40.
8. Економічна безпека підприємств, організацій та установ : навч. посіб. / [В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін.]. – К. : Правова єдність, 2009. – 544 с.
9. Жариков Е. С. Риски в кадровой работе / Е. С. Жариков. – М.: 2005. – 273 с.
10. Кагановська Т. Є. До питання визначення сфери кадрового забезпечення державного управління / Т. Є. Кагановська // Форум права. – 2008. – №2. – С. 202–209.
11. Кадрова безпека підприємства // Праця і закон. – 2011. – № 6 (138). [Електронний ресурс]. – Режим доступу : <http://www.hrd.com.ua/>
12. Кибанов А. Я. Управление персоналом организации / А. Я. Кибанов. – М. : ИНФРА-М, 2002. – 638 с.
13. Кириченко О. А. Менеджмент зовнішньо-економічної діяльності : навч. посіб. / О. А. Кириченко. – [3-тє вид., переробл. і доп.]. – К. : Знання-Прес, 2002. – 384 с.
14. Коваленко Д. В. Методологічні основи соціологічного виміру лояльності персоналу організації / Д. В. Коваленко // Соціологія майбутнього: науковий журнал з проблем соціології молоді та студентства. – 2010. – № 1. [Електронний ресурс]. – Режим доступу: www.sociology.kharkov.ua/socio/docs/magazin/soc_fut/1.../02.pdf.

15. Козаченко Г. В. Економічна безпека підприємства: сутність та механізм забезпечення : моногр. / Г. В. Козаченко, В. П. Пономарьов, О. М. Ляшенко. – К. : Лібра, 2003. – 280 с.
16. Криницин О. Что такое кадровая безопасность компании? / О. Криницин // Антикризисный менеджмент. – 2007. – № 2. – С. 23–27.
17. Кузьменко Л. М. Проблемы проведения оцінки персоналу / Л. М. Кузьменко // Економіка і маркетинг в ХХІ сторіччі. – 2008. – С. 160–162.
18. Лапицкая Л. Предпринимательские риски и управление непредвиденными кадровыми ситуациями / Л. Лапицкая // Управление персоналом. – 2004. – № 5. – С. 66–71.
19. Лисенко М. С. Механізм забезпечення кадрової безпеки підприємств / М. С. Лисенко // Формування ринкових відносин в Україні. – 2008. – №7. – С. 137–140.
20. Логінова Н. І. Місце кадрової безпеки в економічній безпеці підприємства / Н. І. Логвіна // Коммунальное хозяйство городов : Научно-технический сборник. – 2009. – № 87. – С. 371–376.
21. Менеджмент персоналу : навч. посіб. / В. М. Данюк, В. М. Петюх, С. О. Цимбалюк та ін. ; за заг. ред. В. М. Данюка, В. М. Петюха. – К.: КНЕУ, 2004. – 398 с.
22. Моделювання економічної безпеки: держава, регіон, підприємство : моногр. / [Гесць В. М., Кизим М. О., Клебанова Т. С. та ін.] ; за ред. Гейця В. М. – Харків : ВД «ІНЖЕК», 2006. – 240 с.
23. Назарова Г. Передумови створення системи кадрової безпеки підприємства / Г. Назарова // Регіональні аспекти розвитку продуктивних сил України. – 2010. – вип.15. – С. 34–37.
24. Папехин Р. С. Индикаторы финансовой безопасности предприятий / Р. С. Папехин. – Волгоград : Волгоградское научное издательство, 2007. – 516 с.
25. Петров М. І. Економічна безпека підприємства: сутність, трактування, точки зору / М. І. Петров // Менеджер. – 2002. – № 1(17). – С. 67–71.
26. Пилат Н. І. Лояльність персоналу в умовах мотивації професійної діяльності [Електронний ресурс] / Н. І. Пилат // Проблеми сучасної психології. – 2010. – №10. – Режим доступу: www.nbuv.gov.ua/portal/soc_gum/pspl/2010_10/601-612.pdf.
27. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : моногр. / Н. Й. Реверчук. – Львів : Вид-во ЛБІ НБУ, 2004. – 195 с.
28. Рысина Д. Ф. Проверяем благонадежность кандидатов на руководящие и другие ответственные должности (о судимости и дисквалификации) / Д. Ф. Рысина // Кадры предприятия. – 2008. – № 9. – С. 17–32.

29. Сайт Запорожского центра детекции лжи «POLYGRAPH» / [Электронный ресурс] – Режим доступа: <http://www.polygraph.zp.ua>
30. Соціальна безпека: теорія та українська практика : моногр. / І. Ф. Гнибіденко, А. М. Колот, О. Ф. Новікова та ін.; за ред. І. Ф. Гнибіденка, А. М. Колога, В. В. Рогового. – К.: КНЕУ, 2006. – 292 с.
31. Староверов Д. Лояльность персонала как фактор безопасности бизнеса. [Электронный ресурс] / Д. Староверов. – Режим доступа: <http://www.union.kz/ru>.
32. Староверов Д. Что такое безопасность компании? [Электронный ресурс] / Д. Староверов. – Режим доступа : <http://union.kz/ru/biz/kadbez/004kad/>
33. Сушко Н. М. Менеджмент персоналу в банках : навч. посібник / Н. М. Сушко. – К. : Центр учбової літератури, 2008. – 146 с.
34. Терехов И. С. Экономическая безопасность предприятия как успешная составляющая современного бизнеса [Электронный ресурс] / И. С. Терехов. – Режим доступа : <http://www.bre.ru/security>
35. Харский К. Благонадежность и лояльность персонала / К. Харский. – СПб.: Питер, 2003. – 325 с.
36. Цуруль О. А. Менеджмент у державних організаціях : навч. посіб. / О. А. Цуруль. – К.: КНЕУ, 2002. – 142 с.
37. Чаплигіна Ю. С. Етимологічний аналіз категорії «кадрова безпека» / Ю. С. Чаплигіна. [Електронний ресурс]. – Режим доступу: www.nbu.gov.ua.
38. Чумарин И. Г. Заключительные этапы и процедуры отбора персонала / И. Г. Чумарин // Кадры предприятия. – 2003. – № 7. [Электронный ресурс]. – Режим доступа: <http://www.poteri.net/publikatsii/kadry-predpriyatiya-7-2003.html>
39. Чумарин И. Г. Испытательный срок и адаптация с точки зрения кадровой безопасности / И. Г. Чумарин // Кадры предприятия. – 2004. – № 9. [Электронный ресурс]. – Режим доступа: <http://www.poteri.net/publikatsii/kadry-predpriyatiya-9-2004.html>
40. Чумарин И. Г. Кадровая безопасность – представители групп риска в организации / И. Г. Чумарин. [Электронный ресурс] // Персонал-Микс. – 2001. – №6. – Режим доступа к статье: <http://www.poteri.net/publikatsii/personal-miks-6-2001.html>
41. Чумарин И. Г. Планирование персонала с точки зрения кадровой безопасности / И. Г. Чумарин // Кадры предприятия. – 2003. – № 4. [Электронный ресурс] – Режим доступа: <http://www.poteri.net/publikatsii/kadry-predpriyatiya-4-2003.html>
42. Чумарин И. Г. Функции и задачи службы персонала в области обеспечения экономической безопасности / И. Г. Чумарин // Кадры предприятия. – 2003. – № 3. [Электронный ресурс] – Режим доступа : <http://www.poteri.net/publikatsii/kadry-predpriyatiya-3-2003.html>

43. Чумарин И. Г. Что такое кадровая безопасность / И. Г. Чумарин // Кадры предприятия. – 2003. – №2. – С. 45–52.
44. Швець Н. К. Методи виявлення і збереження кадрової безпеки, або як перемогти зловживання персоналу / Н. К. Швець // Персонал. – 2006. – № 5. – С. 31–36.
45. Штамбург Н. В. Складові економічної безпеки підприємства / Н. В. Штамбург // Бюлетень міжнародного нобелівського економічного форуму. – 2011. – № 1 (4). – С. 490–496.
46. Юрасов И. А. Основные показатели качественной работы кадровой службы предприятия / И. А. Юрасов // Кадры предприятия. – 2009. – № 5. – С. 91–100.
47. Alan Price. Employee Fraud. US Human Resources Management – HR Articles and Features [Електронний ресурс]. Режим доступу: <http://www.hrsguide.com>
48. Carpentier R. Prevoir les conduits on conduire son action / R. Carpentier // Humanisme et enterprise. – 1990. – December. – № 184. – P. 12.

Розділ 4

РОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ ТА КОНКУРЕНТНА РОЗВІДКА У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

4.1. Розвідувальна діяльність як засіб конкурентної боротьби у світовому економічному просторі

На сучасному етапі розвитку суспільства, коли посилюється боротьба за природні ресурси, домінуючу роль відіграють транснаціональні компанії, зростає рівень конкуренції, а ситуація на світовому фінансовому ринку є складно прогнозованою, економічно-розвідувальна діяльність – це один з найсуттєвіших засобів конкурентної боротьби. Ця теза стосується як макрорівня, коли державна розвідка в сфері економіки характеризується глибоким проникненням в інформаційне поле країн-конкурентів і, як правило, здійснюючись як законними, так і забороненими законом методами й прийомами, спрямована на отримання необхідної інформації для коригування державної політики, в т.ч. для підтримки свого товаровиробника, та забезпечення необхідного рівня національної безпеки, так і на мікрорівні – стосовно кожного окремого суб'єкта господарювання.

Для підприємницьких структур забезпечення конкурентної позиції та протистояння негативним впливам зовнішнього середовища є неможливим без отримання інформації про дії конкурентів, зміну попиту на продукцію чи послуги, перспективні наукові дослідження та новітні технології. Виникають два протиріччя, дві тісно взаємозв'язані обставини: а) підприємець вимушений виступати як захисник своїх таємниць (цінної комерційної інформації); б) підприємець вимушений з метою конкуренції здобувати (красти,

купувати) чужі таємниці, що захищаються. Важливо, що ці обставини взяті на озброєння і активно використовуються лідерами світового ринку. Так, такі потужні корпорації як «Міцубісі», «Сумімото» і т.д. в останні декілька десятиліть стрімко розвиваються завдяки організації досить потужних служб конкурентної розвідки та вкладаючи в них значні за обсягами фінансові та людські ресурси. Більш того, кожна велика японська компанія проводить моніторинг цін на ключову сировину – від нафти до міді й кукурудзи. Моніторинг охоплює як спостереження за діями конкурентів щодо цих матеріалів, так і політичну ситуацію в країнах, які таку сировину постачають. Саме такий підхід, коли «інформаційним полем» є увесь світ, забезпечує японським товаровиробникам високі темпи розвитку, можливість контролювати ситуацію та сприяти гарантування не лише власної економічної безпеки, але й країни.

У відповідності до вище поданого, сьогодні економічно-розвідувальна діяльність є важливим компонентом господарської діяльності, який суттєво впливає на рівень економічної безпеки різних соціально-економічних систем, а відтак потребує більш ретельного дослідження і, перш за все, в історичному ракурсі.

Розвідувальна діяльність (шпигунство) – явище таке ж стародавнє як і сама наша цивілізація. Економічна розвідка як невід’ємний компонент історичного розвитку продуктивних сил змінювала характер, форми і прояви відповідно до еволюції способу виробництва і рівня розвитку науки і техніки. У історичному аспекті економічна розвідка ледве не старша за військову та політичну.

Ще задовго до появи понять «конкурентна розвідка», «економічна розвідка», «промислове шпигунство» існувала діяльність, яку сьогодні можемо ототожнювати з ними. Основними проявами її були маскування «розвідників» під мирне населення, тобто використання прикриття, а також певні методи промислового шпигунства, які застосовували певні державні й недержавні структури задовго до того, як з’явилися офіційні й приватні розвідувальні служби. Як прикриття використовувався рід занять (торгівець, священик, монах, іноді жебрак тощо). Це були зародки сучасної економічної розвідки і промислового шпигунства.

Найдавніший приклад промислового шпигунства описує відомий французький письменник Жозеф Анрі Беке у своїй книзі «Боротьба за вогонь», коли первісні люди – герої книги –

відправлялися у сусіднє плем'я, щоб викрасти секрет добування вогню [14].

Документальні джерела – зокрема, китайська хроніка, що датується XV ст. до нашої ери, – містять розповідь про китайську принцесу, яка у своєму капелюшку, прикрашеному живими квітами, вивезла з Китаю шовковичних черв'ячків і передала їх своєму коханому разом із секретом виготовлення шовку, чим позбавила Китай монополії в цій галузі [14]. Важливими секретами у цьому історичному періоді володіли і араби. З цієї причини для отримання інформації багато агентів і шпигунів відвідували арабський Схід. Араби вміло зберігали та охороняли свою інформацію, але, на відміну від китайців, в них можна було її купити.

Потрібно наголосити на тому факті, що значна кількість думок та підходів мислителів того часу не лише актуальні у сьогоденні, але і активно використовуються у практиці для досягнення успіху в конкурентній боротьбі. Так, привертає увагу твір відомого китайського філософа Сунь-Цзи, що жив у 5 сторіччі до н.е., «Філософія війни», де сказано: «якщо освічений цар або розважливий генерал здобувають перемогу над супротивниками щоразу, коли вони переходять до дій, то це досягається завдяки попередній інформації. Так звана попередня інформація не може бути отримана ані від парфумів, ані від божества, ані за аналогією з минулими подіями, ані шляхом розрахунків. Її необхідно одержати від людини, яка знайома із ситуацією супротивника».

Сунь Цзи надавав дуже велике значення розвідувальній службі. Найбільшу його увагу притягувала агентурна розвідка. Обгрунтовуючи витрати на агентурну розвідку, цей філософ писав: «захищаються один від одного кілька років, а перемогу вирішують в один день. Тому все потрібно передбачати. Знання ж майбутнього неможливо отримати від богів або демонів, знання про супротивника можна отримати лише від людей, від шпигунів. Користування шпигунами – найсуттєвіше на війні; це та основа, опираючись на яку діє армія. Шпигуни є надзвичайно важливими для війська, тому їх слід нагороджувати краще за всіх, а їх діяльність зберігати у великій таємниці. Шпигуни бувають п'яти видів: місцеві, внутрішні, зворотні, шпигуни життя та смерті. Способи їх діяльності – таємниця. Місцеві шпигуни – з місцевих жителів країни противника, внутрішні – його чиновники, зворотні шпигуни – шпигуни супро-

тивника; якщо зворотні шпигуни передають супротивнику хибні відомості, то це шпигуни смерті; вертаються з донесеннями – це шпигуни життя. Перш ніж почати військові дії, потрібно отримати через шпигунів вичерпні відомості щодо супротивника, зокрема, щодо їх військових керівників, начальників охорони та воїнів охорони. Потім з допомогою шпигунів потрібно ввести противника в оману. Все це забезпечить успіх».

Відповідно до хронології історичних подій, активізація промислового шпигунства припадає на середньовіччя, адже саме у цей період йшла боротьба за секрети «грецького вогню» (самозаймистої речовини, яка в закупорених глиняних посудинах використовувалася для бомбардування ворожих кораблів), а також порцеляни. Технологія виготовлення останньої, будучи викраденою з Китаю, потрапила до Великобританії, Німеччини, Австрії, Росії, Італії, на Скандинавські острови, а звідти – по усьому світу [14].

В аграрну епоху, поруч з державною економічною розвідкою, зародилась і приватна розвідка. Документально підтвердженою датою виникнення першої конкурентної розвідки прийнято вважати кінець XIV століття, коли Дім Фуггерів у Німеччині започаткував використання методів комерційної розвідки на постійній основі, розповсюджуючи серед власних співробітників на місцях так званий «манускрипт новин». Документ містив цілеспрямовано відібрану й проаналізовану комерційну і політичну інформацію, яка дозволяла ключовим співробітникам приймати ефективні рішення. За часів керівництва компанією Якоба Фуггера (1495–1525 рр.) була створена справжня приватна розвідувальна служба, в основі функціонування якої знаходились численні представництва фірм у різних європейських країнах, які збирали необхідні відомості. Вважається, що саме це надало можливість Фуггерам зайняти домінуюче становище в основних галузях промисловості і створити перший в Європі банківський дім.

З XVI до XVIII ст. основним предметом промислового шпигунства були відкриття алхіміків. Наполегливе полювання велось за секретами герметичної закупорки посуду, виробництва золота, кислот для очищення алмазів і, нарешті, пороху (також «запозиченого» у китайців).

Наступною історичною подією, яка засвідчує факт зростання важливості промислового шпигунства, є діяльність кількох

покоління роду Крупп. Так, ще Фрідріх Крупп для виконання умов конкурсу, який оголосив Наполеон Бонапарт на виготовлення французької сталі, скупив у дрібних шпигунів багато формул і таким чином зрозумів суть технологій основних виробників англійської сталі. Його син – Альфред Крупп, налагодивши контакти як у вищому світі, так і серед промисловців Англії, отримав секрети, якими свого часу не зміг заволодіти його батько. Він відразу ж приступив до створення першої у світі приватної організації промислової безпеки, а в 1848 році став єдиним власником фірми. Густав Крупп – внук Фрідріха Круппа, удосконалив розвідувальні діяльність, про що, зокрема, свідчить той факт, що йому вдалося викрасти у французів гігантську гармату, котру він сховав у заводській трубі.

Подальший розвиток промисловості спричинив і все більше поширення промислового шпигунства, яким почали займатися окремі фірми, корпорації та фінансові структури. У зв'язку з тим, що перед державними розвідувальними структурами почали ставитися завдання економічного характеру, розпочалося об'єднання інтересів неурядових організацій та спеціальних служб щодо отримання необхідної інформації. Разом з тим, виходячи з цієї ситуації, спецслужби почали залучати недержавні, нерозвідувальні структури для прикриття своєї розвідувальної діяльності. Так, німецький уряд на державному рівні підтримував промислове шпигунство і у зв'язку з браком державних коштів на використання промислових секретів користувався послугами приватних компаній. Наприклад, німецьким фірмам, які відкривали свої представництва (філії) в інших державах, державне казначейство Німеччини видавало «особливі премії». Окрім цього, німецькі купці під час поїздок по Європі та вивчення ринку дійшли висновку, що за рахунок використання іноземних наукових досягнень у різних галузях промисловості можна усунути зі свого шляху французькі та англійські фірми-конкуренти. На основі, власне кажучи, розвідувальної економічної інформації, котра здобувалася вітчизняними бізнесменами, німці в короткий термін розгорнули власну навчальну і науково-дослідну базу для розвитку нових технологій. Такі методи конкурентної розвідки сприяли тому, що ряд німецьких підприємств вже на початку ХХ ст. стали власниками патентів з багатьох відкриттів у хімічній галузі.

В XIX столітті в Європі однією з найбільших приватних розвідувальних структур економічного напрямку була організація, яку утримував банкірський двір Ротшильдів. Ротшильди налагодили професійно організовану структуру економічної розвідки для збирання інформації як для власних потреб, так і для своїх клієнтів. Діючи з контор у Франкфурті-на-Майні, Лондоні, Парижі, Відні та Неаполі агенти Ротшильда часто могли здобувати надзвичайно важливі відомості раніше, ніж зацікавлені в них уряди.

Формально поява промислового шпигунства пов'язана з введенням в XVIII столітті системи патентів на винахід, які були захищені охороною права винахідника або дослідника. Згідно з нею, власник патенту на винахід отримував право на переслідування викрадачів секретів протягом двадцяти років, після чого секрет ставав власністю суспільства. Це був вже не перший законодавчий захід, спрямований на захист прав винахідників, але особливістю цього закону було те, що вперше заохочувалося промислове шпигунство за кордонами Франції. Тобто, на законодавчому рівні стимулювалось шпигунство: «кожному, хто перший привезе до Франції якийсь іноземний промисел, надаються такі ж пільги, якими б користувався його винахідник» [4].

Зростаюча могутність міжнародних монополій в індустріальну добу перетворила боротьбу за виживання у все більш жорстоку та менш етичну. Для досягнення максимального успіху активно застосовувалося промислове шпигунство, використовуючи при цьому різні методи отримання інформації і новітні досягнення науки та техніки.

Приблизно з 1875 року – часу очевидної промислової переваги Англії – розпочинається історія розвитку промислового шпигунства в США та Японії, що почала розвиватися. У період Першої світової війни промислове шпигунство практично зливається з військовим. Про це, наприклад, свідчить факт викрадення французами у німців у 1914-1915 рр. технології виготовлення снарядів з отруйним газом, коли за декілька днів за дві тисячі марок шпигун здобув секрет, над яким два роки працювали кращі німецькі хіміки і на який було витрачено мільйони.

Висока ефективність розвідувальної діяльності та загроза, яку вона створює для економічного розвитку як окремої компанії, так і країни, сприяли виникненню нових розвідувальних структур –

агентств, які крім викрадання інформації надавали послуги щодо її охорони. Прикладом стало американське агентство Н. Пінкертона, яке окрім промислового шпигунства здійснювало контррозвідку. В Швейцарії та Японії такі агентства існували як цілком легальні офіційні організації, одна з яких – міжнародне детективне агентство «Бернс Інтернешнл детектив ейдженсі» мало спеціальне відділення для виконання завдань промислового шпигунства. Тільки в Токіо існувало понад 380 детективних агентств, які займалися виключно викраденням виробничих секретів різних фірм.

В період між двома світовими війнами за допомогою таких методів як цінова війна, протекціонізм з боку держави, незаконне копіювання технологій, японська текстильна промисловість перемогла своїх британських та американських конкурентів. Промислове шпигунство фактично забезпечило прогресивний розвиток японської економіки.

Якщо ж взяти до уваги сучасний період розвитку суспільства, то спонукальним мотивом до здійснення розвідувальної діяльності стала конкуренція, яка відкриває шлях до процвітання одних і занепаду інших. Водночас забезпечує прогрес і спричиняє конфлікт інтересів учасників ринку. За цих умов, починає діяти правило: створюй розвідувальну структуру, збирай секрети конкурентів та захищай власні. Як і економічна розвідка, так і діючі заходи захисту проти неї є важливими умовами забезпечення конкурентних переваг. Оскільки у всьому світі конкуренція визначається одним із головних факторів, що забезпечують рівновагу економічного розвитку, то конкурентна розвідка буде зберігати свою актуальність у подальшому.

В сучасному світі бізнесу відомий такий вислів: «Капітал боїться відсутності прибутку або дуже малого прибутку, так само, як і природа боїться порожнечі» [2]. Нові досягнення науки і техніки, сучасні методи промислового виробництва змушують економічну розвідку знаходити нові засоби та методи роботи. Щоб встигати за технічним розвитком стає необхідним постійно удосконалювати й техніку економічної розвідки. Розвідувальна діяльність охоплює все нові і нові галузі. Тобто, вона є неминучим та закономірним явищем самої природи бізнесу, заснована на бажанні отримання надприбутку будь-якими дозволеними, а іноді й неетичними методами.

Важливо, що економічна розвідка сьогодні активно використовується як на макро-, так і мікрорівні, але новітнім є пряме залучення розвідок ряду країн для викрадення промислових секретів в інтересах корпорацій. Уряди фінансують операції, у процесі яких вивчається діяльність різноманітних компаній, збираються відомості про майбутні контракти, узагальнюється інформація про фінансовий стан організацій та банківських операцій, аналізуються події, які можуть відбитися на формуванні цін на світовому ринку. Для отримання важливих відомостей розвідувальні служби використовують численні методи, розроблені в період «холодної» війни. Найбільш активною в цьому відношенні є французька розвідувальна служба. Далеко не останні місця займають Японія, Китай, Південна Корея, Індія, Пакистан, Німеччина, Ізраїль, Аргентина, Росія, які також займаються збиранням інформації в інтересах національних компаній.

Можна чітко сформулювати новітні тенденції розвитку розвідувальної діяльності, які полягають у державній підтримці промислового шпигунства. Так, ще в 1990 р. Президент США Джордж Буш у своїй доповіді «Стратегія США в галузі національної безпеки» проголосив економічну розвідку пріоритетним напрямком у діяльності американських спецслужб. Наприкінці 1993 р. Біл Клінтон дав вказівку керівництву розвідувального співтовариства США про поглиблення досліджень у сфері економічної розвідки. Було виділено три пріоритетних напрямки:

макроекономічна розвідка – збір стратегічної інформації про глобальні процеси в економіках інших держав;

мікроекономічна розвідка – збір тактичної й оперативної інформації з тієї ж проблематики;

економічна контррозвідка – протидія спробам іноземних державних спецслужб і комерційних фірм здобути американські торгово-економічні й технологічні секрети.

Потрібно відзначити, що у США промислове шпигунство у повному обсязі фінансується конгресом Сполучених Штатів Америки. На розвиток економічно-розвідувальної діяльності уряд США витрачає значну частку свого ВВП. Це фінансування дає можливість перейти від традиційних методів (викрадення, підкуп) до найсучасніших, з використанням високих технологій («хай-тек»). Для досягнення найкращих результатів застосовується велика кількість

різноманітних способів, таких як: злиття та поглинання фірм, створення спільних підприємств, проведення міжнародних форумів, виставок, наукових симпозіумів та конференцій.

Для характеристики масштабів розвідувальної діяльності значимо, що за даними ООН, у світі діють близько 55 тисяч транснаціональних корпорацій, що займаються комерційним шпіонажем, які збирають дані про фундаментальні і прикладні відкриття, про злиття компаній, про провідних спеціалістів, про рух фінансів, а також про провідних політичних діячів, про провідних спеціалістів і менеджерів фірм з метою чинення впливу на них, про території, перспективні з точки зору вкладання капіталу тощо.

Існуючий попит на розвідувальну діяльність спонукав до активного здійснення теоретичних досліджень в цій сфері. Варто відзначити, що в американських вищих навчальних закладах уже більш ніж 30 років науковці, стажисти, аспіранти та студенти вивчають близько ста розгорнутих курсів з різних аспектів розвідки й контррозвідки.

На відміну від розвинутих країн світу, в Україні робляться лише перші кроки на шляху теоретичного обґрунтування розвідувальної діяльності, зокрема і через переклад іноземних наукових джерел. Результатом зазначеного стало те, що у вітчизняній літературі зустрічаються різноманітні поняття щодо розвідки у сфері економіки, а саме: економічна розвідка, економічний шпигунство, конкурентна розвідка, бізнес-розвідка, ділова розвідка, комерційна розвідка, промислове шпигунство, бізнес-шпигунство. Усі вони в найбільш загальному вигляді передбачають активні дії, направлені на збір, розкрадання, накопичення і обробку цінної інформації, закритої для доступу сторонніх осіб.

Узагальнюючи доробок вітчизняних та закордонних науковців [1-48], ми дійшли висновку, що сьогодні відсутній єдиний підхід щодо класифікації та чіткого визначення ознак розвідувальної діяльності. Серед перелічених вище термінів доцільно приділити увагу двом – «конкурентна розвідка» та «промислове шпигунство», які, на нашу думку, у найбільшій мірі відповідають сучасному трактуванню розвідувальної діяльності та взаємопов'язані із процесом гарантування економічної безпеки. Перш ніж розглянути суть зазначених термінів, чітко вкажемо на їх спільні ознаки та суттєві відмінності.

Метою як конкурентної розвідки, так і промислового шпигунства є одержання інформації, яка б дала змогу здобути конкурентну перевагу на ринку, а також економія коштів та часу на інноваційну діяльність. У свою чергу, головною відмінністю між цими видами розвідувальної діяльності є методи й способи отримання інформації. Служба конкурентної розвідки діє виключно законними методами, користується тільки відкритими джерелами, оскільки робота розвідника – інформаційно-аналітична, тобто збирання й обробка різних даних, що впливають або можуть вплинути на розвиток бізнесу. Промисловий шпіонаж, навпаки, передбачає нелегальні методи й технології. Шпигунство полягає головню в оперативній роботі, зокрема в незаконному проникненні на територію конкурента, знятті інформації з каналів зв'язку, стеженні, підкупі, шапталжі, викраденні інформації тощо.

Потрібно наголосити на тому факті, що досить широко промислове шпигунство використовується у міждержавних відносинах, але, на відміну від бізнесу, для державної розвідки пріоритетним є забезпечення національної безпеки, а відтак законність відходить на другий план.

Оскільки серед визначених нами у першому розділі принципів гарантування економічної безпеки важливу роль відіграла законність дій, то ми лише коротко охарактеризуємо суть промислового шпигунства та для порівняння – в загальному конкурентної розвідки.

Промислове шпигунство як спосіб отримання особливо цінних (конфіденційних) відомостей про стан справ, методи і технології роботи суперника уможлиблює досягнення конкурентних переваг через:

- отримання інформації конкурентів, насамперед конфіденційної, про стратегічні й тактичні наміри їхнього бізнесу;
- здобуття конкурентної переваги на ринку, через витіснення або знищення конкурента.

Довідники описують промислове шпигунство як вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність. Ключове слово в цьому визначенні – «незаконного» [11].

Зазначене пояснюється методами, які застосовуються для отримання інформації:

- крадіжка інформаційного носія з даними, що представляють комерційну або службову таємницю;
- впровадження шпигуна, який мав би можливість доступу до конфіденційної інформації;
- підкуп людини, що володіє такими даними;
- шантаж;
- прослуховування телефонів, перегляд кореспонденції, електронних листів і так далі.

Вагомим мотивом для подальшого активного застосування промислового шпигунства є економічний ефект від його здійснення. Так, в Японії поширена думка: для чого витратити 10 років та мільярд доларів на дослідження, коли хабаром в 1 мільйон доларів інженеру фірми – конкурента можна швидше та ефективніше досягти такого ж результату.

Необхідно наголосити і на тому факті, що незаконність не лише розширює можливість отримання інформації, але і спричиняє кримінальну відповідальність, застосування судових санкцій та негативно впливає на ділову репутацію компанії.

Оцінюючи правовий аспект промислового шпигунства, слід зазначити, що в країнах Європейського союзу немає законів, які трактують промислове шпигунство як протиправне діяння. В окремих штатах США ж промислове шпигунство законодавчо вважається злочином.

На нашу думку, вірними є міркування А. Курмана [23], відповідно до якого промислове шпигунство за законодавством України – це діяння, що підпадають під ознаки складів злочинів, передбачених статтями 231 Кримінального кодексу України «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» і 232 Кримінального кодексу України «Розголошення комерційної або банківської таємниці». Тобто промислове шпигунство – це злочинна діяльність, яка посягає на інтереси, що охороняються законодавством, здійснюється протиправними методами і спрямовується на отримання незаконним шляхом відомостей, що становлять комерційну таємницю підприємства.

Стаття 231 встановлює кримінальну відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю:

«умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, – караються 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».

Стаття 232. «Розголошення комерційної або банківської таємниці»: Умисне розголошення комерційної або банківської 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.

Безпосереднім об'єктом злочинів, передбачених статтями 231, 232 КК України, виступають суспільні відносини щодо збереження комерційної та (або) іншої таємниці, а наслідки їх здійснення визначають як:

- реальну позитивну шкоду – прямі матеріальні збитки, у тому числі витрати на захист своїх прав, перепрофілювання діяльності, впровадження нових технологій, додаткові заходи охорони, повідомлення додаткової інформації споживачам, закупівлю нового обладнання тощо;

- упущену вигоду – неотримання тих майнових вигод, які суб'єкт господарської діяльності повинен був отримати за умови належного користування своїми правами стосовно комерційної таємниці і належного виконання своїх обов'язків іншими суб'єктами суспільних відносин, у тому числі збитки від зниження реалізації продукції, послуг, робіт, спаду виробництва, зменшення клієнтури, зниження цін на товари, роботи й послуги тощо. Розмір такої шкоди, як указано в законі, має бути істотним.

Узагальнюючи, можна стверджувати, що промислове шпигунство уможливорює не лише посилення конкурентної позиції, але і загрожує кримінальною відповідальністю за вчинені незаконні дії.

На протипагу промисловому шпигунству, конкурентна розвідка – постійний процес збору, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії й надання вищому менеджменту компанії інформації, що дозволяє йому передбачати зміни в обстановці й приймати своєчасні оптимальні рішення щодо управління ризиками, впровадження змін у компанії й відповідних заходів, спрямованих на задоволення майбутніх запитів споживачів і підтримку прибутковості.

У вітчизняному бізнесовому середовищі термін «конкурентна розвідка» (competitive intelligence) поки що не є широкоживаним, тому можна натрапити на його еквіваленти – як-от «ділова розвідка», «бізнес-розвідка». Часто саме бізнесову розвідку мають на увазі, коли, не уточнюючи хто, чим, заради чого займається, висловлюються щодо «інформаційно-аналітичної роботи», «моніторингу» тощо [17].

Кінцева мета конкурентної розвідки:

- визначення дійсної стратегії та потенціалу конкурентів (їх сильні і слабкі сторони) для коригування власної стратегії;
- надання інформації для удосконалення організаційних, фінансових, технічних та інших способів забезпечення конкурентних переваг;
- оцінка ступеня вигідності умов співпраці з тими або іншими постачальниками, партнерами і покупцями;
- забезпечення на мікрорівні додаткового прибутку, поперше, шляхом копіювання і впровадження «чужої» інновації і, по-друге, за рахунок економії на умовно-постійних витратах – на науково-дослідних та проектно-конструкторських роботах.

Важливою є та обставина, що конкурентна розвідка здійснює збір інформації про навколишнє бізнес-середовище тільки законними методами, які умовно можна поділити на цілком законні (білі) та методи, які за своєю формою не порушують норм законів, проте не завжди відповідають морально-етичним нормам ведення чесної конкурентної боротьби (сірі методи).

До першої групи методів конкурентної розвідки, тобто до законних, належать:

- вивчення й аналіз публікацій конкурента;
- вивчення, аналіз та обробка відкритої інформації про конкурента.

До другої групи методів належать такі:

- матеріальне заохочення співробітників конкурента з метою отримання конфіденційної інформації;
- «переманювання» спеціалістів конкурента і отримання в них відомостей, що мають обмежений доступ;
- вивідування інформації у співробітника конкурента;
- проведення підставних переговорів з метою вивідування конфіденційної інформації;
- отримання необхідної інформації про конкурента через зв'язки в правоохоронних та контролюючих органах.

В даний час ефективно організована конкурентна розвідка не обмежується вивченням конкурентів, а проводить роботу щодо усього середовища, в якому функціонує підприємство, а це зокрема:

- прогнозування змін на ринку;
- передбачення дій конкурентів і постачальників;
- виявлення нових або потенційних конкурентів;
- можливість вчитися на успіхах і помилках інших компаній;
- відстеження інформації, пов'язаної з патентами і ліцензіями;
- оцінка доцільності придбання нового бізнесу;
- вивчення нових технологій, продуктів і процесів, які можуть вплинути на конкретний бізнес;
- вивчення політичних, законодавчих чи регуляторних змін, які можуть вплинути на конкретний бізнес;
- оцінка відповідності методів ведення бізнесу ринковим реаліям;
- зниження ризиків промислового шпигунства через внутрішні канали;
- використання слабостей конкурента в своїй рекламі;
- збір інформації про партнерів і клієнтів.

Сьогодні за неофіційною оцінкою фахівців СБУ, практично кожна велика вітчизняна фірма збирає інформацію про своїх конкурентів, партнерів та контрагентів і, одночасно, сама є об'єктом пильного вивчення з боку інших учасників ринку.

Проведене порівняння промислового шпигунства та конкурентної розвідки, їх загальна характеристика з однієї сторони

та ієрархічно впорядкована сукупність загроз для вітчизняних підприємств – з іншої, переконливо доводять необхідність удосконалення методичних аспектів здійснення розвідувальної діяльності. Із врахуванням важливості реалізації виключно законних методів гарантування економічної безпеки та можливості отримання із відкритих джерел до 95% інформації про конкурентне середовище, вважаємо за доцільне в наступних підрозділах приділити увагу лише конкурентній розвідці.

4.2. Сучасне трактування та напрямки розвитку конкурентної розвідки

«Хто володіє інформацією – той володіє світом» – цей відомий вислів став не лише особливо актуальним у третьому тисячолітті, але і ключем до розуміння більшості процесів у розвитку людства. Потреба отримання та можливість вільно використовувати інформацію сьогодні зумовлюється рядом ключових обставин. Якщо взяти до уваги макрорівень, то такі обставини в найбільш загальному вигляді можна окреслити наступним чином: формування постіндустріального суспільства, де основна роль відводиться людині із її можливостями сприймати інформацію і на основі цього генерувати нові знання; інтенсивне використання інформації і знань як новітніх нелімітованих ресурсів; умовний поділ країн на ті, для яких пріоритетним є інноваційний розвиток, зокрема через активне застосування інформаційно-комунікаційних технологій, і на сировинноорієнтовані; швидкий розвиток інформаційних технологій та їх використання у всіх сферах суспільного буття; зростання важливості інтелектуальної вартості у розвитку людства; прискорення глобалізації економічних відносин; ріст конкуренції на глобальному та національному рівнях і т.д.

Стосовно ж мікрорівня, то сучасний вітчизняний і зарубіжний досвід розвитку ринкових відносин яскраво демонструє, що жодна особа, жодна організація не можуть ефективно діяти в умовах гострої конкурентної боротьби без глибокого та усестороннього розуміння ринкового середовища або не маючи у своєму розпорядженні новітньої, повноцінної і достовірної інформації про

те, що в ній відбувається. І в цьому контексті, як уже зазначалось в попередньому підрозділі, ключову роль повинна відігравати конкурентна розвідка, мета якої і полягає в аналізі діяльності конкурентів з використанням легальних методів збору і обробки відкритої інформації.

Узагальнюючи вище викладене та беручи до уваги результати теоретичного дослідження, які були раніше, можна стверджувати, що головною категорією конкурентної розвідки є і залишається економічна інформація (від лат. – ознайомлення, пояснення, уявлення, поняття; з англ. – дані) – об'єкт багатofункціонального засобу реалізації конституційних прав і свобод, як елемент управління суспільними, державними справами, прийняття управлінських рішень, як товар у процесах її створення, використання, розповсюдження, як об'єкт права власності [30].

Стосовно можливості отримання інформації, то доречним є цитування міркувань колишнього директора центральної розвідки США Р. Хілленкеттера: «80% розвідувальної інформації виходить із таких звичайних джерел, як іноземні книги, журнали, наукові і технічні огляди, фотографії, дані комерційного аналізу, газети, радіопередачі, а також із загальних зведень, отриманих від осіб, що мають уявлення про стан справ за кордоном». Звідси, полем для розвідувальної діяльності виступають, перш за все, вільнодоступні масові комунікації, але реальною складністю є опрацювання значних обсягів інформації, що можливо здійснити лише за умови чіткої організації роботи та наявності висококваліфікованих фахівців.

На нашу думку, конкурентна розвідка в сучасному постіндустріальному суспільстві – важлива структурна ланка підприємницької діяльності, що використовує динамічно формуючий інформаційний ресурс, який дозволяє передбачати зміни на ринках, дії конкурентів, виявляти нових або потенційних конкурентів, прогнозувати появу нових технологій, забезпечує моніторинг політичних ризиків. Більш того, можна чітко стверджувати, що для виживання в умовах сучасної конкурентної боротьби першочергового значення набуває розвідка намірів конкурентів, вивчення основних тенденцій бізнесу, аналіз можливих ризиків.

Концепція конкурентної розвідки офіційно існує з середини 90-х рр, а сам термін «конкурентна розвідка» пішов з англійської мови, а саме з виразу «competitive intelligence» [44]. Сьогодні існує

безліч тлумачень і розумінь даного поняття. Конкурентну розвідку часто ототожнюють із діловою розвідкою, аналітичною, комерційною, корпоративною, економічною, стратегічною, бізнес-розвідкою, промисловим шпіонажем, маркетингом, бенчмаркінгом і навіть з простим аналізом ділової інформації. Зазначені обставини обумовили необхідність проведення певного теоретичного дослідження, спрямованого на узагальнення точок зору науковців стосовно суті та ключових завдань конкурентної розвідки для потреб вітчизняних підприємств на сьогоднішньому етапі розвитку національної економіки.

Російський науковець Ю. Воронова вважає, що конкурентна розвідка – це маркетинговий інструмент вивчення конкурентного середовища, який є цілеспрямованим збором інформації про конкурентів для ухвалення управлінських рішень щодо подальшої стратегії та тактики ведення бізнесу [10]. В. Абрамов конкурентну розвідку визначає як різновид маркетингової діяльності, заснованої на роботі з відкритими джерелами інформації в правовому полі і що не припускає ніяких нелегальних операцій [1]. Схоже до попередніх трактувань подає визначення і Н. Борісов, трактуючи її як маркетинговий інструмент вивчення конкурентного середовища, що являє собою цілеспрямований збір інформації про конкурентів для прийняття управлінських рішень з подальшої стратегії й тактики ведення бізнесу [7].

Дещо в іншому ракурсі трактує конкурентну розвідку Ж. Міллер, розглядаючи її як службу, що забезпечує керівництво підприємства інформацією, необхідною для превентивного ухвалення рішень. Це не тільки збір інформації, але і її класифікація (за значущістю, ступенем достовірності тощо), і аналіз, і прогноз розвитку ситуації, і підготовка рекомендацій керівництву [46].

Д. Ховіс дав тлумачення конкурентної розвідки, визначивши її як невинне системно організоване відстеження ситуацій на ринках, добірка добре профільтованих і проаналізованих фрагментів «сирої» інформації, перетвореної в придатний для прийняття рішень матеріал з метою виявлення тих тенденцій, що вимагають негайного реагування людей, які приймають рішення [40]. Інший науковець – Є. Ющук, подав її як збір і обробку даних з відкритих джерел для вироблення управлінських рішень з метою підвищення конкурентоспроможності комерційної організації, що проводяться

в рамках закону і з дотриманням етичних норм; а також структурний підрозділ підприємства, що виконує ці функції [43].

У трактуванні Т. Круглякова конкурентна розвідка розглядається як постійний процес збирання, оброблення, оцінки і накопичення даних, а також їх аналізу з метою прийняття оптимальних рішень [22].

А. Мітрофанов визначає суть конкурентної розвідки як діяльність, що допомагає оцінювати та прогнозувати дії конкурентів, спрямовані на дестабілізацію діяльності підзахисної компанії та її керівної підсистеми або руйнування інформаційних зв'язків усередині компанії [25].

Р. Бараннік досить коротко окреслює мету конкурентної розвідки – збирання й оброблення інформації бізнесом [3].

Попри певні відмінності в трактуванні конкурентної розвідки, усі науковці одностайні в тому, що її реалізація передбачає збір та аналіз інформації щодо стану та динаміки зовнішнього середовища, яка повинна стати основою для прийняття управлінських рішень.

Зважаючи на суттєвий і негативний вплив світової фінансової кризи 2008-2009 рр. на ефективність господарської діяльності та низький рівень економічної безпеки вітчизняних підприємств, організована та ефективно діюча конкурентна розвідка повинна стати інновацією, інструментом виживання, засобом перемоги, стратегічною альтернативою і ефективним інструментом ведення бізнесу.

Відповідно до зазначеного, конкурентна розвідка на вітчизняних підприємствах покликана вирішувати наступні завдання:

- інформаційне забезпечення процесу прийняття управлінських рішень як на стратегічному, так і на тактичному рівні;
- завчасне надання інформації працівникам підприємства, що приймають рішення, стосовно загроз та ризиків, які потенційно можуть заподіяти шкоду підприємству;
- пошук сприятливих для розвитку підприємства можливостей;
- виявлення спроб конкурентів отримати доступ до комерційної таємниці підприємства та цінної інформації;
- управління ризиками з метою забезпечення ефективного реагування підприємством на швидкі зміни навколишнього середовища;

– розробку варіантів дій, оптимальних в певній ситуації й здатних призвести до того, що практично негативні тенденції можуть принести користь.

Виконання сформованої сукупності завдань конкурентною розвідкою підприємства є можливим лише у випадку дотримання шести правил логістики, а саме: 1) добувати потрібну інформацію; 2) необхідної якості; 3) в необхідній кількості; 4) представляти її у потрібний час; 5) у потрібне місце (керівникові); 6) з мінімальними трудовими, фінансовими і матеріальними витратами.

Дотримання перелічених правил уможливить не лише виконання ключових завдань, але, що є особливо важливим, забезпечить ефективність здійснення конкурентної розвідки через раціональне використання ресурсів та співрозмірність витрат із очікуваним ефектом.

Зазначене обумовлене тим фактом, що процес отримання потрібної інформації та перетворення її у важливі дані, як зазначалось уже вище, – дуже багатогранний, складний, змістовний та енергомісткий, хоча він набагато дешевший аніж його результат.

Як підсистема суспільних відносин конкурентна розвідка повинна охоплювати наступні відносини:

– виробничі (відносини в процесі виробництва, обміну, розподілу та споживання інформації);

– техніко-економічні (щодо спеціалізації, кооперування, координації та управління діяльністю працівників служби конкурентної розвідки);

– правові (щодо реалізації права на інформацію, юридичної відповідальності у сфері доступу до інформації, використання новітніх інформаційних технологій);

– етичні (щодо дотримання Етичного кодексу міжнародної Спільки професіоналів конкурентної розвідки (SCIP), національних ділових традицій та моральних принципів);

– освітянські (між теоретиками й практиками конкурентної розвідки щодо її розвитку).

Швидка зміна зовнішнього середовища впливає не лише на діяльність підприємницьких структур, але і спричиняє удосконалення конкурентної розвідки. Основні тенденції у змінах цього виду розвідувальної діяльності можна коротко охарактеризувати наступним чином:

- вона набуває пріоритетного значення у порівнянні з військовою та політичною розвідкою;
- об'єктом розвідувальної діяльності стає, перш за все, новітня науково-технічна інформація, а також всі інші види відомостей: фінансові та бізнесові плани корпорацій, маркетингові програми, умови переговорів з партнерами та конкурентами тощо;
- понад 90% економічної та військово-економічної інформації вилучаються з відкритих джерел;
- значно зростають витрати на ведення економічної інформаційно-аналітичної діяльності, але прибутки від неї стають надзвичайно великими;
- разом з традиційними засобами збору, аналізу і узагальнення розвідувальної інформації активно використовуються майже всі досягнення науково-технічної революції для вивчення розвідувальних даних;
- активне і ефективне ведення економічної інформаційно-аналітичної діяльності має особливе значення для тих держав, в яких з тих чи інших причин на певний час загальмувався економічний та науково-технічний прогрес.

Більш того, на нашу думку, активне застосування інформаційно-комунікаційних технологій у всіх сферах людського буття сприяло тому, що головним напрямком розвитку конкурентної розвідки стає широке використання електронної документації; електронних баз даних, корпоративних інформаційних систем, що використовують інтернет-технології, спеціальних комп'ютерних програм, прогнозуючих комплексів, систем моніторингу.

Як підсумок потрібно ще раз підкреслити, що необхідність застосування конкурентної розвідки на вітчизняних підприємствах обумовлюється неможливістю отримати керівництвом підприємства необхідну інформацію від базових структурних підрозділів.

Водночас, ефективна реалізація конкурентної розвідки уможливорює досягнення цілей стосовно гарантування економічної безпеки підприємства через розпізнавання, ідентифікацію та локалізацію загроз та ризиків, джерелами виникнення яких є зовнішнє середовище, а також більш ефективне використання корпоративних ресурсів.

4.3. Методичні аспекти здійснення конкурентної розвідки

Основне завдання сучасного бізнесу, насамперед великого та середнього, полягає в утриманні й здобутті конкурентних переваг на ринку. Як зазначалось уже вище, ключова умова виконання цього завдання полягає в отриманні достовірної інформації про зовнішнє середовище, що можливо здійснити шляхом розвідувальної діяльності. Використовуючи нелегальні методи отримання інформації, тобто методи промислового шпигунства, підприємство не лише ризикує запламувати власну репутацію, але і уможливорює виникнення підстав для порушення кримінальної справи, тому в Європі, США та інших розвинутих країнах дедалі більшої популярності набуває діяльність, яка підпадає під визначення «конкурентна розвідка».

Необхідність застосування конкурентної розвідки на вітчизняних підприємствах зумовлюється складними умовами здійснення господарської діяльності, коли забезпечення необхідного для подальшого розвитку рівня безпеки є можливим лише у випадку виконання певної протилежності. З одного боку, – це намагання своєчасно виявити і нейтралізувати інформаційні загрози, що виходять від наявних й потенційних конкурентів, з іншого, – це намагання створити аналогічні інформаційні загрози конкурентам. Інакше кажучи, забезпечення безпеки є можливим за умови максимально можливого втаємничення конкурентом значимої інформації, що стосується власного бізнесу, та якомога повнішої інформаційної відкритості конкурентів, щоб своєчасно збагнути їх наміри й плани. Звідси, логічний висновок: без ефективного функціонування конкурентної розвідки керівництво підприємства не здатне приймати вірні рішення, адекватні певній ситуації.

Виходячи із узагальненого у попередніх підрозділах історичного досвіду розвитку розвідувальної діяльності можна стверджувати, що розвідка як вид людської діяльності є різновидом конкретної праці щодо збирання, обробки та представлення інформації у вигляді даних керівникам. В процесі цієї праці люди вступають у економічні відносини щодо виготовлення, обміну, розподілу й споживання специфічного продукту – інформації, що з часом набирає товарної форми. Виробником інформації виступає розвідка

(в нашому випадку служба конкурентної розвідки), а споживачем – замовник, керівник, а іноді й держава (в нашому випадку топ-менеджер, керівник підприємства). Праця співробітника конкурентної розвідки полягає у збиранні «сировинного» матеріалу, його аналізі, обробці та перетворення в кінцеву продукцію – дані, що мають доступну форму для сприйняття замовником. На малих підприємствах співробітник конкурентної розвідки є одночасно агентом-розвідником, аналітиком, маркетологом і писарем. На великих підприємствах, як правило, служба конкурентної розвідки внутрішньо структурована і має підрозділи агентури, аудиту й аналізу, власного філолога-аналітика тощо.

Виробничий цикл конкурентної розвідки починається зі спостереження за об'єктом і джерелом інформації, фіксації інформації, її аналізу й синтезу, абстрагування, позбавлення від зайвої та дезінформації, формування суджень, висновків, даних та пропозицій, надання останнім форми, що є доступною для споживання.

Важливим моментом у виробничому циклі є визначення об'єктів та джерел інформації. *Об'єкти* (англ. «Targets») – це люди чи документи, які можуть дати відповіді на питання, що цікавлять. Як правило, це первинні носії інформації. *Джерела* (англ. «Sources») – це люди чи засоби, які можуть допомогти отримати доступ до потрібних осіб та інформації безпосередньо або опосередковано. Вони поділяються на внутрішні й зовнішні. Внутрішні джерела – це особи, що працюють на власній фірмі, персонал компанії. Зовнішні джерела – це ті, хто працює на фірму, але не є її співпрацівниками. Звичайно до них відносять консультантів та клієнтів, а також аналітиків, журналістів та осіб, що добре інформовані. Крім цього джерела поділяють на первинні й вторинні. *Первинні* це ті, хто отримав інформацію безпосередньо від об'єкта й передав конкурентній розвідці. До інформації, отриманої з первинного джерела відноситься й інформація, що добута власноруч фахівцем конкурентної розвідки. *Вторинні* джерела (або інфраджерела) отримують інформацію «з других рук».

Можна виділити наступні категорії джерел, що володіють економічною інформацією чи містять її в собі: люди; документи; публікації; технічні носії; технічні засоби забезпечення виробничої і трудової діяльності; продукція; промислові і виробничі відходи. Розглянемо загалом кожну з цих категорій.

Люди. До цієї групи можна віднести співробітників, обслуговуючий персонал, робітників, продавців продукції, клієнтів, партнерів, постачальників, покупців і т.п. Люди в ряді джерел економічної інформації займають особливе місце як активний елемент, здатний виступати не тільки власне джерелом, але і суб'єктом зловмисних дій. Люди є і власниками і розповсюджувачами інформації в рамках своїх функціональних обов'язків. Крім того, вони ще здатні її аналізувати, узагальнювати, робити відповідні висновки, а також, за певних умов: ховати, продавати і робити інші, в тому числі кримінальні дії, аж до вступу в злочинні зв'язки зі зловмисниками.

Документи. Це найпоширеніша форма обміну інформацією, її нагромадження і збереження. Документ відрізняє те, що його функціональне призначення дуже різноманітне. Система документів має досить розгалужену структуру і є предметом особливого розгляду, тому що документ може бути представлений не тільки різним змістом, але і різними фізичними формами – матеріальними носіями.

За спрямованістю розрізняють організаційно-розпорядницькі, планові, статистичні, бухгалтерські і науково-технічні документи, які містять, власне кажучи, усю масу зведень про склад, стан і діяльність будь-якої організаційної структури від державного до індивідуального рівня, і про будь-який виріб, товар, задум, розробку. Така розмаїтість форм і змісту документів за призначенням, спрямованістю, характером руху і використання, приваблює до них підвищену увагу фахівців з конкурентної розвідки, як до найціннішого джерела важливої інформації.

Публікації. Це інформаційні носії у виді найрізноманітніших видань: книги, статті, монографії, огляди, повідомлення, рекламні проспекти, доповіді, тези і т.д. Відомо, що це найкращі джерела комерційної інформації. От чому конкурентну розвідку цікавлять різні з'їзди фахівців, конгреси, конференції, симпозиуми, наукові семінари, семінари по обміні досвідом і тому подібні публічні форуми. Тут досвідчені фахівці збирають найбільш свіжу і кошовну інформацію. Давно відомо, що більш 60% інформації, що є секретною, можна одержати з так званих «відкритих джерел», – преси, передач радіо і телебачення, книг, спеціалізованих журналів, наукових праць, звітів компаній, внутрішніх видань

підприємств, брошур і проспектів, що роздаються на ярмарках і виставках тощо.

Технічні носії. До технічних носіїв інформації належать кіно-, фото-матеріали (мікрофільми, кінофільми і т.д.), магнітні носії (стрічки, диски), відеодиски, відеофільми, роздруковки даних і програм на принтерах, інформація на екранах ЕОМ, промислових телевізійних установок, табло індивідуального і колективного користування й інші. Можливості технічних носіїв визначається високим темпом росту парку технічних засобів і ПЕОМ, що знаходяться в експлуатації, їхнім широким застосуванням у всіляких сферах людської діяльності, високим ступенем концентрації інформації і масштабністю участі людей у використанні цих носіїв у практичній діяльності.

Технічні засоби забезпечення виробничої діяльності. Технічні засоби як джерела економічної інформації є досить широкими і ємними в інформаційному плані. У групу засобів забезпечення виробничої діяльності входять різні засоби, такі, зокрема, як телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, кіносистеми, системи часофікації, охоронні і пожежні системи й інші, котрі за своїми параметрами можуть бути джерелами перетворення акустичної інформації в електричні й електромагнітні поля, здатні утворювати електромагнітні канали витоку конфіденційної інформації. Особливу групу засобів складають автоматизовані системи обробки даних (АСОД), тому що вони володіють великою інформаційною ємністю.

Продукція. Вона є особливим джерелом інформації, і за її характеристиками активно полюють конкуренти. Особливої уваги заслуговує нова продукція, що знаходиться на етапі підготовки до серійного виробництва.

Промислові і виробничі відходи. Відходи виробництва містять інформацію про використовувані матеріали, їх склад, особливості виробничого процесу, технологію.

У своїй сукупності джерела економічної інформації містять значний обсяг даних про склад, зміст і напрямок діяльності підприємства, що представляє собою значний інтерес для конкурентів.

Цикл обробки інформації включає чотири кроки:

- 1) відокремити важливу інформацію від неважливої;

2) максимально ефективно вибрати серед важливої інформації ту, яка відноситься до даного питання і є достовірною (виокремити достовірну інформацію), організувати її моніторинг ;

3) обробити цю інформацію таким чином, щоб вона повністю відповідала меті організації;

4) переконатися, що результати обробки інформації – усі висновки, судження, прогнози – зрозумілі для керівника, надані своєчасно й у тому вигляді, в якому з ними можна працювати.

Якщо послідовно зробити ці чотири кроки, то можна впевнено сказати, що «сира інформація» перетвориться у важливі, достовірні дані й що служба конкурентної розвідки виконала поставлені завдання. Перелічені кроки можна вважати типовими, стандартними для сучасної служби конкурентної розвідки незалежно від того, на якому підприємстві вона працює і який предмет зараз досліджує.

Першим та найбільш важливим принципом організації економічної розвідки є *об'єктивний підхід* при відборі, систематизації, обробці і передачі замовнику інформації. Оскільки цьому аспекту увагу було приділено вище, то ми його ретельно не будемо розглядати.

Наступним принципом є *системність інформації*. На основі цього принципу забезпечується достовірність інформації, а відповідно й якість та ефективність розвідки. Оскільки суб'єкти підприємницької діяльності являють собою складні системи, які включають такі підсистеми як фінансову, маркетингову, виробничу й інші, то всі вони є взаємопов'язаними між собою, а тому їх показники повинні взаємно підтверджуватись. Так фінансові показники повинні відповідати маркетинговим, маркетингові – виробничим, а виробничі – технологічним.

Важливе місце посідає такий принцип як *конфіденційність*. Оскільки конкурентна розвідка має справу і з секретною інформацією, тут формуються свої правила. Усю конфіденційну інформацію можна розділити на дві групи: ділову і технологічну. Ділова інформація включає в себе фінансові звіти і прогнози, банківські рахунки, умови контрактів і договорів, найближчі перспективні плани фірми.

До технологічних секретів можна віднести дані про науково-технічний потенціал підприємства, обсяг виробничих потужностей і рівень технології, конкретні ноу-хау, норми витрати сировини,

а також інформацію про незахищені патентами винаходи. Економічна розвідка має ряд способів доступу до комерційної таємниці. Найбільш поширеним є спосіб несанкціонованого доступу. Це сукупність прийомів, що дозволяють розвіднику отримати відомості конфіденційного характеру, що охороняються. До основних джерел, що містять конфіденційну інформацію, належать люди. Вони найактивніший елемент, здатний виступати не тільки в якості джерела інформації, але й бути суб'єктом впливу противника. До них належить обслуговуючий персонал, постачальники, партнери, покупці.

Раніше нами уже наголошувалося на тому факті, що успішне ведення розвідувальних операцій з економічних питань приносить вигоди в десятки разів більше в порівнянні з витратами. Водночас, ефективність конкурентної розвідки можна визначити шляхом порівняння результату та витрат на її проведення:

$$E_p = \frac{P_p}{B_p}, \quad (4.1)$$

де: E_p – ефективність розвідки; P_p – результат, отриманий від розвідки; B_p – витрати на проведення розвідки.

Існують три основних умови, що дозволяють ефективно використовувати принципи і методи розвідки, в тому числі і конкурентної, а саме: мистецтво розвідника, організація розвідки, щасливий випадок.

Мистецтво розвідника визначається його інтелектуальними критеріями: компетентністю, ерудицією, працездатністю, вмінням спілкуватися з людьми і навичками пошуку інформації.

Другою важливою умовою ефективного функціонування розвідки є її організація. В рамках якої повинні бути використані такі засоби, які дають можливість завдяки інформаційній базі отримати максимальні прибутки при найменших витратах.

Третьою умовою є щасливий випадок. Незалежно від рівня планування та організації не може передбачити форс-мажорних обставин, які можуть як позитивно, так і негативно вплинути на ситуацію, що склалася.

Ефективність отримання розвідувальної інформації багато в чому залежить від методів, які для цього застосовуються.

Варто підкреслити, що існує кілька класифікацій методів збору інформації в залежності від розв'язуваних задач. З погляду методології їх можна розділити на загальні, особливі та окремі.

Загальні методи збору інформації характерні не тільки для ділової розвідки, але і для наукових досліджень, менеджменту і т. д. Вони містять загальні положення, що визначають вірогідність, системність, своєчасність, цінність, корисність інформації тощо.

Особливі методи збору інформації в рамках досліджуваної тематики стосуються специфіки збору інформації в розвідці взагалі, у тому числі й конкурентної. Внаслідок цього застосовується своя класифікація, оскільки інформація, що добувається, має різноманітний соціально-економічний і правовий статус.

Насамперед, існують легальні джерела інформації: власна інформація компанії, яка оприлюднюється у відповідності із законодавством: рекламні проспекти, буклети, продукція і послуги, книги, наукові статті, публікації в засобах масової інформації, галузеві журнали, довідники і т.п. Ці відомості є відкритими, їх збір не суперечить ні карному законодавству, ні моральним нормам. Стосовно до конкурентної розвідки на рівні підприємства це означає, що подібні завдання, щодо збирання інформації про конкурентів без будь-якого морального збитку можуть бути поставлені перед працівниками відповідного підрозділу.

Наступна група джерел інформації не є об'єктом охорони цивільним і кримінальним кодексами, але разом з тим, оберігається від сторонніх осіб. Поширення і збір інформації цього роду стосується скоріше моральних норм взаємин, адже це конфіденційна інформація. Наприклад, відомості про переговори з партнерами, про взаємини і моральну атмосферу в колективі і т.д. Оскільки збір інформації подібного роду хоча і не спричиняє кримінальної чи цивільної відповідальності, але вважається не етичним, а відтак такі дії намагаються приховувати, оскільки вони мають напівлегальний відтінок.

Нарешті, інформація, що є таємницею підприємства, розкращання якої завдає йому економічних збитків. Відповідно до законодавства України, подібні дії спричиняють правову відповідальність, а збиток від розкращання конфіденційної інформації відшкодовується в судовому порядку. Важливо, що до уваги береться не вартість інформації, а втрачена вигода в зв'язку з її розкращанням.

Таким чином, з погляду *особливих методів*, всю інформацію можна поділити на три групи: відкриту (легальну), напівлегальну і таємну (нелегальну). І відповідно, методи збору можна також класифікувати як *легальні, напівлегальні і нелегальні*.

Окремі методи збору стосуються певної інформації в конкретній ситуації, а відтак вони самі є таємними і розкриваються тільки тоді, коли втрачають актуальність, як, наприклад, використання поштових голубів для зв'язку.

Розглянемо ретельніше методи збору інформації. Особливостями легальних методів збору інформації є те, що з величезної маси матеріалу потрібно витягнути її незначну частку, яка є дійсно цінною. Наприклад, у газетному нарисі про конфлікт на певному підприємстві можна знайти деякі дані, що характеризують конкурента, а саме: про особистості менеджера, його спосіб життя чи відомості про нову технологію, що може бути використана в конкурентній боротьбі.

Збір інформації з легальних каналів повинен розгортатися за багатьма напрямками. На середніх і великих підприємствах роботу зі збору інформації розподіляють за напрямками: фінанси, виробництво, НДДКР, менеджмент, маркетинг, кадри та ін. До неї залучаються окремі працівники. Їм забезпечується доступ до необхідних легальних джерел інформації. За рахунок підприємства купуються книги, довідники, виписуються журнали, газети, включаються в мережу «Інтернет» і т.п. Якщо немає окремих джерел на підприємстві, службовцям, що займаються збиранням 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 стосовно досліджуваного об'єкта.

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 ви-

цих спеціальних навчальних закладів, що мають розвинуті навички аналізу й узагальнення матеріалу.

У сучасних умовах для цілей конкурентної 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 обумовлюється в службових обов'язках працівників цих установ. Зразок організації такої легальної розвідки демонструє Японія, яка створила ефективну систему збору науково-технічної і комерційної інформації про своїх закордонних конкурентів.

Наступним етапом в роботі з інформацією є її систематизація. Серед об'єктів розвідки у першу чергу виділяються конкуренти, постачальники, споживачі, керівники органів державного і місцевого управління профспілкових організацій, політичних партій і рухів. У 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, НДКРР), менеджмент, маркетинг і персонал (рис. 4.1.).



Рис. 4.1. Схема логічної бази даних конкурентної розвідки підприємства

Систематизований у такий спосіб матеріал підлягає подальшій аналітичній обробці.

Окремо потрібно наголосити на тому факті, що при застосуванні легальних методів збору інформації в інформаційному потоці може знаходитися дезінформація конкурента, яку той навмисно запустив для приховання дійсного стану, наприклад, щоб одержати кредит, замовлення, уникнути офіційного визнання банкрутства тощо.

Напівлегальні методи збору інформації. Як відзначалося уже вище, ці методи збору інформації найчастіше торкаються моральних норм міжособистісних взаємин, етики менеджменту, підприємництва, конкурентної розвідки, тому їх не прийнято афішувати. Арсенал напівлегальних методів збору інформації досить широкий. Серед них можна виділити такі як бесіди з фахівцями конкурента в неформальних умовах, удавані переговори про покупку продукції конкурента, несправжні конкурси, зманювання з роботи провідних спеціалістів конкурента, одержання інформації від спільних постачальників, споживачів, через фонди і благодійні організації, через органи контролю тощо.

Найпростіший спосіб одержати необхідну інформацію – *це провести бесіду з фахівцем конкурента за неформальних умовах* (на прийомі, за сніданком, вечерею, на відпочинку і т.п.). Головне тут – створити невимушену обстановку, без видимого інтересу спонукати співрозмовника на обговорення проблем, що цікавлять замовника розвідувальних дій, дати йому можливість висловитися і вміти вислухати.

Наступний, напівлегальний спосіб одержання інформації – *удавані переговори з конкурентом про покупку його продукції, патенту, ліцензії, ноу-хау з наступним відмовленням*. Під час переговорів, цілком природним виглядає інтерес до особливостей продукту, технології, винаходу і т.д.

Таким чином, 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 зазнав аварії. Водночас цей метод нерідко спрацьовує, оскільки важко визначити з дійсними чи помилковими намірами звертається клієнт. Це стане відомим тільки тоді, коли після відмови клієнта від укладання угоди в нього раптом з'являється

власний аналог чужого продукту з ідентичними найважливішими технологічними параметрами.

Великі можливості одержання необхідної інформації про конкурента дають *несправжні конкурси й оголошення про найм на працю*. Методика їх проведення наступна: спочатку виявляються на підприємстві-конкуренті фахівець-носії інформації; вивчаються всі його особисті дані: професійний рівень, кваліфікація, здібності і дарування, захоплення, моральний вигляд, родинний стан, коло друзів, спосіб життя і т.д.; усі ці дані оцінюються з погляду можливості одержання інформації протягом фальшивих переговорів.

Іншою можливістю одержати конфіденційну інформацію напівлегальним чином є запрошення до співробітництва працівників посередницьких структур, що обслуговують і конкурента (постачальників, дистриб'юторів, брокерів, службовців банківських, страхових і транспортних компаній і т.д.). До цієї групи належать і спеціальні консалтингові фірми, працівники науково-дослідних установ, викладачі навчальних закладів.

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 кампанії, як «Дженерал електрик», «Вестингауз» та деякі інші підтримували у фінансовому відношенні американську місію «Нові племена», що вела роботу із християнізації недоторканих цивілізацією племен у 16 країнах Латинської Америки. Представники місії, як правило, розгортали свою роботу серед тих племен, що проживали на території з перспективними покладами корисних копалин.

Не менш важливу роль у напівлегальних і нелегальних способах одержання важливої інформації споконвічно грала жіноча і чоловіча краса. Суть методу полягає у використанні особливостей біологічної природи людини, коли гра на почуттях, дає можливість одержати необхідну інформацію.

Ще одним каналом отримання економічної інформації, є наукові контакти: *конференції, симпозиуми, семінари* і т.п., що проводяться на міжнародному рівні і на яких відбувається вільний обмін науковими ідеями.

Значні можливості для одержання науково-технічної інформації існують при встановленні через фонди стипендій, грантів.

Варто мати на увазі, що їхні учасники – молоді науковці з країн, де рівень життя нижче, маючи високий творчий потенціал, нерідко добре знаючи стан експериментального сектора науки і прагнучи одержати гранти, стипендії готові співпрацювати.

Незаконні методи збору інформації. Як підкреслювалося вище, незаконні методи збору розвідувальної інформації, стосуються комерційної таємниці, яка охороняється власником і законом і не використовується конкурентною розвідкою, але фахівцям з конкурентної розвідки, а ще більше фахівцям з контррозвідки треба мати чіткі уявлення про ці методи збору інформації. Коротко ми їх уже розглядали в контексті загальної характеристики промислового шпигунства і вважаємо, що забезпечення безпеки підприємства потрібно здійснювати виключно законними методами.

Розрізняють два види роботи служби конкурентної розвідки: стратегічна і оперативна. Завдання стратегічного різновиду за змістом близькі до завдань стратегічного планування і маркетингу, вони зводяться до визначення структури і динаміки тієї сфери господарсько-економічної діяльності, в якій працює (або збирається працювати) підприємство, з виявленням й аналізом всіх конкурентів та контрагентів.

Оперативна конкурентна розвідка вирішує нагальні проблеми негативної взаємодії з конкретним конкурентом і, зазвичай, діє на межі етично-юридичних норм і засобів.

Предметом інтересу стратегічної конкурентної розвідки найчастіше є: законодавство (та його частина, що регламентує процеси й обставини, пов'язані з діяльністю підприємства); конкуренти (справжні і потенційні); ринки (що існують і потенційно можливі); нові технології і питання інтелектуальної та промислової власності; ресурси (при намірі підприємства розширити або виробничі, або збутові можливості); тенденції зміни всіх перерахованих вище об'єктів. У свою чергу інтерес оперативної розвідки – істотно інший: історія фірми-конкурента; відомості про її керівництво; структура фірми-конкурента, особливості організації її виробництва; маркетинговий стиль, стратегія конкурента; дослідницькі роботи фірми-конкурента, її перспективні плани; зв'язки з владними структурами, лобіювання; кадрова політика фірми-конкурента.

Сталої і загальновизнаної методики конкурентної розвідки немає. Здійснюючи конкурентну розвідку, відповідний господарю-

ючий суб'єкт переважно розробляє власну методику. Проте, існують і відомі методики конкурентної розвідки. Розглянемо окремі з них ретельніше. Так, Харківське об'єднання аналітиків і професіоналів конкурентної розвідки (SCIP.ORG.UA) дотримується погляду, що існують п'ять етапів, які об'єднані під назвою «Розвідувальний цикл обробки інформації», у результаті якого «сира» інформація перетворюється в «аналітичні матеріали» або знання: планування і вибір об'єкта; збір опублікованої інформації; збирання інформації із первинних джерел; аналіз зібраної інформації і створення нового продукту; доведення результатів до замовників (рис. 4.2) [31]. Сильною стороною цієї методики є те, що вона підкреслює необхідність переходу до первинних джерел після того як проведена робота із публікаціями.

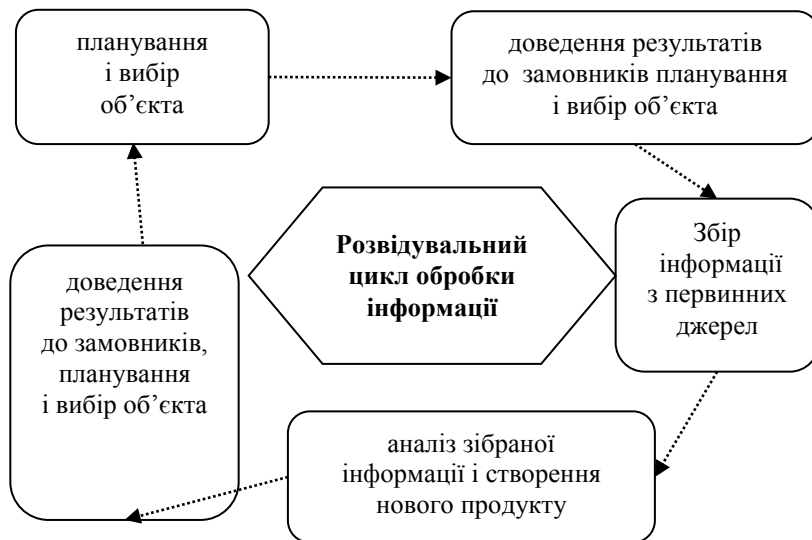


Рис. 4.2. Розвідувальний цикл обробки інформації

В методиці, що використовується членами Європейського об'єднання професіоналів конкурентної розвідки, яка представлена на рис. 4.3, зосереджено увагу на необхідність використання результатів діяльності конкурентної розвідки [35].

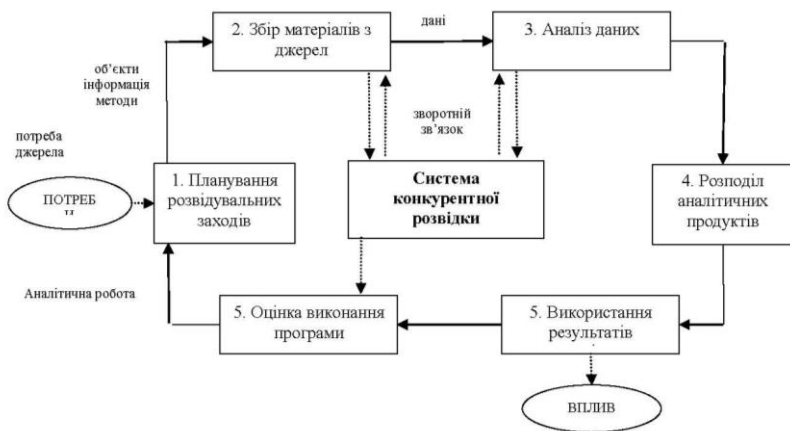


Рис. 4.3. Методика із зворотнім зв'язком
(за версією Ештон&Стейсі (Ashton&Stacey))

Назва «Методика 4С» – похідна від перших літер англійських слів, а саме: Collection (збір інформації), Conversion (перетворення інформації в готовий продукт), Countering (передача споживачу інформації), Communication (включення інформації у процес прийняття рішень) [8]. Ключовим в цій методиці є положення, згідно з яким інформація, отримана у процесі конкурентної розвідки, залежить від змін потреб (рис. 4.4).

Кожен етап процесу, описаного у моделі 4С, містить у собі велику кількість субпроцесів. Перша частина стадії збирання інформації – визначення потреб користувача, або «ключових питань» [45]. Ключові питання встановлюються під час бесіди користувача зі співробітником розвідки, щоб чітко визначити його інформаційні потреби, або навпаки, користувач сам запитує у розвідки інформацію, необхідну йому для конкретних цілей.

Методика запропонована Артуром Вайсом, який є одним із керівників компанії АWАRЕ, яка спеціалізується на конкурентній розвідці і розробці стратегій бізнесу (рис. 4.5) передбачає отримання чотирьох різних, але пов'язаних між собою, типів знань про конкурентів і конкурентне середовище, а саме:

- характеристика конкурента (competitor knowledge) – інформація про окремих конкурентів;

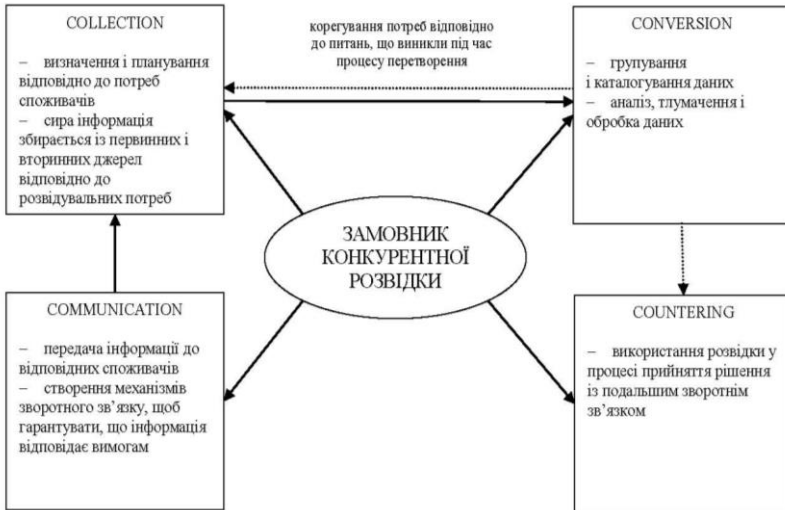


Рис. 4.4. Методика 4С

- порівняльна характеристика (comparative knowledge) – інформація про спільні та відмінні характеристики різних конкурентів;
- характеристика ринку (market knowledge) – розширена інформація про ринок, зокрема споживачів, постачальників, канали реалізації, технології, конкуренцію у галузі, партнерів тощо.
- характеристика самих себе (self-knowledge) – інформація про власну компанію [9].

Усі чотири категорії необхідні для побудови цілісної і повної картини ділового оточення компанії. Лише на основі повного розуміння власного становища на ринку і знанні конкурентів можна приймати правильні рішення, які приведуть до досягнення ринкових переваг і захисту від загроз.

Методика, представлена на рис. 4.6, порівнює конкурентну розвідку із комунікацією. Інформація найчастіше разова й однонаправлена, а комунікація постійна (регулярна) і взаємонаправлена. При комунікації джерело і кореспондент постійно міняються місцями, інформаційні потоки регулюються за допомогою зворотного зв'язку.

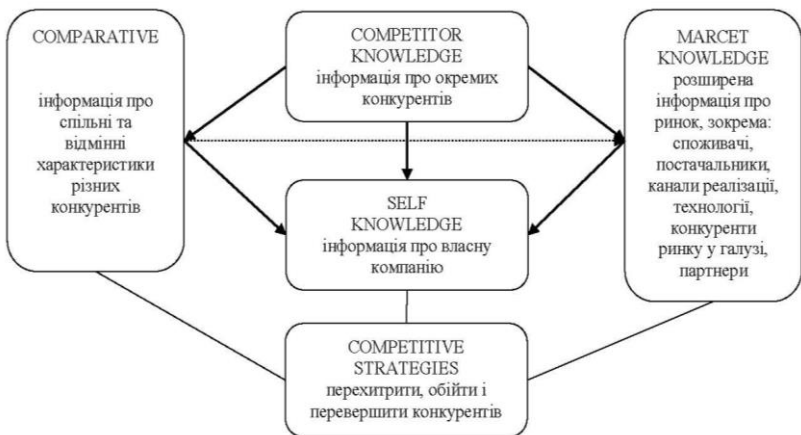


Рис. 4.5. Методика чотирьох типів знань компанії AWARE

Конкурентна розвідка як комунікація результатом передбачає відповідні дії.

На збирання й оброблення даних безпосередньо впливають зміни, що є результатом дій, на саму систему й оточуюче середовище, постійно відбувається корегування завдань, тому ефективність комунікації значно вища [25].

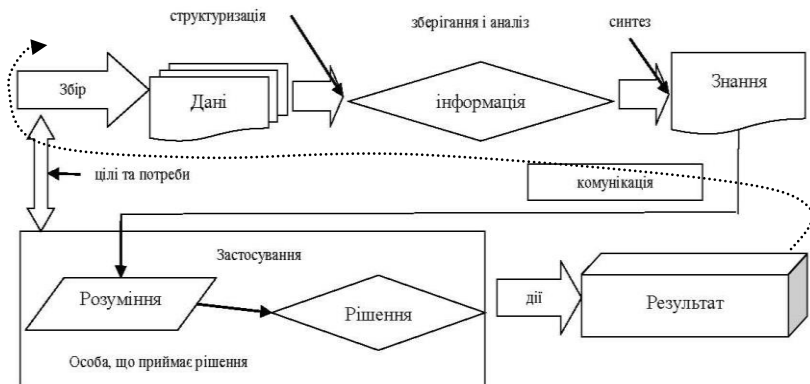


Рис. 4.6. Методика ототожнення конкурентної розвідки та комунікації

Методика 4К+1, представлена на рис. 4.7, передбачає збирання інформації в невеликому переліку привілейованих джерел – «Сімейство джерел» [39].

Однак економічна діяльність завжди пов'язана з виходом інформації в зовнішнє середовище, тому отримання інформації про підприємство може здійснюватися через певні канали.

Перший канал: відкриті загальні й спеціальні публікації й бази даних.

Другий канал: клієнти, постачальники, інвестори, кредитні організації, посередники, агенти.

Третій канал: суспільні служби, адвокатські контори, аудиторські фірми, страхові компанії, консультанти, податкові інспекції, санітарні й пожежні служби, органи статистики, правоохоронні органи.

Четвертий канал: представництво на ярмарках, салонах, конференціях.

Розглянемо ці канали більш докладно.

1. Використання відкритих загальних і спеціальних публікацій і баз даних у якості об'єктів аналітичної обробки дозволяє одержати 30–40% інформації. Їх доступність практично нічим не обмежена, крім вартості передплати на інформаційні видання, бази даних і вартості аналітичної роботи. У наш час налічуються десятки інформаційних видань. Ці джерела дозволяють одержати досить свіжі відомості, які можуть бути використані для організації розвідувальної роботи конкуруючими підприємствами.

2. Клієнти, постачальники, інвестори, банки, посередники, агенти одержують інформацію в результаті контактів персоналу підприємства з ними як зі своїми партнерами.

Через цей канал також може проходити від 30 до 40% інформації.

Структура інформації, що проходить по цьому каналу, якщо її класифікувати по підставі запитання «про що?», має наступну характеристику:

- 60% інформації – про конкурентів, ринок, ресурси;
- 15% – про технологію;
- 15% – про регламентуючі документи;
- 10% – про тенденції розвитку.

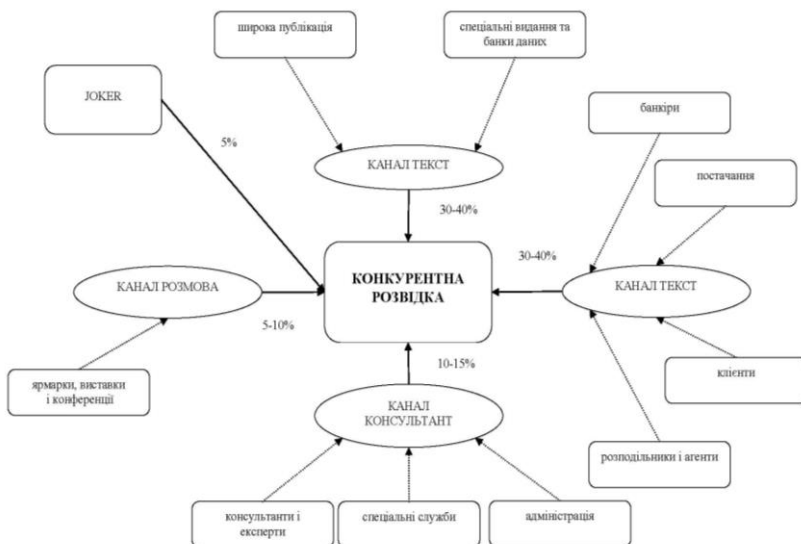


Рис. 4.7. Методика 4K+1

3. Залучені до співробітництва з підприємством експерти суспільних служб і консультанти, можуть надати 10–15% інформації. Робота консультантів і експертів сторонніх консультаційних і експертних фірм завжди несе деяку ймовірність порушення роботи підприємства.

4. І останній канал розвідувальної діяльності – представництво на різних організаційних формах демонстрації продукції й можливостей – дозволяє одержувати 5–6% інформації.

Однак ступінь вірогідності цієї інформації досить висока, якщо вона сприймається підготовленими фахівцями, які перед відвідуванням заходів даної групи джерел ознайомилися з каталогами, що анонують ці заходи.

Суттєва відмінність в методиках здійснення конкурентної розвідки спонукала нас, з метою удосконалення існуючих методичних засад, до розроблення типового алгоритму дій здійснення конкурентної розвідки, який не враховує специфіки кожного з них, але містить ключові етапи у наступній послідовності (рис. 4.8).

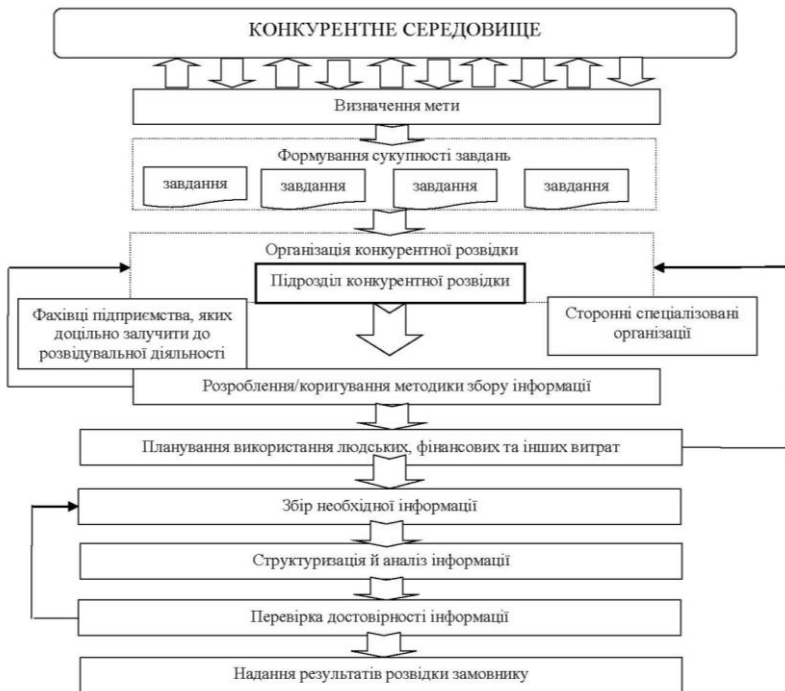


Рис. 4.8. Алгоритм здійснення конкурентної розвідки

Коротко охарактеризуємо кожен етап алгоритму.

1. Формулювання проблеми, яку необхідно вирішити, тобто чітко визначення мети.

2. Конкретизація проблеми через формування сукупності завдань. Це може виразитися, наприклад, в складанні зразкового списку ключових питань, на які потрібно відповісти для успішного досягнення поставленої мети.

3. Організація конкурентної розвідки передбачає, у відповідності до здійсненої конкретизації, оцінку обсягу, складності та вибору методу, виконавців та формування попереднього кошторису. Ретельне виконання цього пункту може значно полегшити всю подальшу роботу, оскільки може виявитися, що частину задач можна відкласти, частину розв'язати простішими засобами, частина їх вже має готове рішення, а частина взагалі є зайвою. За результа-

тами такого ранжування завдань створюється власний підрозділ конкурентної розвідки та/або доукомплектовується існуючий необхідними фахівцями. Окрім цього, якщо за попередньою оцінкою внутрішній підрозділ не зможе у повній мірі виконати поставлені завдання, то вирішується питання щодо залучення сторонніх фахівців чи укладання угоди із спеціалізованими організаціями.

4. Розроблення методики збору інформації залежно від того, з якими джерелами передбачається працювати.

5. Рациональний розподіл людських ресурсів, які залучаються до збору інформації. Так, збір інформації з Інтернет і робота з людьми вимагає абсолютно різного підходу, властивостей характеру і умінь. Особливо це торкається спілкування з людьми, що володіють інформацією. На цьому ж етапі створюється календарний план заходів, визначаються дати подання проміжних-контрольних звітів та уточнюються кошторис витрат.

6. Збір необхідної інформації (люди, книги, газети, журнали, Інтернет).

7. Структуризація й аналіз зібраної інформації.

8. Перевірка достовірності отриманої інформації через узгодження отриманих даних з різних джерел.

9. Представлення інформації у вигляді коротких висновків

10. Своєчасно подання висновків керівникам, які приймають рішення.

Потрібно ще раз підкреслити, що запропонований алгоритм не враховує ні масштабів діяльності, ні специфіки, ні наявного досвіду та характеру об'єкту конкурентної розвідки, тобто може служити виключно орієнтиром.

4.4. Конкурентна розвідка та контррозвідка як складові системи економічної безпеки підприємства

У попередніх підрозділах нами було ретельно розглянуто сутність та методичні засади здійснення конкурентної розвідки. Водночас, неодноразово наголошувалось, що розвідувальна діяльність сьогодні проводиться більшістю вітчизняних підприємств,

а відтак поруч із потребою отримання достовірної інформації про конкурентне середовище не менш актуальною і важливою є проблема захисту власних таємниць, тобто виникає проблема ефективного функціонування контррозвідки.

З біблійних часів і до нашого «цифрового» століття в розвідці існують чітко визначені принципи, які залишаються непорушними донині. Серед них – зв'язок між збиранням розвідувальних даних і захистом власної інформації. За одним із визначень, «контррозвідка – це захист своєї конфіденційної інформації від шпигунства». Слід зазначити, що тільки з переходом підприємств до ринкових відносин економічна (промислова) контррозвідка одержала легітимність і стала складовим елементом ділового процесу. В умовах конкуренції роль вивчення намірів конкурента і приховування своїх планів стає визначальною. Як і в традиційній контррозвідці, запобігання розкриттю своїх джерел інформації (нехай навіть і відкритих), а також методів збору інформації для конкурентної контррозвідки є пріоритетним завданням. Особливо розвинена ця система в США, за довгі роки практики американські розвідники і контррозвідники розробили методики і технології захисту як збору даних про конкурентів, так і захисту власної компанії від просочування конфіденційної, стратегічно важливої інформації. Багато вітчизняних підприємств ще в 90-і рр. на етапі становлення роботи своїх служб безпеки брали приклад із західних фахівців з конкурентної розвідки, а також охоче залучали до роботи колишніх працівників спецслужб.

У найзагальніших рисах процес конкурентної розвідки і контррозвідки в системі економічної безпеки підприємства складається з трьох етапів: внутрішнього моніторингу, зовнішнього моніторингу і аналітичної роботи.

Внутрішній моніторинг припускає, що працівники служби безпеки всіляко захищають підприємство від проникнення «шпигунів» і розвідників, а також відстежувати дотримання співробітниками підприємства внутрішніх правил щодо нерозголошення конфіденційних даних. Для цих потреб активно застосовуються і спеціальні інформаційні системи. Однією із найбільш поширених є ІРС (Information Protection and Control), яка захищає інформацію методом шифрування носіїв, а також повним контролем всіх можливих носіїв і каналів, через які, з технічної точки зору, може відбува-

тися витік важливої інформації (e-mail, icq, Skype, соціальні мережі, принтери, зовнішні носії, накопичувачі, USB, WiFi, Bluetooth і так далі). Особливої цінності така система набуває, враховуючи той факт, що до 75% конфіденційної корпоративної інформації розголошується мимоволі, помилково або з необачності персоналу.

Зовнішній моніторинг, відповідно до вище викладених положень, – це і є конкурентна розвідка в найбільш загальному розумінні. Він припускає збір повного об'єму інформації про конкурентів: технології, управління, об'єми збуту, чинники конкурентної переваги, стратегічні плани на майбутнє, стратегії завоювання ринку, можливі загрози для власного підприємства, методи оптимізації роботи, інновації і так далі.

Аналітична робота припускає проведення порівняльної характеристики, виявлення своїх сильних і слабких сторін, розробку конкретних рекомендацій для менеджменту з метою недопущення збитків, втрати частки ринку тощо.

Для того щоб інформація, яка належить підприємству, набула підстав для правового захисту, її слід подати як комерційну таємницю й конфіденційну інформацію, що є власністю підприємства. Цей аспект як полегшує роботу контррозвідки, так і ускладнює, адже вимагає виконання певної процедури щодо визначення інформації як комерційної таємниці.

Необхідно зауважити, що чіткого нормативного регламентування процесу організації та реалізації режиму комерційної таємниці немає. Існує тільки імперативна вказівка на те, що комерційна таємниця має бути «предметом адекватних існуючим обставинам заходів збереження її секретності».

Користуючись правом, закріпленим у ч. 5 ст. 30 Закону України «Про інформацію» підприємство у своїх нормативних документах визначає порядок одержання, використання, поширення та зберігання комерційної таємниці. Важливо зазначити, що процес оформлення та реалізації режиму обмеженого доступу до комерційної таємниці має бути економічно та юридично обґрунтованим і проводитись в декілька етапів, які логічно витікають один з одного.

Перш за все зазначимо, що згідно зі ст. 36 Господарського кодексу України 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. Відповідно до ст. 505 Цивільного кодексу України комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі й 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 чим має комерційну цінність і була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону.

Відповідно до положень чинного законодавства інформація є комерційною таємницею за наявності таких ознак: 1) має дійсну або потенційну комерційну цінність унаслідок необізнаності з нею третіх осіб; 2) до неї не існує вільного доступу на законних підставах; 3) власник або уповноважена ним особа вживає заходів щодо збереження її конфіденційності. Інформація, що становить комерційну таємницю, повинна бути зафіксована на матеріальному носії (папері, магнітному чи оптичному носії, фотонегативі чи іншому матеріальному об'єкті) та забезпечена реквізитами, що дозволяють ідентифікувати її. Це можуть бути: результати дослідів і їх протоколи, дані про якість матеріалів, документація з виготовлення продукції, креслення, формули та рецепти, статистичні розрахунки, звіти про виготовлену продукцію або надані послуги, картотеки й електронні бази даних клієнтів, відомості про організацію виробництва, методи реклами, інформація про джерела фінансування тощо. У деяких ситуаціях інформація, що становить комерційну таємницю, може втілюватися в предметах – виробках, блоках, агрегатах, приборах і речовинах. Однак і в цьому разі для визнання відомостей, втілених у предметах, комерційною таємницею необхідно, щоб інформація була попередньо задокументована в установленому порядку.

Поруч із поняттям «комерційна таємниця» окремо виділяється «банківська таємниця», збереження якої регламентується окремими законодавчими актами. Банківською таємницею вважається інформація щодо діяльності й фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин

з ним чи третіми особами при наданні послуг банку й розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

Банківською таємницею, зокрема, є: 1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України; 2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3) фінансово-економічний стан клієнтів; 4) системи охорони банку та клієнтів; 5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; 6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7) інформація щодо звітності по окремому банку за винятком тієї, що підлягає опублікуванню; 8) коди, що використовуються банками для захисту інформації; 9) інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду [29].

Документальне забезпечення правового статусу комерційної таємниці та конфіденційної інформації на підприємстві сприятиме надійному її захисту як у випадку розголошення відповідних відомостей працівниками підприємства, так і цілеспрямованими діями конкурентів щодо її викрадення. Зазначене стає можливим при послідовному поетапному виконанні наступних організаційних дій.

1. Існування комерційної таємниці та конфіденційної інформації бажано обумовити в установчих документах підприємця, включивши, наприклад, в установчий договір й (або) статут підприємства розділ, що регламентує захист інформації з обмеженим доступом.

2. При формуванні переліку відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства, його керівник видає наказ про відбір відомостей, які мають становити комерційну таємницю, що є підставою для створення комісія, яка, враховуючи пропозиції керівників всіх структурних одиниць підприємства, складає перелік відомостей, що належать до комерційної таємниці та конфіденційної інформації. До складу комерційної таємниці повинні бути віднесені різні види ноу-хау; відомості про винаходи і рацпропозиції, які не захищені авторським або патентним правом; інформація про факти укладання договорів і їхній зміст.

3. Особливу увагу необхідно приділити розробці положення про комерційну таємницю та конфіденційну інформацію на підприємстві. Таке положення є основним у системі правового захисту інформації від несанкціонованого доступу. У ньому розкриваються загальні положення у сфері захисту інформації, принципи і процедури розмежування доступу до такої інформації, порядок прийому, реєстрації, інвентаризації та обліку носіїв інформації, що містить комерційну таємницю та конфіденційну інформацію. У такому положенні прописуються також механізм забезпечення схоронності інформації, що є комерційною таємницею та конфіденційною інформацією, зокрема деталізуються процедури забезпечення доступу до комерційної таємниці сторонніх осіб (включаючи контролюючі органи). Рекомендується закріплювати правило, згідно з яким сторонні особи допускаються до ознайомлення з документами, що містять комерційну таємницю та конфіденційну інформацію, з дозволу керівника при обов'язковій наявності письмового запиту. При цьому такі особи повинні видати розписку про нерозголошення комерційної таємниці або укласти угоду з підприємством про таке нерозголошення. У положенні рекомендується прописати порядок поширення комерційної таємниці та конфіденційної інформації, а також процедуру виключення інформації з переліку комерційної таємниці та конфіденційної інформації.

4. Інструкція про порядок підготовки, обліку, зберігання та знищення документів, справ, видань і матеріалів, що містять комерційну таємницю та конфіденційну інформацію підприємства, встановлює конкретні механізми охорони комерційної таємниці та конфіденційної інформації.

5. Рекомендується включати норму про нерозголошення комерційної таємниці та конфіденційної інформації в трудовий договір (контракт) як керівника підприємства, так й інших співробітників.

Працівник під розписку повинен бути попереджений про відповідальність за невиконання взятих на себе зобов'язань. У трудовому договорі (контракті) або його невід'ємній частині (зобов'язанні про нерозголошення інформації, що становить комерційну таємницю) варто передбачити порядок ознайомлення працівника з діючими на підприємстві положеннями й інструкціями із забезпечення схоронності комерційної таємниці.

7. На підприємстві варто розробити спеціальний договір про збереження комерційної таємниці та конфіденційної інформації. Дотримання даної рекомендації дозволить представникам підприємця почувати себе впевнено при проведенні перевірок контролюючими органами. Перевіряючі повинні будуть дотриматися всіх процедур, які встановлені на підприємстві для одержання доступу до комерційної таємниці. І природно, підписавши документ про нерозголошення комерційної таємниці та конфіденційної інформації, такі особи не мають права використати отриману інформацію у своїй діяльності без згоди керівництва підприємства.

8. Правила внутрішнього розпорядку і посадові інструкції осіб, що працюють із комерційною таємницею, а також інструкції про ведення переговорів, інструкції про роботу з документами також повинні містити застереження про комерційну таємницю та конфіденційну інформацію.

9. Застосування технічних засобів захисту відомостей.

10. Особливістю організації інформаційних потоків на підприємстві з метою захисту «критичної» інформації, протидії промисловому шпигунству та організації дезінформування є розробка на підприємстві Порядку поширення інформації з обмеженим доступом, яка належить підприємству.

Керівник підприємства вирішує всі питання щодо розповсюдження власними силами, оприлюднення через ЗМІ та реалізації права на розпорядження комерційної таємниці. Проте необхідно взяти до уваги виняток, зафіксований в ч. 11 ст. 30 Закону України «Про інформацію»: «Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист».

Тобто, звідси слідує, що питання про оприлюднення через ЗМІ інформації, що становить комерційну таємницю та конфіденційну інформацію, вирішує керівник підприємства за винятком випадків, коли така інформація підпадає під кваліфікацію ч. 11 ст. 30 Закону України «Про інформацію».

У криміналістичній літературі слушно зазначається, що не існує тотожних злочинів. Водночас кожна одиночна подія – це вияв однотипних (однопорядкових) подій, що характеризуються наявні-

стю не тільки індивідуальних, а й типових ознак [26; 42]. Способи конкретного виду злочину мають загальні ознаки, які повторюються, що дає змогу узагальнити їх, тобто типізувати системи операцій і прийомів злочинних діянь.

Можна виділити три групи типових способів злочинних посягань на відомості, що становлять комерційну або банківську таємницю:

1) незаконне збирання відомостей, що становлять комерційну або банківську таємницю;

2) незаконне використання таких відомостей;

3) умисне розголошення такої інформації.

Незаконне збирання відомостей може виявлятися у:

1) викраденні відповідної інформації чи об'єктів, що її містять, з приміщень, де вони зберігалися. Така крадіжка може бути як відкритою, так і завуальованою, коли справжні предмети посягання (документи, вироби, що містять комерційну таємницю) викрадаються разом із іншими і в такий спосіб створюється хибне уявлення про дійсні цілі злочинців;

2) таємному проникненні злочинця до приміщення й копіювання інформації паперовим чи електронним способом. Для фіксації інформації та її пересилання можуть застосовуватися мобільні телефони з вбудованими фотокамерами й послуга MMS;

3) підкупі співробітника підприємства, який мав чи має законний доступ до інформації. Працівник за певні матеріальні чи інші блага копіює інформацію та передає її замовникові. Якщо людина вже звільнилася або на сьогодні не має законного доступу, але інформація, якою вона володіла раніше, ще не втратила комерційної привабливості, то вона її просто повідомляє;

4) підкупі посередників у переговорах, які володіють певною інформацією;

5) незаконному отриманні інформації у співробітників правоохоронних або контролюючих органів, яким вона стала відома внаслідок виконання ними службових обов'язків;

6) погрозах фізичним насильством над особою чи її близькими родичами, якій інформація була довірена в результаті виконання її трудових обов'язків;

7) шантажі працівника, який знаходиться на «гачку» внаслідок певних життєвих обставин;

8) впровадженні свого агента в штат підприємства під виглядом звичайного співробітника;

9) вербуванні діючого працівника або спонуканні до розголошення звільненого із застосуванням мотивів етнічної, расової, релігійної близькості, бажанням помститися керівникові за незаконне звільнення, переведення на іншу роботу, зняття з посади;

10) використанні різних технічних пристроїв, що фіксують і передають інформацію. За допомогою спеціальної техніки здійснюється прослуховування приміщень або зняття інформації з каналів зв'язку. Для цього застосовуються радіозакладки, мікрофони направленої дії, пристрої для зняття інформації з вікон за допомогою лазерних промінів, апаратура для виявлення й розшифрування електромагнітного випромінювання від офісної техніки, мініатюрні фото- та відеокамери. Таку техніку можуть встановлювати або використовувати як спеціально підготовлені особи, так і завербовані співробітники підприємства;

11) проникненні в комп'ютерні мережі. Для цього злочинці застосовують спеціальні комп'ютерні програми, які дозволяють відшукувати необхідні дані та копіювати їх.

Програмні засоби, які використовуються для несанкціонованого доступу, поділяються на декілька видів [15]:

– експлоіти (сканери) – програми, які використовують певні недоліки в програмному забезпеченні ЕОМ чи мережі, що призводить до настання бажаних для злочинця результатів;

– сніфери – дозволяють перехоплювати дані, що передаються мережами електров'язку;

– «троянський кінь» – програми цієї групи приховано встановлюються в будь-який спосіб на комп'ютері, що цікавить злочинців, як правило шляхом вбудовування в іншу легальну програму. При цьому програма-носії, виконуючи свої прямі функції, здійснює й додаткові, закладені в неї розробником (наприклад, збирання й передавання конфіденційної інформації);

– руткити – набір програм, який дозволяє злочинцю внести певні зміни в програмне середовище комп'ютера-жертви для здійснення контролю та отримання в подальшому легкого доступу до нього.

Незаконним використанням комерційної чи банківської таємниці є впровадження у виробництво або врахування під час

планування чи здійснення господарської діяльності без дозволу власника чи уповноваженої на те особи таких відомостей. Зокрема, незаконне використання може мати такі форми:

1) пред'явлення майнових або інших вимог до власника комерційної чи банківської таємниці за повернення або нерозголошення відповідних відомостей. Такі вимоги можуть стосуватися повернення на роботу, призначення на вищу посаду, звільнення іншого працівника, надання послуг тощо;

2) продаж інформації третім особам (електронних баз даних операторів телефонного зв'язку, ДАІ, БПІ та ін.);

3) обмін інформації, що становить комерційну чи банківську таємницю, на іншу або матеріальні цінності;

4) корегування своїх дій при укладанні договорів з власником такої таємниці.

Незаконне використання відомостей, що становлять комерційну або банківську таємницю, є можливим і в іншому вигляді, наприклад, умисне розголошення таких відомостей [21]. Розголошення може здійснюватися усно, письмово, із використанням засобів зв'язку й масової інформації, комп'ютерних мереж та ін. Таке розголошення вчиняють особи, яким ця інформація стала відома внаслідок професійної або службової діяльності. Це можуть бути як працівники самого підприємства, установи, організації, так і співробітники правоохоронних чи контролюючих органів, які отримали цю інформацію, користуючись своїм службовим становищем, але не для виконання своїх функцій, а для передавання конкурентам чи використання в інших протиправних цілях, наприклад, різних видах шантажу щодо здійснення чи нездійснення певних дій за нерозголошення комерційної або банківської таємниці.

Охарактеризованим вище злочинам щодо незаконного отримання і використання інформації, яка підлягає під визначення «комерційна таємниця» повинна протистояти контррозвідка. Водночас, на нашу думку, запобігання злочину є набагато ефективнішим засобом у порівнянні з ліквідацією наслідків. Зазначене обґрунтовується тим, що проведення внутрішнього моніторингу дозволяє визначити сукупність слабких місць, завчасна ліквідація яких і унеможливить реалізацію значної кількості загроз. Типовий перелік таких слабких місць для вітчизняних підприємств можна визначити наступною сукупністю.

Неефективна кадрова політика. Для більшості вітчизняних підприємств є традиційним здійснення найму на роботу працівників, послуговуючись таким критерієм як «родинні зв'язки». При цьому доволі частими є випадки, коли прийняті за таким принципом фахівці є абсолютно некомпетентними у своїй роботі. Більше того, практика показує, що наявність родинних або дружніх зв'язків не є гарантією порядності й чесності. Багато з таких працівників уміло користуються своїм особливим становищем, будучи впевненими в повній безкарності. Але навіть там, де працівники набираються на конкурсній основі, їх минуле, а також деякі людські якості перевіряються досить поверхнево. У результаті усередині підприємства, практично з моменту його відкриття виявляються потенційні зловмисники, про яких навіть не підозрюють.

Відсутність потрібного інструктажу та регулярних перевірок.

Більшість співробітників підприємства не має уявлення, що одержувана ними в ході роботи інформація є конфіденційною й не підлягає розголошенню. Звідси особливо важливим є проведення роз'яснення при прийомі на роботу щодо необхідності збереження комерційної інформації, визначення безпосередніх об'єктів, які підпадають під цю категорію, здійснення періодичних перевірок щодо дотримання даних вимог.

Відсутня мотивація робітника. Низький рівень заробітної плати та незадоволення умовами роботи можуть перетворитися на реальну загрозу для економічної безпеки підприємства.

Неефективне керівництво, яке спричинено низьким рівнем менеджменту, що ускладнює процес діяльності підприємства і негативно впливає на рівень його економічної безпеки.

Атмосфера в колективі. Одним з найважливіших факторів, від якого залежить не тільки безпека підприємства й ефективність його роботи, є взаємини в колективі. Усім відомо, що гарний колектив – запорука успіху підприємства. І дійсно, якщо працівник відчуває себе не найманцем, якого безжалісно експлуатують, а «членом родини» або частиною системи, то він, напевно, виявиться відданим власній фірмі. Якщо підприємство намагається допомогти працівникові з вирішенням особистих проблем, намагається піклуватися про свій персонал не на словах, а на ділі, то й працівник відповідь тим же. Він стане сприймати проблеми підприємства

як власні та, як наслідок, стане активно допомагати в їх ліквідації. Навпаки, ті колективи, відносини в яких прийнято називати «складними», є ласим шматком для зловмисників, які уміло використовують невдоволення й ненависть окремих співробітників та суттєво шкодять підприємству зсередини за допомогою його ж працівників.

Підводячи підсумки в проведеному дослідженні, доцільно взяти до уваги науковий доробок відомого фахівця з організації служб безпеки підприємств В. Мак-Мака, який у відомій книзі «Служба безпеки підприємства. Організаційно-управлінські і правові аспекти діяльності» не лише включив в організаційну діаграму служби безпеки підприємства відділ розвідки, але і приклав до загального опису діяльності розроблене ним положення про підрозділ розвідки, корпоративний нормативний документ, що визначає основні напрями її діяльності, функціональні обов'язки співробітників, їх права у взаєминах з іншими підрозділами компанії. Останнє важливо у зв'язку з тим, що до сил конкурентної розвідки корпорації належать і співробітники інших підрозділів компанії, що займаються збором і дослідженням інформації, підтримують комунікацію із співробітниками підрозділами розвідки. Значний внесок у формування структурних підрозділів служби безпеки підприємства вніс А.А. Мітрофанов [25].

Звернувшись до іноземного досвіду, як приклад можна привести організаційну структуру конкурентної розвідки американської корпорації Motorola, яка була першою корпорацією, що організувала таку структуру. Гібридна структура складається з центрального відділу розвідки, а також по одному-двох співробітниках інших підрозділів, яким доручено підтримувати комунікацію з відділом розвідки. В сукупності в корпорації Motorola конкурентною розвідкою займається до 30 осіб.

Правильно побудована взаємодія між підрозділами дозволяє отримати значну економію. Як показало дослідження, проведене в одній з європейських телекомунікаційних компаній, лише за рахунок централізації закупівлі і обробки інформації там за рік економиться до 20 мільйонів доларів.

Зважаючи вище викладені аргументи, нами створено модель функціонування системи економічної безпеки підприємства, в якій виокремлено діяльність щодо конкурентної розвідки та контр розвідки (рис. 4.9).

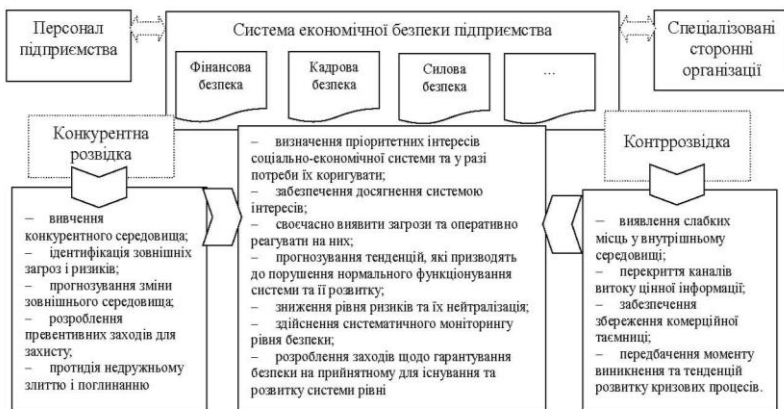


Рис. 4.9. Структурна модель системи економічної безпеки підприємства

Побудована модель не враховує специфіки діяльності певного підприємства, але відповідає ключовим позиціям сформованої у першому розділі роботи концепції забезпечення економічної безпеки підприємства та сучасним завданням, які ставляться перед системою економічної безпеки на вітчизняних суб'єктах господарської діяльності.

ЛІТЕРАТУРА ДО ЧЕТВЕРТОГО РОЗДІЛУ

1. Абрамов В. Деловая разведка в системе обеспечения предприятия / В. Абрамов // БДИ. – 2002. – № 2. – С. 22–26.
2. Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны / Г. А. Андрощук, П. П. Крайнев. – К. : Вид. Дім «ІнЮре», 2000. – 398 с.
3. Бараннік Р. В. Конкурентна розвідка: уявність та реальність / Р. В. Бараннік // Право України. – 2007. – № 11. – С. 72–76.
4. Безпекознавство: актуальні питання методології, методики та практики викликання : матеріали круглого столу 30 жовт. 2007 р. / М-во освіти і науки України, Європ. Ун-т, Навч.-наук. ін.-т права та безпеки підприємництва редкол.: І. І. Тимошенко [та ін.] ; відп. О. Й. Гринкевич. – К. : Вид-во Європ. ун-ту, 2007. – 167 с.
5. Белкин Р. С. Курс криминалистики / Р. С. Белкин. – [3-е изд. дополн.]. – М. : ЮНИТИ-ДАНА, Закон и право, 2001. – С. 731–739.
6. Боган К. Бизнес-разведка / К. Боган. – М.: Инглиш. – М.; СПб. : Вершина, 2006. – 363 с.
7. Борисов Н. И. Конкурентная разведка как инструмент конкурентной борьбы / Н. И. Борисов. [Электронный ресурс]. – Режим доступа : http://www.marketing.spb.ru/lib-research/competition_spy.htm.
8. Вайс А. Краткое руководство по конкурентной разведке: как собирать и использовать информацию о конкурентах : Часть 2 [Электронный ресурс] / А. Вайс. – Режим доступа : <http://it2b.ru/blog/arhiv/767.html>.
9. Вайс А. Сбор конкурентной информации / А. Вайс. [Электронный ресурс]. – Режим доступа : <http://it2b.ru/blog/arhiv/769.html>.
10. Воронова Ю. Конкурентная разведка : учеб. пособ. / Ю. Воронова. – Новосибирск : Новосибирский государственный университет, 2007. – 264 с.
11. Демидов Б. Тайный фронт / Б. Демидов, А. Величко, И. Волощук // Національна безпека України. – 2005. – № 7–8. – С. 17–23.
12. Деревянко А. С. Технологии и средства консолидации информации / А. С. Деревянко, М. Н. Солощук. – Харьков : НТУ «ХПИ», 2008. – 432 с.
13. Доронін О. І. Бізнес-розвідка / О. І. Доронін. – М.: Ось-89, 2007. – 490 с.
14. Сгоров В. 3 історії розвитку промислового шпигунства / В. Сгоров // Дзеркало тижня. – 1994. – 31 грудня. – № 13. – С. 14.
15. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та комп'ютерних технологій / [Л. П. Скалозуб, В. І. Василичук, С. А. Лебідь та ін.] ; за ред. О. М. Джужі. – К. : ДДСБЕЗ, 2009. – С. 56–58.

16. Зуйков Г. Г. Поиск преступников по признакам способов совершения преступлений: учеб. пособ. / Г. Г. Зуйков. – М. : ВШ МВД СССР, 1970. – 191 с.
17. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контролрозвідка / О. Івченко. [Електронний ресурс]. – Режим доступу : <http://www.justinian.com.ua>.
18. Колесниченко А. Н. Криминалистическая характеристика преступлений : учеб. пособ. / А. Н. Колесниченко, В. Е. Коновалова. – Х. : Юрид. ин-т, 1985. – 92 с.
19. Коммерческий шпионаж: самые известные скандалы последних лет. [Електронний ресурс]. – Режим доступу : <http://www.rb.ru/inform/44717.html>.
20. Конкурентная разведка [Электронный ресурс] // Сайт Юшука Евгения Леонидовича. – Режим доступа : <http://ci-razvedka.ru/>.
21. Кримінальне право України: особлива частина : підруч. / [Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін.] ; за ред. В. В. Сташиса, В. Я. Тація. – [4-те вид., переробл. і допов.]. – Х. : Право, 2010. – С. 229.
22. Куглякова Т. Методы деловой разведки / Т. Куглякова // Услуги и цены. – 2004. – № 24. – С. 5–7.
23. Курман О. В. Типізація способів учинення злочинних посягань на відомості, що становлять комерційну або банківську таємницю / О. В. Курман // Теорія та практика судової експертизи і криміналістики. – 2010. – Вип. 10. – С. 62–68.
24. Макаров А. Изучение конкурентной среды: взгляд профессионала [Электронный ресурс] / А. Макаров. – Режим доступа: <<http://www.4p.ru/main/theory/3570>>.
25. Митрофанов А. А. Экономическая безопасность коммерческих предприятий и деловая разведка / А. А. Митрофанов. [Электронный ресурс]. – Режим доступа : <http://www.bre.ru/security/22843.html>.
26. Настільна книга слідчого : наук.-практ. вид. для слідчих і дізнавачів / [М. І. Панов, В. Ю. Шепітько, В. О. Коновалова та ін.]. – [2-ге вид., перероб. і допов.]. – К. : Ін Юре, 2007. – С. 179.
27. Пилипенко А. А. Організація обліково-аналітичного забезпечення стратегічного розвитку підприємства : наукове видання / А. А. Пилипенко. – Харків : Вид. ХНЕУ, 2007. – 276 с.
28. Прескотт Дж. Е. Конкурентная разведка. Уроки из окопов / Дж. Е. Прескотт, С.Х. Миллер. – М.: Альпина Паблишер, 2003 – 336 с.
29. Про банки і банківську діяльність : Закон України від 7 грудня 2000 р. № 2121-III // Відом. Верхов. Ради України. – 2001. – № 5–6. – Ст. 30.
30. Про інформацію : Закон України від 2 жовтня 1992 // Відомості ВРУ, 1992. – № 48.
31. Розвідувальний цикл обробки інформації [Електронний ресурс] // Competitor Analysis – A Brief Guide The Basic Principles of Competitive Intelligence. – Режим доступу : http://www.scip.org/Library/intell_cycle.pdf.

32. Розслідування злочинів у сфері господарської діяльності: окремі криміналістичні методики: монографія / [В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.] ; за ред. В. Ю. Шепітька. – Х. : Право, 2006. – С. 11–19.
33. Сайт профессионалов конкурентной разведки [Электронный ресурс]. – Режим доступа: <http://www.scip.org>.
34. Создание системы конкурентной разведки компании. Ч. 2 [Электронный ресурс]. – Публикация от 18-09-2008. – Режим доступа: <http://daily.sec.ru>.
35. Техническая разведка в бизнесе: понимание технологии угроз и возможностей [Электронный ресурс] // Європейське об'єднання професіоналів конкурентної розвідки. – Режим доступу : <http://www.marketing-intelligence.co.uk/competitor-analysis.htm>.
36. Титов В. В. Конкурентная разведка в современных условиях [Электронный ресурс] / В. В. Титов. – Режим доступа : <http://www.bre.ru>.
37. Ткачук Т. Визначення оптимальної моделі конкурентної розвідки у контексті забезпечення інформаційної безпеки підприємства / Т. Ткачук // Інформаційна безпека людини, суспільства, держави. 2012. – № 2 (9). – С. 88–98.
38. Философия корпоративной разведки // PR в России (Москва). – 2003. – 29 авг. – № 8. – С. 23–24. [Электронный ресурс]. – Режим доступа: <<http://it2b.ru/it2b2.view3.page88.html>>.
39. Хант Ч. Разведка на службе вашего предприятия: информация – основа успеха / Ч. Хант, В. Заргарьян. – К. : Укрзакордонвизасервис, 1992. – 159 с.
40. Ховис Д. Конкурентная разведка. Уроки из окопов / Д. Ховис. – Альпина Паблишер, 2003. – 532 с.
41. Шаваев А. Г. Галерея шпионажа / А. Г. Шаваев. – М.: Инфра-М, 2009. – 416 с.
42. Шепітько В. Ю. Криміналістика : курс лекцій / В. Ю. Шепітько. – Х. : Одиссей, 2003. – С. 249;
43. Юшук Е. Л. Конкурентная разведка: маркетинг рисков и возможностей / Е. Л. Юшук. – М.: Вершина, 2006. – 240 с.
44. Юшук Е. Л. Конкурентная разведка / Е. Л. Юшук. – М.: Вершина, 2006. – 237 с.
45. Herring J.P. A Process to Identify and Define Intelligence Needs / Jan P. Herring. [Электронный ресурс]. – Режим доступа : <http://www.ciphersys.com/>
46. Miller J. Millenium Intelligence; Understanding and Conducting Competative Intelligence in the Digital Age, Business Intelligence Braintrust, 2000. – 469 p.
47. Starting a CI Program. Houston: APQC [Electronic resource]. – Available from: <http://www.APQC.org>.

Розділ 5

ПРОТИДІЯ РЕЙДЕРСТВУ ЯК ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

5.1. Рейдерство: сутність та роль в ринковій економіці

Рейдерство як явище не є новим і невідомим, скоріше навпаки – воно в різноманітних проявах спостерігалось в різні часи і майже в усіх країнах з ринковою економікою. Водночас, незважаючи на суттєву загрозу, яку несе в собі рейдерство як суспільно-небезпечне явище, в сучасній юридичній та економічній науці практично відсутній усталений понятійний апарат з питання, що досліджується, тривають дискусії щодо визначення та змісту цього поняття. Для того, щоб зрозуміти й осмислити усю небезпеку, яку рейдерство представляє для розвитку корпоративного сектору економіки, необхідно дослідити саму сутність рейдерства, а почати необхідно з витоків – з того, що означає поняття «рейдерство».

Слово «рейдер» має англійське походження, адже у середині ХХ століття за часів військового протистояння Великобританії та Іспанії так називалося одне з англійських морських піратських суден, котре здійснювало напад лише на іспанські торгові судна. З того часу поняття «рейдер» увійшло в лексику військово-морської справи, воно означало проведення морських операцій під час військових дій спеціально підготовленими для знищення бойових і торгових суден ворога морськими суднами. Це поняття застосовувалося під час війни багатьма країнами світу [16].

Термін «рейдерство» походить від англійського слова «raid», яке тлумачиться у двох аспектах, а саме як іменник і дієслово. Як-

що його розглядати як іменник, то це означає «набіг», «раптовий напад», а як дієслово – «грабувати», «спустошувати», «робити спроби знищити курс акцій шляхом продажу великої кількості цінних паперів» [47]. Таким чином, беручи до уваги основні смислові ознаки цього слова, «рейдерство» означає вороже поглинання, перехват оперативного управління або власності підприємства за допомогою спеціально ініційованого бізнес-конфлікту.

У вільній електронній енциклопедії «Вікіпедія» [10] знаходимо таке визначення рейдерства: від англ. Raider «учасник нальоту», – силове недружнє поглинання підприємства проти волі його власника, який має переважне положення на даному підприємстві, та/або керівника. Процес, сумісний з рейдерством, називається «рейдерський захват».

Таке визначення дає лише загальне уявлення, хоча і з нього слідує, що рейдерство пов'язане із перерозподілом власності, яке відбувається всупереч волі однієї із сторін.

Здійснене дослідження наукових джерел дозволило виявити, що в економічній літературі присутні суттєво відмінні трактування рейдерства, що частково можна пояснити дією таких обставин: активне використання перекладних джерел; відсутність власних фундаментальних теоретико-практичних досліджень в цій сфері, суттєва відмінність в змісті процесів, які називаються рейдерством в країнах з розвинутою економікою та в Україні. За результатами проведеного узагальнення нами були виділені три ключові підходи, які найбільш широко подані в науковій літературі.

Перший із них представляє рейдерство максимально наближено до західної наукової думки, тобто як високоєфективний бізнес, який не містить загрози, а скоріше, навпаки, – сприяє регулюванню кількості учасників ринку. Так, Ю. Борисов доводить, що рейдерство – це складний, високоінтелектуальний та високодохідний бізнес [5].

О. Беліков дотримується думки, відповідно до якої під рейдерством слід розуміти загальну назву ланцюжка операцій, що за допомогою прогагин у законодавстві дозволяє отримати у володіння певний капітал [3].

Схоже визначення дає й інший російський науковець О. Полушкін, трактуючи його як інструмент захоплення, який включає

в себе комплекс юридичних, психологічних, економічних, військово-спортивних методик та технологій [42].

Точка зору наступного науковця – В. Горбова, у порівнянні із вище процитованими, містить менше позитивізму, адже автор схиляється до думки, що рейдерство – це поглинання, яке означає скуповування контрольного пакету акцій компанії без будь-якого узгодження з акціонерами та менеджментом компанії [13]. До другого, більш реалістичного підходу, доцільно віднести і міркування інших науковців. Так, на думку О. Киреева, рейдерство – це систематична проектна діяльність на ринку корпоративного контролю, що спрямована на несилowe правове та неправове отримання контролю над активами інших суб'єктів економічної діяльності із завданням їм економічних та інших видів збитків [27]. Близьким до цього визначення є міркування А. Єфіменко, який подає його як «вилучення майна на законних підставах, в основі виникнення яких лежать прогалини в законі або системні недоліки функціонування державних інститутів (судової та правоохоронної систем, системи реєстрації юридичних осіб тощо)» [17]. Тобто, можна стверджувати, що відповідно до другого підходу, рейдерство це законний та/або незаконний перехід прав власності на бізнес без згоди однієї зі сторін.

Третій підхід, на наш погляд, найбільшою мірою відповідає реальному стану справ в нашій країні. Зазначене чітко відображено в наступних трактуваннях. На думку З. Варналія та І. Мазур, під рейдерством слід розуміти недружнє, поза межами дії цивільного законодавства, спрямоване проти волі власника, захоплення чужого майна на користь іншої особи, встановлення над майном повного контролю нового власника в юридичному й фізичному розумінні з використанням корумпованості чиновників та (або) із застосуванням сили [6]. П. Берназ та О. Середа вважають, що під рейдерством слід розуміти комплекс дій (здебільшого незаконних), які здійснюються особами з метою заволодіння майном іншого суб'єкта (фізичної або юридичної особи) [2]. М. Іонцев відстоює позицію, що рейдерство – це встановлення над компанією або активом повного контролю як в юридичному, так і фізичному значенні всупереч волі менеджменту та/або власника цієї компанії або активу [23]. Н. Касьяненко подає досліджувану категорію як процес недружнього поглинання організації будь-якої форми власності

за допомогою спеціально ініційованої корпоративної суперечки з використанням адміністративних та корупційних ресурсів, технологій та викрадання акцій й різноманітних шахрайських схем, а також трактуванням на свою користь неоднозначних положень нормативних та законодавчих актів [25]. В. Петренко під рейдерством розуміє захоплення чужої власності чи прав через реалізацію деяких спірних судових рішень із застосуванням дій органів виконавчої служби, міліції та силових структур. Його мета – перерозподіл чужої нерухомості, а тому воно приносить значні прибутки загарбникам [40].

Отримані результати знаходять підтвердження і в напрацюваннях експертів Центру дослідження корпоративних цінностей, терміном «рейдерство» позначають доволі широкий спектр дій: від звичайного законного недружнього поглинання об'єктів власності до відверто «бандитського» захоплення підприємства. Експерти Центру вважають, що визначити поняття «рейдерство» в Україні можна виключно на основі побічних ознак та за аналогією з тим, що називають «рейдерством» за кордоном. Так у корпоративному праві США та Західної Європи існує велика кількість різновидів рейдерства («рейд на світанку», «рейд преміальний», дружні поглинання (friendly take-over) та недружні (ворожі) поглинання (hostile take-over), американська та британська моделі, «біле», «сіре» та «чорне» рейдерство) і саме тому досі не існує єдиного, стовідсотково правильного і точного значення даного терміна.

Охоплюючи різні сфери суспільного життя рейдерство набрало системного характеру, з огляду на що визначити його сутність непросто. На Заході поняття рейдерство визначають як «вороже поглинання» – hostile takeover. Hostie takeover – the situation, in which one company tries to acquire another company without the approval of the target corporation's Board of Directors or owners of the business [62]. В перекладі це означає: ситуація, в якій одна компанія хоче заволодіти іншою компанією без згоди керівництва та власників компанії.

Слово «рейдер» (у своєму класичному визначенні), вживаючи заходи з придбання чужої компанії, не порушує закон, а лише діє всупереч волі її керівництва та контролюючих акціонерів, що дозволяє розглядати навіть випадки ворожого (недружнього) поглинання підприємств, як об'єктивні процеси, що сприяють динамі-

ці економічного зростання та розбудові потужної конкурентоспроможної економіки [21].

Рейдерство в сучасному розумінні, тобто знищення компанії і перерозподіл її власності та корпоративних прав, з'явилося у США в 60–70-х роках ХХ століття. Найпершим рейдером, за оцінками спеціалістів, став Джон Рокфеллер, засновник Standard Oil, який різними способами скуповував акції своїх конкурентів для зміцнення і процвітання власного бізнесу ще наприкінці ХІХ століття.

У багатьох країнах з розвинутою ринковою економікою ефективне корпоративне управління тісно пов'язане з такими явищами як злиття та поглинання. Саме вони досить часто стають ефективними інструментами в системі перерозподілу власності, адже передбачають в собі реструктуризацію підприємства з подальшим його оздоровленням та покращенням діяльності, часто зі зміною власника. Злиття як форма трансформації здійснюється шляхом об'єднання підприємства-боржника з іншими фінансово стійкими підприємствами. Внаслідок такого об'єднання підприємство-боржник втрачає власний самостійний юридичний статус. На відміну від злиття, поглинання проводиться у вигляді значних капіталовкладень одного суб'єкта господарювання в інший. Підприємство, яке поглинається, перестає бути самостійним, хоча як юридична особа може зберігатися у вигляді дочірнього підприємства.

Серед економістів, юристів, політиків є такі, що вважають недружні поглинання природнім процесом, який несе в собі позитивні моменти, наприклад, загальне оздоровлення економіки, адже захоплюються, зазвичай, ті підприємства, в яких існують значні недоліки управління. Якщо керівництву не вдається вчасно ліквідувати свої помилки, підприємство переходить до іншого, більш ефективного власника, що сприяє розвитку виробництва, а отже економіки загалом. Та, на жаль, практика показує, що процвітання підприємства після захоплення є швидше винятком.

Головною метою рейдера є отримання прибутку, але добивається він цього не виробництвом певного виду продукції, а перепродажем підприємства, над яким він отримав контроль шляхом «недружного поглинання», оскільки це набагато дешевше, ніж шукати з власником підприємства компроміс, і набагато простіше, ніж переконувати бізнесмена продати власну прибуткову справу [46].

Ще кілька років тому рейдерство активно процвітало в Російській Федерації, вкрай негативно впливаючи на всі параметри розвитку російської економіки. Та сьогодні, завдяки чітко визначеному чинному законодавству, рівень рейдерства в державі істотно скорочено. Між іншим, саме у зв'язку з цим дуже багато структур, які спеціалізуються на рейдерстві, «перепрофілювались» звідти в Україну. За оцінками експертів, до 50 відсотків рейдерського ринку країни вже захоплено російськими рейдерами.

Необхідно чітко зрозуміти, що західні рейдери виглядають зовсім безневинно, порівняно з їх російськими й українськими «колегами», адже з вітчизняних і російських ЗМІ, які повідомляють про факти рейдерства, ми дізнаємося не стільки про купівлю акцій, скільки про захоплення територій і офісів підприємств збройними загонами [12]. У зв'язку з чим на пострадянському просторі під рейдерством часто розуміють незаконне поглинання (захоплення) одного суб'єкта господарювання (підприємства) або його власності іншим, із застосуванням корупції і насильства [15].

Як підсумок можна стверджувати, що поняття «рейдерство», за змістом та впливом на корпоративний сектор економіки, є суттєво відмінним в умовах різного рівня розвитку ринкової економіки. Зважаючи на те, що рейдерство в умовах національної економіки має у більшості негативний характер, загрожуючи існуванню певного суб'єкта підприємницької діяльності, доцільним є розгляд світового досвіду протидії цьому явищу та розроблення власних методичних засад в рамках удосконалення системи управління економічною безпекою на мікрорівні.

5.2. Світовий досвід протидії рейдерству

Рейдерство як високоприбутковий бізнес є поширеним явищем у всьому світі, присутнє як в межах окремих національних економік, так і на міжнародному рівні. Сьогодні можна говорити про загальноприйняті методи і про те, що в різних країнах світу рейдерські атаки мають свої особливості розв'язання та ведення, існують різноманітні форми та стадії проведення рейдерських акцій, різні способи захоплення підприємств. І, як наслідок, у кожній

країні світу механізм протидії рейдерству має свої особливі ознаки, постійно розробляються та реалізуються різноманітні заходи щодо ефективного захисту від рейдерства та його подолання.

На нашу думку, вивчення світового досвіду протидії рейдерству уможливить розроблення нових та удосконалення існуючих методичних засад управління системою економічної безпеки вітчизняних підприємств. Багатою досвідом протидії рейдерству можна вважати таку країну як Сполучені Штати Америки (США), пік зростання кількості рейдерських атак в якій припадає на 80–90-ті роки ХХ ст. [61]. Для прикладу, протягом 1995-2000 років у США відбулося рейдерське захоплення 26 тис. компаній на суму близько 26 трлн дол., а вже у 2006 р. компанії США повідомили про 37594 угод на суму 3,8 трлн дол. [49]. Поруч із значною кількістю рейдерських атак, потрібно взяти до уваги, що ворожі поглинання ніколи не становили більше 20% від загальної кількості угод на американському ринку корпоративного контролю. Важливою відмінністю рейдерства в цій країні є те, що у 80-х роках з'явилися компанії для яких ворожі поглинання стали основним напрямком діяльності. Зазначені компанії шляхом скуповування акцій неефективних компаній та розпродажу їх по невеликих частинах суттєво змінили структуру власності американської економіки, що сприяло виділенню недружніх поглинань (рейдерські акції) в особливий вид високодохідної діяльності на ринку американського корпоративного контролю [65].

Слід зазначити, що протягом останніх років поглинання підприємств в США, на відміну від України, де рейдерські захоплення мають кримінальний характер, є відносно рідкісним явищем та здійснюється переважно в інтересах стратегічного розвитку бізнесу та за згодою обох сторін. На нашу думку, це зумовлено зростанням доступності інформації про ринок капіталу, змінами в антимонопольному та податковому законодавстві, відпрацьованій юридичній практиці вирішення корпоративних конфліктів. Підґрунтям висловленої тези є те, що основним нормативно-правовим актом, який регулює ринок корпоративного контролю в США, у тому числі регламентує порядок діяльності щодо поглинання підприємств, є Закон Вільямса, відповідно до якого, претенденти на участь у бізнесі компанії мають повідомляти про свої наміри Комісію з цінних паперів США, після чого повинні обов'язково дотримуватися вста-

новлених термінів, протягом яких претендентам забороняється здійснювати будь-які дії, спрямовані на участь у бізнесі конкретної ком-панії [49].

На підставі вивчення діяльності американських компаній варто зробити висновок, що найбільш ефективними засобами недопущення здійснення ворожих поглинань в США є вчасна зміна президента та голови ради директорів та внесення змін до статутів підприємств під час активізації діяльності «чорних» рейдерів на ринку корпоративного контролю.

Протягом майже 40 років у США було вироблено та впроваджено дієвий механізм протидії рейдерству як явищу, розроблено державну політику, що сприяє реформуванню рейдерства у необхідну для національної економіки форму активності та сформовано основи для інноваційного розвитку економіки країни. Саме цим можна пояснити, що на американському ринку корпоративного контролю дружні поглинання підприємств сприяють підвищенню ефективності та конкурентоспроможності підприємств, а ворожі поглинання (рейдерські акції) здійснюються нечасто.

Досліджуючи досвід протидії рейдерству у Великобританії, перш за все потрібно відзначити, що в цій країні превалюють дружні поглинання підприємств, а недружні – засуджуються представниками бізнесу та суспільством. Зазначене зумовлено тим, що для Західної Європи (у тому числі і для Великобританії) до будь-якого підприємства ставляться не тільки як до виключної власності акціонерів, а як до окремого соціального інституту, відповідальність за належне функціонування якого покладено на працівників підприємства, контрагентів, органи державної влади та суспільство в цілому. Іншими важливими відмінностями є те, що вибір об'єкта рейдерських атак не залежить від фінансового стану компанії та рівня ефективності управління нею, а також те, що для економіки цієї країни нехарактерна участь у ворожих поглинаннях спеціалізованих компаній, що займаються перерозподілом активів усупереч інтересам і правам інших суб'єктів економіки [28].

Для Німеччини, як і для США, кількість поглинань у другій половині минулого століття має чітку тенденцію до зростання. Так, у 1970-ті роки протягом одного року здійснено близько 370 поглинань, у 1980-ті роки їх кількість зросла до 830, а з 1990 по 1998 роки становила вже 1650 [28]. Водночас у структурі поглинань як і

у Великобританії основна частка припадає на дружні форми, а конфлікти, у тому числі ті, що виникли внаслідок спроб недружніх поглинань, надзвичайно рідкісні [63]. Низький рівень конфліктності на ринку корпоративного контролю цієї країни зумовлений високою концентрацією власності, незначною кількістю акцій у вільному обігу, наявністю ефективних механізмів захисту від недружніх поглинань.

Для корпоративного ринку Японії уже протягом досить тривалого часу характерним є принцип виключної добровільності об'єднань або поглинань підприємств, оскільки для недружніх (ворожих) поглинань існують жорсткі інституціональні та соціальні бар'єри [49]. Сутність інституційних бар'єрів полягає в тому, що менеджмент компанії залучає постійних акціонерів, яким належить близько 60–80% акцій підприємства. Саме наявність у руках постійних акціонерів значної частини акцій не допускає навіть виникнення загрози ворожого поглинання компанії шляхом скуповування акцій.

Джерелом виникнення соціальних бар'єрів для ворожих поглинань підприємств виступають культурні традиції японського бізнесу, які розглядають підприємство як спільноту працівників, які довічно працюють у компанії. Отже, працівники компанії самі зацікавлені у безперервному функціонуванні свого підприємства та докладають значних зусиль щодо усунення загроз захоплення компанії іншим власником.

Незважаючи на наявність дієвих інституціональних та соціальних бар'єрів для ворожих поглинань підприємств, у Японії протягом останніх двох десятиріч років також зростає кількість незаконних захоплень підприємств. Так, зокрема, щорічне зливання та поглинання (у тому числі й вороже) підприємств в Японії зросло з 500 у 1990-х роках до 2211 за підсумками 2004 р., що було зумовлено великою фінансовою кризою 1990 р., коли питома вага акціонерів, орієнтованих на довгострокові фінансові вливання, скоротилася удвічі і становила 25%, а ступінь участі іноземних власників зріс до 20%. Отже, саме зміни у складі акціонерів та структурі власності підвищили питому вагу акцій, які знаходяться у вільному обігу, що значно активізувало власників та сприяло зростанню кількості недружніх поглинань (рейдерських акцій) [64].

Для ринку корпоративного контролю Китаю характерним є високий ступінь участі держави в процесах управління компаніями. Так, у період з 1993 по 2000 роки варто зробити висновок, що у той час державні службовці та представники власників підприємств, підконтрольних державі, входили до складу більшості рад директорів китайських корпорацій; майже 50% членів рад директорів були делеговані власниками, підконтрольними державі, інші 30% членів ради директорів були безпосередньо пов'язані з різними рівнями урядових відомств [28].

Водночас, незважаючи на значний вплив органів державної влади на ринок корпоративного контролю та відсутність вагомого впливу з боку інституціональних інвесторів, у Китаї все ж таки спостерігається збільшення кількості ворожих поглинань. Особливістю рейдерства в Китаї є те, що учасниками корпоративних конфліктів дедалі частіше стають транснаціональні корпорації.

За результатами аналізу особливостей здійснення ворожих поглинань у країнах з розвинутою економікою варто зробити окремі узагальнення:

- національні корпоративні ринки розвиваються не за єдиним сценарієм, що обумовлюється низкою економічних, політичних, соціальних, культурних особливостей розвитку кожної держави;

- в кожній країні світу сторони конфлікту (рейдерської атаки) діють за власним сценарієм, а варіанти їх поведінки під час здійснення рейдерської атаки суттєво відрізняються один від одного;

- в окремих країнах різке збільшення кількості рейдерських захоплень зафіксовано в різні проміжки часу. Так, наприклад, у США активізація діяльності спеціалізованих фірм, спрямована на незаконні поглинання, припадає на 1970-ті роки; у Японії, внаслідок фінансової кризи та через протистояння західного і традиційно японського стилів корпоративного управління, багатопрофільні компанії спрямовують свою діяльність на здійснення рейдерських акцій в 1990-ті роки; у Німеччині, через об'єднання Східної та Західної Німеччини, банки (у менш виразній формі) стали тими економічними агентами, що взяли на себе функцію перерозподілу прав в економіці у 1990-ті роки;

– у формуванні загальних підходів до принципів захисту від рейдерства активну участь беруть не тільки урядові інститути, а й недержавні організації і групи. Якщо зусилля державних органів спрямовані насамперед на удосконалювання корпоративного законодавства з метою закріплення обов'язковості визначених стандартів забезпечення дотримання конкуренції, розкриття інформації про компанію, захисту прав акціонерів та забезпечення рівного ставлення до них, то діяльність ділових кіл та інших недержавних структур і груп зорієнтована на формування правил і процедур корпоративного управління, які були б добровільно прийняті бізнес-товариством, відповідали міжнародновизнаним принципам і разом з тим враховували національні особливості. Результатом такої роботи стала поява в різних розвинених країнах так званих Кодексів корпоративного управління – зводів добровільно прийнятих стандартів і внутрішніх норм, що встановлюють і регулюють порядок корпоративних відносин [29]. Правовий статус Кодексів корпоративного управління в різних країнах неоднаковий. В одних країнах він є частиною обов'язкових умов, яких компанії мають дотримуватися, щоб їх цінні папери оберталися на біржі, в інших – Кодекс є документом, що має рекомендаційний характер і не пов'язаний з будь-якими обов'язковими вимогами [19];

– в розвинених країнах для захисту підприємств від ворожих поглинань, активно застосовується корпоративне законодавство країни. Наприклад, у США деякі важливі методи захисту компаній винесені на рівень державного корпоративного законодавства. Таким чином, вони автоматично стають застосовними до всіх господарських товариств (хоча можуть бути зафіксовані і в статутах окремих підприємств). У більшості європейських країн були прийняті спеціальні закони, які регулюють процеси злиття і поглинань, також у цих країнах ворожі поглинання були засуджені бізнес-товариством. В Італії, наприклад, встановлено кримінальну відповідальність за злочини проти корпоративних відносин. Чинним законодавством Великобританії передбачено, що Комісія з питань добросовісної конкуренції в підприємницькій діяльності зобов'язана відстежувати інформацію про плановане злиття і поглинання. Проте, на практиці більшість компаній вважають за краще добровільно інформувати цю організацію про майбутнє злиття чи поглинання. Схвалення операції захищає компанії від можливого

застосування до них санкцій Комісії з питань конкуренції. А регулювання самих процесів злиттів і поглинань здійснюється за допомогою Кодексу злиттів і поглинань, який має рекомендаційний характер [60]. У корпоративному законодавстві Німеччини чітко визначені механізми ворожого поглинання, вимоги та обмеження, пов'язані з цим процесом. У 1995 р. у Німеччині було розроблено добровільний Кодекс про ворожі поглинання, у якому зазначалось, що перш ніж компанія-агресор зробить пропозицію про скупку акцій, вона повинна завчасно попередити про свої наміри компанію-мету, Німецьку біржу і Комісію з поглинань. При цьому пропозиція про скупку акцій публікується в газеті федерального масштабу. Акціонери компанії повинні мати не менш ніж 28 днів для прийняття рішення про продаж своїх акцій за справедливою ціною. У 1998 р. Німецька біржа визначила дотримання Кодексу як обов'язкову умову для включення компаній до основних німецьких фондових індексів [60];

– ефективними державними засобами запобігання рейдерству провідних країн світу є запровадження регулювання облікової системи ринку корпоративних цінних паперів, а документарна форма існування цінних паперів поступово замінюється бездокументною (електронною), що зумовлено здатністю бездокументної форми прискорювати, спрощувати та здешевлювати розрахунки і рух цінних паперів від одного власника до іншого, а також збільшувати захист прав власника від можливих махінацій з його цінними паперами [56]. Встановлення чітких і прозорих умов для здійснення бездокументного обігу цінних паперів у депозитарній системі унеможливає існування «подвійних реєстрів», оскільки єдиний центральний депозитарій є суб'єктом, що веде і контролює реєстр власників іменних цінних паперів товариства. При цьому велика увага приділяється механізмам захисту від розкриття й розголошення інформації із системи депозитарного обліку емісійних цінних паперів і запровадженню обов'язкового використання електронного документообігу й електронного цифрового підпису;

– головною передумовою існування ефективного ринку контролю в розвинутих країнах є розвинутий фондовий ринок та велика кількість корпорацій з розпорошеним серед багатьох учасників акціонерним капіталом;

– кошти для фінансування великих операцій з недружнього поглинання залучаються на відкритому фінансовому ринку, зокрема через пайові фонди, які спеціалізуються на скуповуванні акцій і подальшій реструктуризації підприємств, що неефективно працюють.

Необхідно звернути увагу, що у розвинутих країнах протидії рейдерству на державному рівні приділяється неабияка увага. Так, під час розроблення нормативно-правових актів, спрямованих на протидію та боротьбу з рейдерством, у США, країнах Західної Європи та Азії особлива увага приділяється тим наслідкам в економіці, до яких призводить рейдерство. Сформована система перетворила суто негативне явище, яким є рейдерство, на частково або і майже позитивне. Рейдери сприяють економічному розвитку: вони усувають від керування бізнесом неефективний менеджмент, запобігають зловживанням з боку великих акціонерів, реструктурують підприємства, які неефективно працюють. Причому власники атакованої компанії зрештою навіть виграють від вдалої «рейдерської» операції, оскільки вартість їх акцій (разом з вартістю акцій, придбаних рейдером) підвищується. Власне, інститут «рейдерства» став одним із найважливіших інструментів захисту інтересів міноритарних акціонерів. Рейдери об'єднують голоси, розпошені між сотнями і тисячами міноритаріїв, і змушують топ-менеджмент і власників великих пакетів акцій зважати на їхні вимоги. Дружні поглинання в країнах з розвинутою ринковою економікою відрізняються від ворожих лише згодою або незгодою менеджменту компанії-мети на поглинання, а отже, всі законодавчі й внутрішньокорпоративні прийоми захисту від рейдерства спрямовані на обмеження можливості неузгодженої скупки акцій на відкритому ринку.

На нашу думку, потрібно чітко підкреслити, що у практиці країн з розвинутою ринковою економікою рейдер діє в рамках чинного корпоративного законодавства і використовує ринкові механізми захоплення.

Наприклад, кошти для фінансування великих операцій з недружнього поглинання можуть залучатися на відкритому фінансовому ринку, зокрема через пайові фонди, які спеціалізуються на скуповуванні акцій і подальшій реструктуризації підприємств, які неефективно працюють [37].

Досвід провідних країн світу засвідчує, що процеси злиттів і поглинань (у тому числі ворожих) відіграють суттєву роль у розвитку як кожного окремого підприємства, так і всього корпоративного сектору країни. У країнах із сталими ринковими відносинами ці процеси набули цивілізованих форм завдяки розвиненому корпоративному законодавству, формуванню і підтриманню корпоративної культури. Більшість питань щодо злиттів і поглинань підприємств внесені до чинного національного корпоративного законодавства таких країн, розроблені Кодекси корпоративного управління, Кодекси про злиття і поглинання, при цьому випадки рейдерства як ворожого поглинання, що здійснюється поза нормами корпоративного законодавства, засуджується бізнес-товариством.

Проведене теоретичне дослідження та зроблені узагальнення з однієї сторони доводять цінність накопиченого досвіду протидії рейдерству, яке в розвинутих країнах використовуються як стимул для більш ефективного ведення бізнесу. Інша сторона полягає в тому, що поточна суть явища рейдерства в Україні та в США, Великобританії чи в інших країнах, розглянутих вище, є суттєво відмінною і застосовувати їх не лише не можна, але і недоцільно, щоб не спровокувати подальших ускладнень. На нашу думку, накопичений досвід потрібно вивчати та брати до уваги, але обов'язково шукати власне вирішення проблеми. В цьому контексті показовою є ситуація, яка склалася у сусідній з нашою країною РФ.

Перш за все зазначимо, протягом тривалого проміжку часу Російська Федерація та Україна були у складі Радянського Союзу, з розпадом якого в обох країнах одночасно почав активно формуватися особливий вид діяльності, що базувався на веденні жорсткої конкурентної боротьби (частіше за все із застосуванням неправових форм та силових методів боротьби) за активи підприємств усіх форм власності – рейдерство.

В Російській Федерації ринок корпоративного контролю почав активно формуватися на початку 1990-х років, і протягом наступних 20 років його розвиток характеризувався високою динамічністю та суперечливістю. Слід зазначити, що цивілізованому розвитку цього ринку заважали корупція, недосконалість законодавства, політична нестабільність, наявність масштабного тіньового сектора економіки, відсутність поваги до вимог законо-

давства у бізнес-середовищі, ігнорування судової та правоохоронної систем більшістю суб'єктів економічної діяльності.

Нормативно-правова база, що поступово формувалася в той період часу, не лише не запобігала, а й навіть стимулювала появу нових форм перерозподілу власності, до яких належить і рейдерство. Так, зокрема, Федеральний закон «Про акціонерні товариства» на законодавчому рівні забезпечував широкі можливості для корпоративного шантажу і, як наслідок, здійснення незаконних захоплень підприємств [27]. Наступним нормативно-правовим актом, положення якого сприяли виникненню рейдерства, є Федеральний закон «Про неспроможність (банкрутство)». Саме з його прийняттям пов'язана інтенсифікація перерозподілу власності (силові методи та неправові форми боротьби за активи підприємств усіх форм власності) протягом 1998–2000 років, зокрема шляхом уведення процедури спостереження за підприємством-боржником та отримання контролю за ним шляхом призначення зовнішнього управляючого [27].

Характерною ознакою рейдерства в Росії у 1990-ті роки є урегулювання спорів у бізнес-середовищі із залученням силових підприємців (бандитів). Слід підкреслити, що окремі ознаки силового підприємництва наявні не лише в боротьбі за малий бізнес, а й у великих конфліктах регіонального та федерального значення.

Зважаючи на вищевикладене, варто зробити висновок, що для бізнес-середовища в Росії у 1990-ті роки була широко поширена практика досягнення власних інтересів із застосуванням різноманітних форм та засобів, не враховуючи прав та інтересів інших суб'єктів підприємницької діяльності, а активними учасниками корпоративних конфліктів були як російські компанії, так і закордонні транснаціональні корпорації.

Починаючи з 2000-х років на російському ринку корпоративного контролю виникає нове явище: формуються стійкі формальні та неформальні угруповання, що здійснюють систематичну діяльність зі встановлення контролю над активами інших суб'єктів економіки шляхом завдання їм економічних та репутаційних збитків.

Високий рівень доходності та відсутність ефективних механізмів протидії таким рейдерським акціям сприяли тому, що протягом 2–3 років на ринок корпоративного контролю в Росії вийшли

десятки формальних та неформальних угруповань, для яких захоплення чужого бізнесу стало основним видом діяльності [27].

При цьому слід підкреслити, що спрямованість діяльності зазначених угруповань не залежала від галузевої приналежності підприємства, його розмірів, фінансово-економічного стану, ступеня взаємодії з іншими суб'єктами.

Розмах рейдерства зріс на початку XXI століття і домінує серед поглинань: в 2002 році в Російській Федерації відбулося 1870 поглинань, з них три чверті (76%) недружніх. З 2004 по 2007 рік сума недружніх угод зросла більш ніж в чотири рази [25]. Тільки за 2008 рік МВС зареєструвало понад 3000 звернень про рейдерські захоплення [1].

Внаслідок того, що ця проблема стала явною загрозою перш за все для національної безпеки, в Російській Федерації було зроблено ряд важливих кроків до її розв'язання, зокрема шляхом удосконалення законодавчої бази, активізації роботи Генпрокуратури, Розрахункової палати, створення координаційних центрів і міжвідомчих координаційних комітетів економічної безпеки на рівні федеральних округів.

Безперечно, що цей досвід, який за базовими умовами є максимально наближеним до українських реалій можна та потрібно використовувати.

Стосовно доцільності використання досвіду США, країн Західної Європи та Азії щодо протидії рейдерству, то необхідно звернути увагу на те, що існують істотні міждержавні відмінності, через які використання досвіду зазначених країн для вирішення проблем українського ринку корпоративного контролю стає практично неможливим.

Отже, спроби впровадження в Україні механізмів протидії рейдерству, які були ефективними в інших країнах, не будуть успішними.

Водночас, зважаючи на те, що рейдерство в Україні постійно трансформується, державна політика щодо протидії рейдерству має сприяти реформуванню рейдерства в необхідну національній економіці форму активності та сформувати основи для інноваційного розвитку економіки.

5.3. Практика рейдерства в Україні

та засади захисту вітчизняних підприємств

В країнах із сталими ринковими відносинами практика рейдерства набула цивілізованих форм, зокрема завдяки розвитку системи обліку корпоративних цінних паперів та корпоративного законодавства. Оскільки в Україні фактично відсутнє корпоративне законодавство, яке б регулювало поглинання акціонерних товариств (придбання значного пакета акцій), то на практиці це призводить до застосування різноманітних напівлегальних, тіньових схем рейдерських захоплень. Окремо потрібно наголосити, що в розвинутих країнах рейдерство, яке здійснюється в рамках чинного законодавства, засуджується суспільством, а в нашій країні – отримує мовчазну згоду у владних кабінетах.

Рейдерство як явище стало реальною загрозою для економіки нашої країни, адже руйнується вітчизняний бізнес, банкрутують ефективні виробництва, знижується інвестиційна привабливість окремих галузей та країни в цілому, посилюється напруга в економічному просторі, а тиск рейдерів на бізнес щорічно віднімає в Україні до 1-2% економічного зростання. Більш того, об'єктом рейдерських атак стають як найліквідніші приватні підприємства, так і найменш захищені, але стратегічно важливі науково-дослідні інститути та наукомісткі підприємства, тобто фактично рейдерської атаки може зазнати будь-яке підприємства і це набуло масового характеру, а відтак рейдерство можна визнати явною загрозою не лише для економічної безпеки на мікрорівні, але і для національної безпеки в загальному.

Головні негативні наслідки рейдерства в Україні можна визначити такою сукупністю [60]:

- негативний вплив на підприємницький клімат;
- дестабілізація роботи вітчизняних підприємств;
- пограбування та розорення законного власника;
- зупинка технологічного процесу;
- створення шокової атмосфери на підприємстві;
- руйнація трудових колективів та соціальні конфлікти;
- втягування персоналу в конфлікт, що саме по собі провокує незаконні, нерідко насильницькі дії.
- формування несприятливого інвестиційного клімату та міжнародного іміджу країни в цілому тощо.

Злочинна і безкарна діяльність рейдерських угруповань, яка інколи отримує і мовчазну згоду у владних структурах, негативно впливає на соціальну атмосферу в суспільстві, породжуючи в громадян апатію до праці, сіє зневіру в можливості і бажання держави захистити їхні інтереси. Звідси логічним є висновок, що боротьба з такими протиправними захопленнями повинна вестися не тільки на рівні окремих підприємств, а й насамперед на державному рівні за умов наявності чіткої програми дій та застосування адекватних механізмів, адже для держави важливим завданням є не лише максимізація доходів бюджету, але і створення прийнятних умов для господарської діяльності платників податків та можливості реалізації потенціалу кожного громадянина.

Попри високий статус проблеми рейдерства, яка безпосередньо торкається інтересів держави та впливає на рівень національної безпеки, об'єктом нашого дослідження є все таки мікрорівень, а тому, на нашу думку, можна чітко стверджувати, що існування кримінальних, рейдерських, дискримінаційних дій щодо суб'єктів підприємницької діяльності є прямою (фізичною) загрозою для незалежного функціонування та відповідно економічної безпеки підприємництва.

Всупереч вище зазначеному, у вітчизняного підприємництва ще не сформувалося цілісне розуміння причин і джерел виникнення загроз недружнього поглинання і не розроблені та не використовуються заходи протидії йому, а відтак розробка підходів, форм і способів захисту суб'єктів господарювання від їх силових захватів є досить актуальною.

Зазначимо, що основними причинами вагомого впливу рейдерства на рівень економічної безпеки підприємств та складність здійснення ефективної протидії йому зумовлені дією таких чинників:

- недосконалість ринкових інструментів перерозподілу власності, які застосовують сьогодні в Україні;
- незаконна приватизація суб'єктів підприємницької діяльності;
- нечітка та непрозора система реєстрації прав власності, порушення різноманітними формальними та неформальними групами прав та інтересів інших суб'єктів економіки;
- відсутність повноцінного правового та прозорого ринку купівлі / продажу бізнесу. Великі вітчизняні підприємства, як пра-

вило, не створюються, а купуються внаслідок роздержавлення чи вторинного перерозподілу роздержавленої власності, часто пов'язаного з непрозорими неринковими діями зацікавлених сторін. Малий та середній бізнес із високим рівнем персоніфікації, суб'єктивними обмеженнями та обтяженнями (в т.ч. економічного або кримінального характеру), а також внаслідок відсутності офіційної, закріпленої у відповідних державних нормативно-правових актах системи щодо його придбання-продажу, фактично не має вторинного ринку його купівлі/продажу;

– відсутність або недостатня розробленість нормативно-правової бази, яка б регламентувати порядок діяльності на ринку корпоративного контролю [7]. Зазначимо, що на відміну від України, у більшості європейських країн уже давно прийняті спеціальні закони проти рейдерів. Щодо ситуації із вітчизняною законодавчою базою, то в Україні відповідних та вкрай необхідних нормативно-правових актів ще не існує, хоча це питання активно обговорюється на усіх владних рівнях і зокрема у Верховній Раді;

– висока корумпованість органів державної влади України, до повноважень яких входить вироблення дієвого механізму протидії порушенням встановленого порядку діяльності на ринку корпоративного контролю;

– відсутність профільних державних інституцій, які б ефективно захищали права власника на ринку корпоративного контролю;

– недосконалість судової влади (на нашу думку, саме судова влада має бути найважливішим інструментом захисту економіки від рейдерів);

– експансія з-за кордону спеціальних корпоративних технологій, які стимулюють бездіяльність української влади у сфері протидії рейдерству та боротьби із цим суспільно-негативним явищем;

– низький рівень правової культури населення та правовий нігілізм у суб'єктів економічної діяльності та у представників органів державної влади України.

Дія усіх перелічених чинників зумовила ситуацію, що протягом останніх років рейдерство в Україні перетворилося на справжню суспільну катастрофу, яка загрожує позитивному розвитку української економіки, спричиняє колапс правової систе-

ми, висвітлює сумнівні перспективи існування та розвитку в Україні приватного середнього і малого бізнесу. Так, за оцінками експертів інвестиційних компаній, щорічний обсяг сегмента поглинань і злиття становить в Україні понад 3 млрд дол. США, дві третини поглинань мають недружній характер рейдерських захоплень [6]. Зазначимо, що на даний момент в Україні діє щонайменше 40–50 спеціалізованих рейдерських груп, які складаються з досвідчених юристів та економістів, а кількість рейдерських захоплень сягає 3000 на рік. Завдяки високій ефективності організації цього злочинного бізнесу, результативність рейдерських атак сягає рівня 90%. Середньостатистична норма прибутку рейдера в Україні, за експертними оцінками, становить близько 1000%. Українське рейдерство має відчутну кримінальну складову: протиправні дії чиняться із залученням збройних формувань, а подекуди – навіть співробітників правоохоронної системи тощо. Відомо, що на сьогодні рейдерство в Україні набуло системного характеру, оскільки починаючи з 2005–2006 роках до схем протиправного привласнення підприємств почали широко залучатися державні та правоохоронні органи, суди, державна виконавча служба тощо.

Зважаючи на вище викладені аргументи, вважаємо, що виправданою є підвищена увага з боку науковців та посадових осіб відповідних органів державної влади України до вивчення такої нової форми порушень прав власності як рейдерство, розроблення ефективних механізмів захисту, що є можливим лише у випадку удосконалення системи економічної безпеки кожного суб'єкта підприємницької діяльності.

Розглянемо фактичний досвід реалізації рейдерства в Україні з метою розроблення методичних засад здійснення захисту. Так, рейдерство в Україні здійснюється такими суб'єктами:

- окремі особи, що використовують корумпованість певних структур влади й управління, що прагнуть заволодіти чужим житлом й іншою власністю;
- спеціальні фірми або групи людей, що об'єдналися з метою професійного зайняття рейдерством, у тому числі групи, що спеціалізуються на захопленні земель, квартир, підприємств, акцій тощо;
- галузеві холдинги, що прагнуть до усунення конкурентів у своїй сфері шляхом їхнього поглинання;

- великі холдинги й фінансово-промислові групи, що знаходяться, як правило, у великих містах, і володіють великими ресурсами й можливостями, скуповують землі, бізнес у різних галузях і все коштовне для збільшення своїх активів;

- несумлінні керівники, що мають доступ до особливо важливих для компанії документів, схем керування та активів;

- партнери по бізнесу або дрібні акціонери тощо.

Виходячи з визначення та поданої вище класифікації потенційно небезпечного для бізнесу суб'єкта, яким і є в Україні рейдер, можна виділити його ключові інтереси, які спонукають до злочинних дій:

- збільшення частки ринку;
- усунення конкурентів;
- встановлення контролю за продавцями або постачальниками;

- пограбування підприємства, що атакується;
- перепродаж активів або компанії в цілому за вищою ціною.

Якщо проаналізувати практику здійснюваних в Україні рейдерських захоплень, можна виділити такі основні ознаки і складові рейдерства (рис. 5.1):

- *це завжди недружне поглинання*, втрата контролю над підприємством або майном поза волею його власника;

- *раптовість здійснення рейдерських атак*. Підставою для «нападу» є зазвичай документи, про існування (створення, ухвалення) яких підприємство не має ніякої інформації. Усвідомлення того, що підприємство стало об'єктом рейдерської атаки у переважній більшості випадків приходить по факту пред'явлення незаконного рішення державним виконавцем або фізичного усунення менеджменту від управління підприємством.

- *неефективний менеджмент, який сприяє успішності реалізації рейдерських атак*. Часто раптовість і несподіваність рейдерських атак обумовлена неухважністю основних власників до процесів, що відбуваються на підприємстві, до стану активів, відсутність контролю над менеджментом, що вказує на незадовільний рівень організації та виконання безпосередніх функцій усіма підрозділами економічної безпеки;



Рис. 5.1. Відмінні характеристики рейдерства в Україні

- *протизаконність дій рейдерів.* Ця ознака характерна для більшості рейдерських атак, які здійснюються в Україні, але не завжди є притаманною рейдерству, тому що перехід контролю над підприємством поза волею власника, але з дотриманням чинного законодавства, також можливий. Це так зване «біле» рейдерство, при якому використовуються законні способи захоплення, такі як, наприклад, скуповування акцій (часток) міноритарних учасників, переобрання органів управління. Така практика є прийнятною в розвинених країнах, і не суперечить прийнятим в цивілізованому світі правилам гри у бізнесі. Отже, протизаконність дій рейдерів – це ознака, так званих, «сірого» і «чорного» рейдерства. У першому випадку рейдери формально дотримують закон, діючи на підставі відповідних рішень і визначень судів, актів органів влади, рішень загальних зборів, які, проте, приймаються без достатніх на те підстав. «Чорне» рейдерство, відповідно, передбачає досягнення поставлених цілей з використанням протиправних методів, включаючи підробку документів та підписів, погроз, насильства, фізичного захоплення підприємства;

- *використання судових рішень (у тому числі і третейських судів), які винесені без достатніх законних підстав.* Судовими рішеннями обґрунтовується практично все – заборона проведення

загальних зборів, недопущення конкретних учасників до участі в загальних зборах, зміна органів управління, накладення арешту на майно, підтвердження права власності на майно, акції, долі і т.д. На підставі рішень судів також здійснюються недружні поглинання через процедуру банкрутства і ліквідації підприємства. У випадку якщо дані рішення в майбутньому будуть скасовані, за час їх оскарження рейдери встигають зміцнити свої позиції іншими методами. Про істотну роль судів в рейдерських схемах свідчить і те, що за останній час запропоновано декілька законопроектів, направлених на створення умов для неможливості участі третейських судів в рейдерських схемах і встановлення кримінальної відповідальності суддів за ухвалення рішень, що виходять за межі їх компетенції.

- *підтримка з боку державних органів* (органи влади і управління, судові, податкові та правоохоронні органи тощо) *причому як підприємства-жертви, так і компанії-агресора*. Часто здійсненню рейдерської атаки передують численні перевірки контролюючих органів, які проводяться без достатніх підстав. Державні органи, що мають відповідні повноваження, використовуються рейдерами для отримання інформації про підприємство, а численні виснажливі перевірки дестабілізують його роботу;

- *застосування силових методів захоплення*. Поширеною практикою для рейдерських атак є фізичне захоплення підприємств. Не рідко таке захоплення відбувається під час примусового виконання державною виконавчою службою рішень судів, для чого притягуються правоохоронні органи, приватні охоронні фірми.

- *використання рейдерами порушень законодавства зі сторони підприємства-об'єкта атаки*. Будь-яке українське підприємство може стати жертвою недружнього поглинання через різні порушення, що виникли або при приватизації, або при здійсненні емісії акцій, або при проведенні зборів акціонерів тощо, і такі фактори завжди є зручною зачіпкою для потенційних загарбників.

Поруч із наявністю суттєво відмінних ознак, які притаманні для практики вітчизняного рейдерства, потрібно звернути увагу і на схожі риси, зокрема з американськими рейдерами. Спільним, що фактично об'єднує українських та американських «рейдерів» є орієнтація на швидкий перепродаж активів захопленої корпорації. Однак легальність набуття контролю над корпорацією американського «рейдера» дозволяють йому не поспішати із продажем

активів та отримати за них найвищу ціну. У випадку з американським рейдером можна бути впевненим, що активи будуть продані сторонній особі за найвищою можливою ціною і будуть вжити всі необхідні заходи щоб мінімізувати шкоду, що може бути завдана таким активам.

Тоді як «рейдерство» по-українськи здебільшого полягає у набутті сумнівними шляхами тимчасового права розпоряджатися активами та якнайскорішим продажем цих активів, пов'язаним із рейдером особам, із наступними перепродуваннями вилучених активів між пов'язаними особами, маючи на меті завадити (унеможливити) їх повернення законним власникам. Елемент протиправності, порушення закону чи принципів права є визначальним для розуміння природи українського «рейдерства».

Таким чином, підсумовуючи вищевикладене, можна визначити суть рейдерства в Україні як направлене проти волі власника протизаконне захоплення контролю над підприємством або його активами (коштами; технікою; продукцією підприємства; зайнятими підприємством територіями; будинками й спорудами; засобами виробництва; бізнесом у цілому тощо) з використанням рішень державних і судових органів і, як правило, із застосуванням сили.

Для визначення сукупності захисних заходів, на нашу точку зору, важливим є дослідження процесу планування та здійснення рейдерської атаки.

Підготовка та проведення рейдерських захоплень у більшості випадків проходить наступні етапи: розвідка бізнесу, оцінка здатності захисту підприємства та реакції на зміну власника, розробка схеми захоплення підприємства, організація захоплення, забезпечувальні заходи. На кожному з цих етапів об'єкт захоплення певним чином може протистояти [24].

Способів рейдерських захоплень у вітчизняній та зарубіжній практиці існує не так вже й багато. Вибір конкретної схеми захоплення залежить від характеристик об'єкта атаки:

- організаційно-правової форми підприємства;
- розмірів підприємства (мале, середнє, велике);
- рівня захисту основних ресурсів та можливості чинити активний опір;
- ступеня суспільної значимості підприємства.

За результатами проведення розвідки, відповідно до вище поданих чотирьох факторів будується тактика захоплення підприємства.

В Україні найчастіше використовуються такі схеми захоплення підприємства (рис. 5.2) [3; 33]:

- через акціонерний капітал;
- через кредиторську заборгованість підприємства;
- через органи правління;
- шляхом оскарження результатів приватизації в суді.

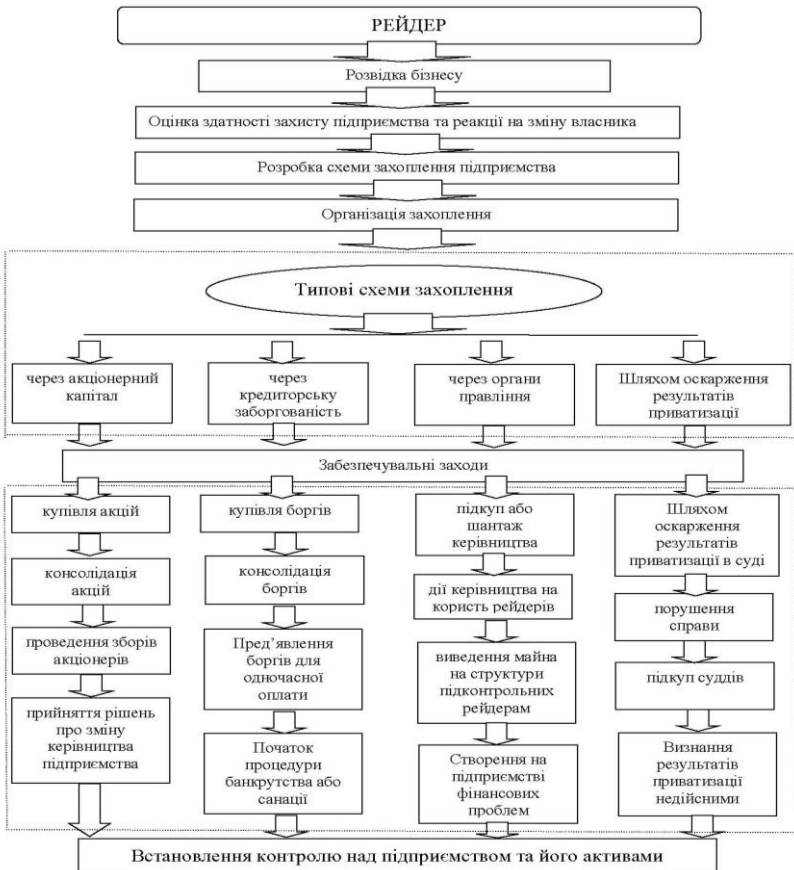


Рис. 5.2. Схема рейдерських захоплень підприємств

Захоплення через акціонерний капітал свідчить про те, що він сильно розпорошений або недостатньо контролюється. Початком атаки є скупка акцій. Як правило, рейдери планують скупити близько 10–15% акцій – ця кількість є достатньою, щоб ініціювати проведення зборів акціонерів з «потрібним» порядком денним, наприклад, зміною керівництва підприємства. Акціонерне товариство, власником якого є трудовий колектив, – найпривабливіший об'єкт для рейдера. Одержуючи невисокі зарплати, працівники без особливих коливань продають свої цінні папери тому, хто пропонує ціну в 5–10 разів більше номінальної вартості (однак все-рівно менше їхньої реальної вартості). Приклади застосування подібної тактики досить відомі: дії компанії «Сармат», яка в свій час скупила через ІК «Керамет-Інвест» 41,5% акцій київського пивзаводу «Оболонь»; а також атака компанії «Кліринговий будинок» на черкаський «Азот».

У другій половині 90-х найбільш популярним способом було відбирання власності через кредиторську заборгованість. Застосовується він і сьогодні. Прострочені борги підприємства скуповуються в дрібних кредиторів за низькими цінами, потім консолідуються й пред'являються до одночасної виплати. Нездатність підприємства розрахуватися за своїми обов'язками дає підстави для початку процедури банкрутства або санації з усіма наслідками, що випливають з цих процедур. Завод, що перебуває на санації, не підконтрольний ані його власнику, ані менеджменту. Головна діюча особа-керуючий санацією, якого, як правило, рейдери легко можуть зацікавити «співпрацею».

Однією зі слабких ланок підприємства, яким зацікавились рейдери, може бути наймане керівництво. Наділений значними повноваженнями директор може сприяти швидкому виведенню майна з підприємства на підконтрольні рейдеру структури. Таким чином, власник підприємства може залишитися з акціями, які нічого не варті. Менеджмент легко може спровокувати фінансові проблеми на заводі, наприклад, санкціонувавши покупку сировини за завищеними цінами або взявши кредит під нереальні відсотки. Переконати керівництво діяти на користь рейдера можна різними способами: від звичайного підкупу до підсаджування на «гачок» шляхом шантажу, кримінального переслідування та погроз. Атака через менеджмент дешевше всього обходиться на держпідприємствах, на яких відсутній ефективний контроль над оперативною діяльністю з боку власника.

Зміна влади в 2004 році в Україні, а відповідно – й наступний переділ власності – став поштовхом до дії для вітчизняних рейдерів. Та й чому б не скористатися законним способом, який був запропонований самим урядом – оспорування підсумків приватизації. Тоді Уряд готував до повторного продажу «Криворіжсталь», підсилювався тиск на інших власників великих та середніх підприємств, почастішали випадки недружніх захоплень і поглинань. Водночас, справжня рейдерська війна з усіма атрибутами, властивими недружнім захопленням і поглинанням, була розв'язана проти ФК «Динамо» (Київ). Значного розголошу набув і переділ власності та укрупнення підприємств на ринку фасованого соняшникового масла.

При наявності такого різноманіття схем рейдерських атак виникає необхідність розроблення адекватних захисних дій.

Відразу треба зауважити, що рецептів, які підходили б кожній компанії стосовно її стратегії й тактики протидії рейдерству, не існує, що, звичайно, кількість традиційних варіантів захисту обмежена, але якщо вміло застосовувати їх поєднання, то в тій або іншій ситуації можна одержувати такі неповторні комбінації, які зможуть гарантувати перемогу в корпоративній війні [52; 55]. Проте слід зважити на те, що не можна побудувати достатньо конструктивний план свого захисту, не беручи до уваги те, наскільки він здійснений. У випадку, якщо рейдерська атака на підприємство вже почалася, планувати та діяти доведеться одночасно, що вкрай складно – необхідно, щоб тактичні плани співвідносились з реальністю, до того ж, в арсеналі рейдерів достатньо інструментів для досягнення поставленої мети, які заради отримання надприбутків вони готові використати.

В цьому контексті доцільно згадати сформовані нами у попередньому розділі завдання конкурентної розвідки та контррозвідки в системі економічної безпеки. На нашу думку, роль конкурентної розвідки у вітчизняному бізнесі насамперед зводиться до вчасного запобігання рейдерській атаці. Якщо брати до уваги, що конкурентна розвідка та контррозвідка – це постійний процес збору, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії й надання вищому менеджменту компанії інформації, що дає змогу йому передбачати зміни в обстановці й приймати своєчасні оптимальні рішення щодо керування ризиками, впровадження змін у компанії й відповідних заходів, спрямованих на задоволення майбутніх запитів споживачів й підтримку

прибутковості, то, відповідно, важливу, а може, й критично необхідну інформацію, обов'язково буде здобуто службою конкурентної розвідки.

Спектр завдань конкурентної розвідки та контррозвідки для цілей захисту від рейдерських атак не обмежується захистом важливих об'єктів, ресурсів, комунікацій та конфіденційних даних, як часто вважають, він є на порядок ширшим:

- виявлення загроз політичного, фінансово-економічного, соціально-психологічного характеру у сфері інтересів підприємства;
- інформаційна оцінка партнерів, клієнтів, конкурентів, контрактів;
- проведення моніторингу партнера/конкурента як в Україні, так і в будь-якій країні світу;
- інформаційно-аналітична підтримка процесів підготовки, прийняття і супроводження рішень підприємства, систематизація результатів реалізації раніше прийнятих рішень;
- інформаційний контроль розвитку інфраструктури ринку, конкурентів, їх рекламних дій;
- інформаційний супровід власних активних дій на ринку (публікації, реклама, виставки, дезінформація тощо);
- забезпечення координації і взаємодії функціональних підрозділів організації на основі взаємного обміну інформацією про його оточення;
- створення системи технічного захисту конфіденційної інформації;
- інформаційно-аналітичне супроводження злиття чи поглинання;
- розробка правової бази захисту інформації з обмеженим доступом;
- кадровий консалтинг.

Практичним втіленням такої роботи є створення інформаційної бази даних.

Ефективний захист підприємства лежить винятково усередині самого підприємства. І цю небезпеку можна перебороти тільки побудувавши систему ефективних превентивних заходів захисту бізнесу комплексного характеру. У свою чергу, для успішної протидії рейдерам, треба розуміти основні принципи їх роботи, насамперед те, що: будь-який рейдер намагається отримати максимально можливий швидкий прибуток; рейдер використовує корумпованих

представників влади (правоохоронних та судових органів) для досягнення своїх цілей; у своїх діях рейдер розраховує на те, що підприємство-об'єкт атаки злякається та надасть перевагу укладенню невігідної угоди, а не боротьбі; рейдер використовує у своїй діяльності суперечності чинного законодавства.

При здійсненні захоплення витрати рейдерів, зазвичай, в 10–20 разів менше, ніж коштують активи підприємства-об'єкта атаки. Саме це дає суттєву вигоду та є економічною основою рейдерства.

Аналіз захоплень показує, що реальні результати захисту підприємства від рейдерської атаки можливі лише на перших етапах, на подальших етапах позитивний для підприємства результат можливий лише у 10–20%. Звідси зростає важливість ефективного здійснення превентивних заходів, в т.ч. за рахунок діяльності структурних підрозділів системи економічної безпеки підприємства.

До пріоритетних превентивних заходів з протидії незаконним захопленням підприємств можна віднести:

- історія створення підприємства повинна бути бездоганною, а його установчі документи повністю відповідати чинному законодавству України. За рішенням суду підприємство може бути ліквідоване тільки якщо при його створенні були допущені порушення, які не можна усунути. Тобто, навіть якщо нинішній власник підприємства не був його засновником, ніколи не пізно критично переглянути свої установчі документи і внести до них відповідні зміни;

- побудова чіткої схеми управління підприємством;
- регулярний моніторинг поточного стану документів;
- формування позитивного іміджу компанії;
- робота із ЗМІ;
- зміцнення зв'язків з місцевими органами реєстрації;
- чітка податкова і фінансова звітність;
- регулярне внесення змін у засновницькі документи акціонерного товариства;
- концентрація акціонерного капіталу або викуп частки в учасників, які не беруть участі в діяльності підприємства;
- контрольне скуповування акцій і додаткова емісія;
- забезпечення регулярної перевірки стану реєстраційних документів підприємства;
- здійснення постійного контролю за заборгованістю компанії;

- обтяження кредиторською заборгованістю підприємства. При цьому таке обтяження має здійснюватися не банком, а спорідненої структурою, з належним документарним оформленням;
- забезпечення ефективного контролю за отриманням вхідної кореспонденції за всіма адресами підприємства;
- роз'яснювальна робота з трудовим колективом, профспілками, пенсіонерами організації, що володіють акціями підприємства;
- постійний моніторинг змін у складі акціонерів;
- реструктуризація підрозділів зі зміною їх організаційно-правового статусу;
- визначення правового статусу власності, здійснення переоцінки майна. В умовах значного ризику буде корисною реструктуризація власності з використання дочірніх структур, створення штучної заборгованості підприємства і передача нерухомості та інших активів у позичку під кредитування;
- удосконалення роботи менеджменту та персоналу (недопущення конфліктних ситуацій, протиправного звільнення працівників тощо);
- підвищення культури суб'єктів господарювання (прозорі конкурентні відносини, підтримання ділової репутації тощо);
- використання в службі економічної безпеки способів і методів конкурентної розвідки;
- залучення громадськості й засобів масової інформації до боротьби з рейдерством.
- надійна і ефективна охорона активів (території, будівель, обладнання, транспорту тощо).
- використання можливостей системи страхування стосовно захисту прав власності, прийнявши загрозу рейдерства за потенційний підприємницький ризик – це буде правовою гарантією від загрози втрати прибутковості бізнесу (можливості втрати частини часток на підприємстві).
- ведення бізнесу на основі прозорості власності й адекватної капіталізації вартості активу підприємства – оскільки рейдери йдуть на захоплення тих організацій, які можна дешево купити, а потім дорого продати.
- вживання відповідних заходів із зниження прибутку від рейдерських захоплень (зараз в Україні за експертними оцінками вона нерідко перевищує 1000%, тому її зниження хоча б до

100% вже саме по собі здатне різко обмежити кількість незаконних захоплень).

- здійснення постійного внутрішнього аудиту фірми із залученням сторонніх юристів з метою ретельного дослідження документації підприємства за останні декілька років, визначення прогалин і помилок, що потребують усунення та розробки заходів із зміцнення безпеки підприємства.

- придбання (відчуження) активів підприємства слід здійснювати у суворій відповідності із законодавством. Всі розрахунки бажано проводити офіційно, із зазначенням у договорах їх реальних сум. У разі визнання відповідних договорів недійсними, підприємству, згідно закону, повинна буде бути повернута реальна вартість активів, що може бути економічно не вигідним для рейдерів.

- у статуті підприємства, його локальних актах, більш ніж бажано закріпити ефективний механізм контролю за здійсненням менеджерами операцій, що передбачають відчуження активів підприємства, розпорядження великими сумами коштів, залучення крупних позик і кредитів. Наприклад, можна закріпити необхідність узгодження найважливіших для бізнесу операцій загальними зборами, менш значних – наглядовою радою. Всі обмеження щодо здійснення операцій від імені підприємства необхідно внести до Єдиного державного реєстру юридичних осіб і фізичних осіб – підприємців, щоб вони відображалися у виписках з реєстру. У подальшому виписки з реєстру можна використовувати як доказ неправомірності укладення договорів в суді.

- доцільно також прийняти на підприємстві Положення про комерційну таємницю і конфіденційну інформацію. У такому положенні необхідно передбачити можливість її надання третім особам тільки за рішенням загальних зборів (наглядової ради) і встановити відповідальність за її розголошення осіб, що мають до неї доступ. За законодавством України до категорії конфіденційної інформації можуть бути віднесені будь-які дані про підприємство (його діяльність), окрім передбаченої Ухвалою Кабінету Міністрів України «Про перелік відомостей, які не складають комерційної таємниці».

В усіх договорах, що укладаються підприємством та за якими підприємство виступає стороною-боржником, повинна бути передбачена умова, що уступка права вимоги за договором може бути здійснена тільки за згодою боржника. Це дозволить запобігти неконтрольованій скупці боргів підприємства.

Необхідно здійснювати постійний моніторинг:

а) активів і зобов'язань підприємства шляхом періодичного отримання виписок з реєстрів операцій, іпотек, заборон відчуження нерухомого майна, обтяження рухомого майна;

б) судових рішень відносно підприємства (на сьогоднішній день це дозволяє робити створена і вже працююча система реєстрів судових рішень у господарських, цивільних, кримінальних справах, яка доступна всім у мережі Інтернету);

– доцільно також зробити пакет нотаріально-засвідчених документів, що складається із установчих документів, протоколів загальних зборів, рішень керівних і контролюючих органів підприємства, зразків підписів основних власників і менеджменту, відбитку печатки, правовстановлюючих документів на основні активи. Такий пакет варто зберігати за межами території підприємства в важкодоступному для третіх осіб місці, наприклад, у нотаріуса, в банківському осередку та ін.;

– якщо мова йде про холдингову структуру, то бажано розділити між підконтрольними підприємствами процес виробництва і закупівлі сировини і реалізації продукції, що дозволить відокремити активи, що беруть участь у виробництві, від діяльності, яка може призвести до появи заборгованості на підприємстві, що має такі активи. Для цього створюються торгові доми, фірми-посередники між підприємством і постачальником сировини.

Перелічені вище заходи за характером дії належать до превентивних, спрямованих на попередження виникнення загроз рейдерства. До реактивних заходів належать, перш за все, дії конкурентної розвідки та контррозвідки, спрямовані на виявлення сигналів того, що на підприємство готується рейдерська атака, а саме:

– поява оголошень про купівлю акцій підприємства, зростання частоти їх купівлі-продажу;

– активізація інтересу до підприємства з боку податкових, правоохоронних органів чи інших владних структур, контролюючих та перевіряючих організацій;

– спроба порушення кримінальних справ чи судових позовів стосовно основних акціонерів і топ-менеджерів об'єкта;

– інформація про збирання працівниками підприємства чи сторонніми особами будь-якої інформації про об'єкт, його акціонерів і топ-менеджерів;

– несподівані спроби будь-яких осіб, в тому числі меншарних акціонерів, отримати статутні документи і протоколи засідань ради директорів і правління;

- поява нових ініціативників-інвесторів;
- прихід у регіон великого капіталу, особливо, якщо його бізнес-інтереси співпадають з діяльністю можливого об'єкта захоплення і він має підтримку у владних структурах тощо.

Якщо рейдерська атака все ж таки неминуха або вже відбулася, діяти слід швидко, але продумано. Природно, у кожному конкретному випадку необхідний індивідуальний підхід, проте деякі методи можуть виявитися доречними у будь-якому випадку. Так, якщо власник отримав інформацію про скупку корпоративних прав, що розпочалася рейдерами, можливо організувати контркуповування, адже частіше всього увагу міноритаріїв привертає саме ціна, запропонована рейдерами, а отже, він повинен погодитися на більш вигідні умови. Також можна провести додаткову емісію акцій (збільшити статутний фонд, якщо мова йде про ТОВ), чим істотно зменшити фактичний розмір рейдерського пакету корпоративних прав.

Активи підприємства необхідно законним способом передати у власність іншого підконтрольного підприємства більш стійкого до рейдерських атак організаційно-правовою формою – продати, внести до статутного фонду та ін.

У разі силового захоплення підприємства на підставі рішень судів слід невідкладно оскаржити такі рішення в судовому порядку та одночасно подати клопотання про припинення їх виконання. Також основним власникам варто власноруч звернутися до суду з позовами про визнання недійсними рішень загальних зборів, проведених без їх участі, а також рішень нового нелегітимного менеджменту.

Окрім вище переліченого, доцільно застосовувати:

- затягування процесу: якщо процес захоплення АТ гальмується, його ініціатори звичайно втрачають інтерес до АТ (якщо, звичайно, ними не витрачені значні кошти на придбання пакету акцій);
- моніторинг потенційних корпоративних конфліктів з метою своєчасного виявлення рейдерів, яких треба не боятися, а краще атакувати тоді, коли вони ще не готові до повноцінної «війни».
- використання існуючих невідповідностей чинного законодавства в інтересах АТ проти рейдерів.

Не зайвим буде звернутися із заявами в правоохоронні органи про здійснення нападу на підприємство, державні органи

по боротьбі з рейдерством, а також висвітлити вашу проблему в ЗМІ.

На сьогодні в Україні створена й діє система органів з протидії рейдерству:

- Громадська організація «Антирейдерський Союз підприємців України»;

- Український Національний комітет міжнародної торгової палати;

- Міжвідомча комісія з питань протидії протиправному поглинанню та захопленню підприємств при Кабінеті Міністрів України (Склад: представники МВС, СБУ, міністерств юстиції, економіки, фінансів, Держагентства з інвестицій і інновацій, Союзу промисловців і підприємців та Торгово-промислової палати, Держпідприємництва, Генпрокуратури, Фонду держмайна України);

- Бюро протидії комерційним злочинам та рейдерству (використання рекомендацій міжнародних організацій у боротьбі з рейдерством);

- Робочі групи з питань протидії протиправному поглинанню та захопленню підприємств при облдержадміністраціях.

Співпраця із переліченими організаціями суттєво посилить захист підприємства та забезпечить необхідний рівень економічної безпеки.

Як підсумок, потрібно ще раз підкреслити, що єдиного алгоритму протидії рейдерській атаці не існує. Найявніші суттєвих відмінних характеристик, які притаманні для вітчизняного рейдерства і у більшості пов'язані із злочинними протизаконними діями суттєво ускладнює процес захисту.

Від ефективності антирейдерських дій безпосередньо залежить існування та подальше функціонування підприємства, тому ігнорування або не приділення достатньої уваги проблемі гарантування економічної безпеки є суттєвою помилкою. В умовах сьогодення захисту бізнесу – це пріоритетне завдання системи економічної безпеки, а для його виконання потрібно організувати, вкласти кошти та підтримувати у постійній готовності власний підрозділ безпеки.

ЛІТЕРАТУРА ДО РОЗДІЛУ 5

1. Артемьев А. Б. Неприкосновенность собственности в законодательстве РФ // Актуальные проблемы частного правового регулирования. – Самара: Самарский государственный университет, 2004. – 421 с.
2. Берназ П. В. Рейдерство в Україні: визначення поняття / П. В. Берназ, О. О. Серета // Проблеми цивільного та господарського права. – 2008. – №1. – С. 82–84.
3. Беліков О. Рейдерство в Україні – реалії сьогодення / О. Беліков // Юридичний журнал. – 2007. – № 4. – С. 105–109.
4. Богарова О. Способи поглинання акціонерних товариств / О. Богарова // Підприємство, господарство і право. – 2009. – № 10. – С. 149–151.
5. Борисов Ю. Д. Рейдерство – это купить на грош пятаков [Электронный ресурс] / Ю. Д. Борисов // Известия – 20.07.2006. – Режим доступа до журн. : <http://www.izvestia.ru/news/315575>
6. Варналія З. Основні передумови та шляхи подолання рейдерства в Україні [Електронний ресурс] / З. Варналія, І. Мазур. – Режим доступу: <http://www.niss.gov.ua/monitor/juli/1.htm>.
7. Варналій З. С. Рейдерство в Україні: передумови та шляхи подолання / З. С. Варналій // Стратегічні пріоритети. – 2007. – № 2 (3). – 129 с.
8. Василенко П. Обережно: рейдери! / П. Василенко. – К. : Знання України, 2007. – 100 с.
9. Виханский О. С. Менеджмент: учебн. / О. С. Виханский, А. И. Наумов. – М.: Экономистъ, 2006. – 669 с.
10. Вільна енциклопедія Вікіпедія. [Електронний ресурс]. – Режим доступу: <http://uk.wikipedia.org/wiki/> – 12.10.2011р.
11. Голибард Є. І. Кучмізм і кучмономіка. Частина перша : Документальна доповідь про афери корумпованої влади / Є. І. Голибард. – К. : Пульсари, 2005. – 511 с.
12. Головань И. Удар в стык: почему процветает «рейдерство» в Украине [Электронный ресурс] / И. Головань // Зеркало недели. – 2006. – Режим доступа : <http://www.cripo.com.ua>.
13. Горбов В.В. Правовая защита акционерного общества от недружественного поглощения: Автореф. дис. на соиск. учен. степ. канд. юрид. наук. / В.В.Горбов – М., 2004.
14. Грачев В. Некорпоративные методы захвата чужого бизнеса / В. Грачев // Враждебные поглощения в Украине. – 2008. – № 3 (6). – С. 57–61.

15. Диба І. Обличчя зла, або як боротися з рейдерством / І. Диба // Юридичний вісник України. – 2006. – № 17. – С. 8.
16. Дічек О. Рейдерство в Україні: правові ознаки і шляхи запобігання / О. Дічек, Ю. Нікітін // Юридичний журнал. – 2008. – С. 34–41.
17. Єфіменко А. «Рейдерство або ринок контролю» / А. Єфіменко // Юридичний журнал. – 2008. – № 11(57). – С. 117–119.
18. Житомирский В. С. В блокнот предпринимателю. Рейдерство: явления, причины, профилактика, защита / В. С. Житомирский. – СПб.: Ленинградская торгово-промышленная палата. – 2006. – 54 с.
19. Задихайло Д. Корпоративне управління : навч. посіб. / Д. Задихайло, О. Кібенко, Г. Назарова. – Х. : Фоліо, 2003. – 687 с.
20. Защита бизнеса от рейдерских атак: методические рекомендации. / Ю. И. Кравец. – Изд. 2-е, изм. и доп. – О. : Феникс, 2009. – 24 с.
21. Зеркалов Д. В. Антирейдер : пособ. / Д. В. Зеркалов. – Киев : Дакар, КНТ, Основа, 2007. – 224 с. – (Серия : Международная и национальная безопасность).
22. Зубков А. Е. Накануне рейдерской атаки / А. Е. Зубков // Враждебные поглощение в Украине. – 2007. – №2 (10). – С.5–8.
23. Ионцев М. Т. Корпоративные захваты: слияние, поглощение, гринмейл / М. Т. Ионцев. – М.: Ось-89. – 2008. – 272 с.
24. Интернет-проект НацБез [Электронный ресурс]. – Режим доступа: <http://www.nacbez.ru> – 25.10.2011 р.
25. Касьяненко Н. С. Недружественные поглощения (рейдерство) организаций в России / Н. С. Касьяненко // Вестник Челябинского государственного университета Экономика. – 2009. – Вып. 18. – С. 119–124.
26. Кацун Ю. Вічне свято / Ю. Кацун // День. – 2006. – 13 травня.
27. Киреев А. Ю. Рейдерство в Российской экономике: сущность, тенденции и возможность противодействия : автореф. дис. на соискание учен. степени канд. экон. наук : спец. 08.00.05 «Экономика и управление народным хозяйством» / А. Ю. Киреев. – М., 2008. – 22 с.
28. Киреев А. Рейдерство на рынке корпоративного контроля: результат эволюции силового предпринимательства / А. Киреев // Вопросы экономики. – 2007. – №8. – 80 с.
29. Кныш М. И. Стратегическое управление корпорациями / М. И. Кныш, В. В. Пучков, Ю. П. Тютиков. – СПб. : Культинформпресс, 2002. – 239 с.
30. Королев М. И. Устранение рисков при слияниях и поглощениях / М. И. Королев // Бизнес и безопасность. – 2010. – № 1. – С. 19–21.
31. Краснодарська З. Вакцина проти рейдерства / З. Краснодарська // Урядовий кур'єр. – 2007. – 22 лютого.
32. Куц В. Рейдерство: кримінально-правовий аспект / В. Куц // Підприємництво, господ. і право. – 2007. – № 10. – С. 128–131.

33. Лазуренко В. И. Рейдерство: слиния и поглощения / В. И. Лазуренко, Я. Н. Ломакин, Ю. В. Хазуренко. – М.: ГУКВН, 2009. – 232 с.
34. Мамутов В. Рейдерство в законі / В. Мамутов // Дзеркало тижня. – 2008. – № 38. – С. 2–3.
35. Мескон М. Основы менеджмента / М. Мескон, М. Альберт, Ф. Хедоури ; пер. с англ. – М.: Издательство «Дело», 1997. – 492 с.
36. Михайлів У. Влада проти церкви: план на знищення / У. Михайлів // Україна молода. – 2011. – 5 січ.
37. Основні передумови та шляхи подолання рейдерства в Україні : аналіт. зап. // Персонал. – 2007. – № 27 (230). – С. 33–37.
38. Паславський І. Основні етапи протидії українському бізнесу: роль і позиції ЗМІ / І. Паславський // Вісник Львів. нац. ун-ту. – 2011. – Вип. 34. – С. 158–172.
39. Патиківський Ю. Чорний переділ / Ю. Патиківський // Україна молода. – 2007. – № 93. – С. 34–41.
40. Петренко В. А. О защите лучше думать до захвата / В. А. Петренко // Враждебные поглощение в Украине. – 2007. – №1 (07). – С. 51–56.
41. Положення про Міжвідомчу комісію з питань протидії і протиправному поглинанню та захопленню підприємств / Затверджено постановою Кабінету Міністрів України від 21 лютого 2007 р. №257
42. Полушкин О. А. Рейдерство: пути решения актуальных проблем / О. А. Полушкин // Закон и право. – 2008. – №3. – С. 23–27.
43. Рейдерство в Україні: загрози та шляхи протидії. – К., 2010. – 148 с.
44. Рид Стенли Фостер. Искусство слияний и поглощений / Стенли Фостер Рид, Александра Рид Ложу; пер.с англ. – М.: «Алпика бизнес букс», 2004. – 958с.
45. Ростоцька Ю. Рейдерство: прогресуюча хвороба української економіки / Ю. Ростоцька. [Електронний ресурс]. – Режим доступу: <http://www.anti-crime.org>
46. Савельев Є. В. Економічна та майнова безпека підприємства і підприємництва. Антирейдерство / Є. В. Савельев, З. В. Гуцайлюк, В. В. Козюк та ін. – Тернопіль: Вид. Терно-граф, 2008. – 424 с.
47. Словарь иностранных слов / [под ред. И.В. Лёхина и проф. Ф.Н. Петрова]. – М. : Гос. Изд-во иностр. и нац. словарей, 1954. –598 с.
48. Страна должна знать своих героев: крепнейшие рейдеры Украины. [Електронний ресурс]. – Режим доступу : <http://www.management.web-standart.net>.
49. Тарханова З. Э. Функционирование института рейдерства в РФ : дис. ... канд. экон. наук : 08.00.01. – Владикавказ, 2008. – 223 с.
50. Тіньова економіка: сутність, особливості та шляхи легалізації / за ред. З. С. Варналія. – К.: НІСД, 2006. – 576 с.

51. Ткачук М. Рейдерство «від Бога» / М. Ткачук // Україна молода. – 2010. – 2 черв.
52. Туник И. Ю. Антирейдер: пособие по противодействию корпоративным захватам / И. Ю. Туник, В. А. Поляков. – СПб.: Питер, 2007. – 208 с.
53. Устаев Н. Как противостоять рейдерству / Н. Устаев // Діловий вісник. – 2007. – №4. – С.16–17.
54. Фоміна К. Шляхи подолання рейдерства / К. Фоміна // Правовий тиждень. – 2008. – №39 (112). – 23 верес.
55. Фёдоров А. Ю. Рейдерство и корпоративный шантаж (организационно-правовые меры противодействия) / А. Ю. Фёдоров. – М.: Волтерс Клувер, 2010. – 480 с.
56. Хоружий С. Про деякі проблеми ринку цінних паперів / С. Хоружий // Фінансові ризики. – 2000. – № 2. – С. 5–13.
57. Цивільний кодекс України, № 435-IV від 16 січня 2003 р., остання редакція.
58. Черних Д. Протидія «рейдерству»: теоретико-правовий аспект / Д. Черних // Вісник прокуратури. – 2007. – №5. – С.64–70.
59. Шевченко І. Л. Рейдерство: основні схеми здійснення та способи захисту / І. Л. Шевченко // Економічний простір. – 2008. – №13. – С. 69–76.
60. Шляхи подолання рейдерства: удосконалення законодавства та посилення реагування правоохоронних органів на протиправні дії його організаторів і виконавців: матеріали Комітетських слухань Верховної Ради України. – К. : Міжвідом. наук.-дослід. центр з пробл. боротьби з організованою злочинністю при РНБО, 2008. – 127 с.
61. Andarad G. New Evidence and Perspectives on Mergers / Andarad G., Mitchell M., Stafford E. // Journal of Economic Perspectives. – 2001. – Vol. 15. – P. 103–120.
62. Edilberto Segura Hostile Takeovers in Ukraine //Sigma Blazer 2007.
63. Koeke J. The Market for Corporate Control in Germany: Causes and Consequences in Ultimate Share Ownership / J. Koeke. – Mannheim : Centre for Economic Research (ZEW), 2000. – 39 p.
64. Milhaupt C. J. In the Shadow of Delaware? The Rise of Hostile Takeovers in Japan / Milhaupt C. J. // Columbia Law Review. – 2005. – Vol. 105. – P. 2171–2216.
65. Shleifer A. The Takeover Wave of the 1980s / Shleifer A., Vishny R.W. // Science. – 1990. – Vol. 249. – P. 713–828.

ПІСЛЯМОВА

Здійснене теоретико-аналітичне дослідження дозволило комплексно дослідити теоретичні основи гарантування економічної безпеки на мікрорівні, охарактеризувати поточний стан, виявити ряд ключових загроз та окреслити напрямки вдосконалення управління економічної безпеки підприємства.

При цьому отримані наступні результати:

- охарактеризовано сучасне трактування поняття «економічна безпека підприємства», що ґрунтується на пріоритетності забезпечення безпеки для існування будь-якої соціально-економічної системи та важливості управління цим процесом внаслідок складності та непередбачуваності змін у зовнішньому середовищі, неможливості здійснення абсолютного контролю внутрішнього середовища та зростанні, як наслідок, кількості зовнішніх та внутрішніх загроз;

- узагальнення доробку закордонних та вітчизняних науковців дозволило сформуванню власний підхід до управління економічною безпекою підприємства через створення механізму управління комплексною системою економічної безпеки підприємства, який передбачає виділення у структурі економічної безпеки ряд ключових функціональних складових, забезпечує оцінку поточного рівня безпеки, передбачає розроблення тактики і стратегії, здійснення оперативного управління у взаємодії із системою управління усього підприємства та уможливорює зменшення негативного впливу внутрішніх та зовнішніх загроз;

- в сьогоденних складних умовах функціонування, ефективне управління економічною безпекою підприємства є неможливим без формування відповідної концепції, яка, за результатами проведеного теоретичного дослідження, повинна враховувати специфіку господарської діяльності певного підприємства, містити обґрунтування функціональної та інституційної позицій, чітко визначення системи забезпечення із обов'язковим поділом на науко-

во-методичну, практичну та організаційно-економічну складові та сам механізм управління комплексною системою економічної безпеки підприємства;

- спираючись на офіційні статистичні дані було охарактеризовано поточний рівень економічної безпеки підприємств в Україні, через концентрацію уваги на пріоритетних аспектах, зокрема динаміки кількості суб'єктів господарювання, забезпечення та ефективністю використання трудових ресурсів, фінансових результатах, що уможливило ідентифікацію та визначення сутності окремих загроз для економічної безпеки;

- здійснене аналітичне дослідження дозволило сформува-ти сукупність ключових загроз для економічної безпеки вітчизняних підприємств, що, в подальшому, завдяки застосуванню математичного моделювання із використанням ієрархічних моделей дозволило визначити пріоритетність впливу окремих загроз та стало основою для удосконалення процесу управління економічною безпекою на мікрорівні;

- виконання працівниками підприємства ролі як об'єкта, так і суб'єкта безпеки спонукала до ретельного дослідження сутності поняття «кадрова безпека» та обґрунтування природи й характеру загроз, джерелом виникнення яких є персонал, що, в подальшому, уможливило формування концептуальних основ управління кадровою безпекою підприємства та визначення переліку й послідовності реалізації заходів для протидії негативному впливу;

- дослідження історичних аспектів розвитку конкурентної розвідки та пріоритетності інформаційних ресурсів для гарантування економічної безпеки підприємства уможливили обґрунтування необхідності активного застосування розвідувальних та контррозвідувальних дій в системі економічної безпеки, що стало основою для побудови моделі з чітко окресленим визначенням функціональних завдань конкурентної розвідки та контррозвідки;

- охарактеризована суттєва відмінність ролі рейдерства в розвитку підприємництва в розвинутих країнах світу та в Україні спонукала до ретельного дослідження сутності даного явища, розгляду заходів протидії та розроблення методичних засад захисту, які б враховували найбільш поширені схеми захоплення, вплив чинників, що можуть як знизити рівень опору рейдерській атаці, так і сприяти збереженню бізнесу.

НАУКОВЕ ВИДАННЯ

Живко Зінаїда Богданівна

ЕКОНОМІЧНА БЕЗПЕКА
ПІДПРИЄМСТВА:
СУТНІСТЬ, МЕХАНІЗМ
ЗАБЕЗПЕЧЕННЯ
ТА УПРАВЛІННЯ

Монографія

Коректура – *Ілона Живко*
Комп'ютерна верстка – *Михайло Живко*

Папір офсетний. Друк на різнографі. Гарнітура Times.
Ум. друк. арк. 14,88. Ум. фарб.-від. 14,9.
Тираж 500 прим.

Видавництво:
ТзОВ «Ліга-Прес»
79006 м. Львів, а/с 11018

Друк:
СПДФО «Марусич М.М.»
м. Львів, пл. Осмомисла 5/11
тел. (032) 261-51-31