МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ІНСТИТУТ ЕКОНОМІКО-ПРАВОВИХ ДОСЛІДЖЕНЬ
НАН УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА В УМОВАХ РЕЙДЕРСЬКИХ ЗАГРОЗ

Колективна монографія за науковою редакцією
О.А. Бурбело, С.К. Рамазанова

Монографія

Київ
2015

УДК 351.863:343.722
ББК 65.290.4
Е 45

Рекомендовано
Вченою радою Інституту економіко-правових досліджень
Національної академії наук України
(Протокол № 10 від 30.11.2015 р.)

Рецензенти:

Калінеску Т.В.–д. е. н., професор, завідувач кафедри «Оподаткування і соціальної економіки» Східноукраїнського національного університету імені Володимира Даля;

Ляшенко О.М.–д. е. н., професор, вчений секретар Національного інституту стратегічних досліджень.

Погорелов Ю.С.– д. е. н., доцент, завідувач кафедрою обліку та аудиту Полтавського національного технічного університету імені Юрія Кондратюка.

Е 45 **Економічна безпека підприємства в умовах рейдерських загроз:** колективна монографія [Текст] / [О.А.Бурбело, С.К. Рамазанова, О.М.Заєць, Т.С. Гудіма, О.М. Кузьменко / за наук. ред. О.А.Бурбело, С.К. Рамазанова]. – Сєвєродонецьк: Вид-во СНУ ім. В. Даля, 2015. – 285 с.

ISBN 978-617-11-0052-7

У монографії розглядаються теоретичні й практичні аспекти забезпечення економічної безпеки підприємства в умовах рейдерських загроз, розкривається її економіко-правова природа та понятєвий апарат, визначаються основні напрями забезпечення економічної безпеки суб'єктів господарювання та окремих секторів економіки держави. Подаються висновки та рекомендації щодо вдосконалення існуючої методики забезпечення економічної безпеки підприємства та галузей економіки, а також законодавства України.

Для науковців, аспірантів, студентів юридичних та економічних навчальних закладів, а також усіх, хто цікавиться цією проблемою.

УДК 351.863:343.722
ББК 65.290.4
ISBN 978-617-11-0052-7

© Бурбело О.А.,
Рамазанов С.К.,
Заєць О.М.,
Гудіма Т.С.
Кузьменко О.М

З М І С Т

ПЕРЕДМОВА 5

РОЗДІЛ 1. РЕЙДЕРСТВО: ПОНЯТТЯ ТА ПЕРЕДУМОВИ ВПЛИВУ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА 8
1.1.Виникнення та розвиток рейдерства..... 8
1.2. Передумови та особливості розвитку рейдерства в Україні 28
1.3. Вплив загроз рейдерства на економічну безпеку підприємства ... 43

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ЗАГРОЗ РЕЙДЕРСЬКИХ ПОСЯГАНЬ НА ПІДПРИЄМСТВО 62
2.1. Виявлення факторів небезпеки для підприємства..... 62
2.2. Діагностика рівня економічної безпеки підприємства та оцінка їх захищеності 72
2.3. Методи управління безпекою підприємства..... 90
2.4. Визначення детермінант, що сприяють здійсненню рейдерських атак на підприємство..... 99

РОЗДІЛ 3.СТРАХУВАННЯ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА..... 117
3.1. Поняття, сутність та правовий зміст страхування, його місце у системі забезпеченні економічної безпеки 117
3.2. Страхування ризиків підприємства: поняття та класифікація 126
3.3. Мінімізація ризику втрати права власності, шляхом рейдерського захоплення, завдяки використанню титульного страхування..... 138

РОЗДІЛ 4.ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ..... 145
4.1. Напрями забезпечення економічної безпеки залізничного транспорту..... 145
4.2. Чинники, що впливають на економічну стійкість підприємства..... 151
4.3. Показники і методи оцінки економічної стійкості підприємства.....162
4.4. Прогнозування та оцінка рівня економічної безпеки підприємства 176

РОЗДІЛ 5. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ЯК СКЛАДОВА ЙОГО ЕКОНОМІЧНОЇ БЕЗПЕКИ 201
5.1. Сутність і зміст інформаційної безпеки промислового підприємства 201
5.2. Методи оцінки інформаційної захищеності підприємства 211
5.3. Комплексна оцінка інформаційної захищеності підприємства ... 220
5.4. Оптимізація системи захисту інформації на підприємстві 224

РОЗДІЛ 6. РОЗРОБКА ІМІТАЦІЙНОЇ МОДЕЛІ ДЛЯ КОМПЛЕКСНОЇ ОЦІНКИ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ В УМОВАХ РЕЙДЕРДЕРСЬКИХ ЗАГРОЗ 235
6.1. Оптимізація та оцінка витрат на створення інфраструктури захисту інформації на підприємстві 235
6.2. Основні властивості та структура імітаційної моделі 240
6.3. Синтез інфраструктури захисту інформації підприємства 244
6.4.Система моніторингу та шляхи вдосконалення інфраструктури захисту інформації 248
6.5. Імітаційна модель вірогідності реалізації загроз інформаційній безпеці підприємства 255

ВИСНОВКИ 266

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 267

П Е Р Е Д М О В А

Сучасні економічні реалії, пов'язані перш за все з глобалізацією світової економіки, вимагають переосмислення підсумків економічного розвитку України за роки незалежності та оцінки перспективності різних альтернативних стратегій економічного розвитку держави в контексті формування та забезпечення національної безпеки.

Проблеми економічної безпеки як складової національної безпеки залишаються понад двадцять років одними з життєво важливих як в справі існування і розвитку України у вигляді незалежної, єдиної та могутньої держави так і в справі наукових досліджень нових напрямів безпекознавства. Економічна безпека підприємств є одним з важливих розділів безпекознавства і наукові здобуття у цій сфері є доволі вагомими. Достатньо назвати дослідження таких відомих вітчизняних науковців як О.О. Ашуркова, І. А. Білоусова, О. А. Бурбело, В. В. Вітлінського, В. М. Гейця, І. В. Заблодської, В.А. Устименка, М. О. Кизима, Г. В. Козаченко, О. Є. Користіна, О. М. Ляшенко, В.К. Мамутова, І. П. Мігуса, Ю.С. Погорелова, С.К. Рамазанова, В. І. Франчук, а також російських М. А. Бендикова, Л. П. Гончаренко, Т. Б. Клейнер, В. К. Сенчаков та багато інших.

Інститут економіко-правових досліджень має значний досвід роботи досліджень тематики економічної безпеки. Так були підготовлені та видані: монографія (Економічний суверенітет держави та напрями його правового забезпечення (2012 р.)), Методика системної діагностики впливу стану зовнішньої торгівлі на зміну рівня економічного суверенітету України (2012 р.), проведено круглий стіл (Правове забезпечення економічного суверенітету держави в умовах міжнародної інтеграції (2010 р.), реалізовано два конкурсних проекту НАН України («Правове забезпечення економічного суверенітету в умовах міжнародної інтеграції» (2010 р.) та «Економічні важелі забезпечення державного суверенітету» (2011 р) тощо.

За підсумками досліджень за двома вищевказаними конкурсними проектами співробітники Інституту брали участь у підготовці Концепції правового забезпечення економічного суверенітету в умовах міжнародної інтеграції (О.О. Ашурков, 2011 р.) та Національної доповіді «Національний суверенітет України в умовах глобалізації» (О.О. Ашурков, О.Ю. Ілларіонов, 2011 р.).

При всій повазі до наукових внесків названих авторів в дослідження проблеми економічної безпеки підприємств слід зазначити, що дослідженню питань забезпечення економічної безпеки підприємств в умовах протиправного їх злиття та поглинання було приділено недостатньо уваги.

Виробнича діяльність постійно пов'язана з ризиками. Усі фінансово-господарські операції в тій чи іншій мірі піддаються ризикам, серед множини яких певне місце займає один з видів неправомірного заволодіння майном (активами) – рейдерство. Відбити рейдерську атаку вельми важко, ніж атакувати. На практиці дуже часто буває так, що підприємству треба за короткий час активної фази здійснити ті кроки, на які рейдер витратив не поспішаючи декілька місяців.

На сучасному етапі економічного розвитку держави рейдерські захоплення здійснюють олігархічні та фінансово-промислові групи з метою свого подальшого розвитку або диверсифікації власних бізнес-корпорацій, створення нових більш потужних корпорацій, консорціумів тощо.

Загрози економічній безпеці підприємств виникли не сьогодні, вони є результатом розвитку національної економіки у минулому, помилок у проведенні економічних реформ у 90-ті роки, а також аморфності поточної науково-промислової політики, втрати керованості економікою країни.

Монографія складається з шістьох розділів.

У першому розділі розглянуто теоретичні питання виникнення та розвитку рейдерства, передумови та особливості його розвитку в Україні, впливу загроз рейдерства на економічну безпеку підприємства.

Другий розділ містить дослідження факторів небезпеки для підприємств, механізму діагностики рівня економічної безпеки підприємств та оцінки їх захищеності, методів управління безпекою підприємств та визначення детермінантів, що сприяють здійсненню рейдерських атак на суб'єкти господарювання.

У третьому розділі досліджено процеси формування системи страхування ризиків підприємства, розробки, що забезпечують мінімізацію ризику втрати права власності шляхом рейдерського захоплення, завдяки використанню титульного страхування, а також сутність ефективності функціонування системи страхування ризиків економічної безпеки підприємства.

У четвертому розділі на прикладі підприємств залізничного транспорту проведено комплексне дослідження напрямків забезпечення

економічної безпеки підприємств, чинників, що впливають на економічну стійкість транспортних підприємств, показників і методів оцінки стійкості, а також здійснено прогнозування та оцінку рівня економічної стійкості суб'єктів господарювання.

П'ятий розділ присвячено дослідженню інформаційної безпеки підприємств в умовах рейдерських загроз з розробленням концептуальної моделі(моделі формування інфраструктури захисту інформації підприємства від рейдерських посягань).

У шостому розділі розроблено імітаційну модель комплексної оцінки засобів захисту інформації на підприємстві як основи оцінки та оптимізації витрати на створення інфраструктури захисту інформації на підприємстві, а також запропоновано систему моніторингу та шляхи вдосконалення цієї інфраструктури.

Монографія є результатом наукового співробітництва вчених Одеського державного університету внутрішніх справ України, Інституту економіко-правових досліджень НАН України та Східноукраїнського національного університету імені В. Даля.

Автори глибоко вдячні рецензентам: завідувачу кафедрою «Оподаткування і соціальної економіки», доктору економічних наук, професору Східноукраїнського національного університету імені Володимира Даля, Калінеску Т. В.; вченому секретарю Національного інституту стратегічних досліджень, доктору економічних наук, професору Ляшенко О. М.; завідувачу кафедрою обліку та аудиту Полтавського національного технічного університету імені Юрія Кондратюка, доктору економічних наук, доценту Погорелову Ю.С., а також всім тим, хто сприяв публікації монографії.

Р О З Д І Л 1

РЕЙДЕРСТВО: ПОНЯТТЯ І ПЕРЕДУМОВИ ВПЛИВУ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА

1.1. Виникнення та розвиток рейдерства

Найважливішим інститутом національної ринково орієнтованої економіки у своїй середньостроковій і довгостроковій перспективі є інститут власності.

На жаль, ретроспективний аналіз національної моделі господарювання свідчить про наявність системних проблем розвитку національного інституту приватної власності. Це виявляється в недосконалості методології перерозподілу власності, декларативності національної моделі ринкової оцінки ліквідних активів суб'єктів господарювання, корупційній та прихованій для громадського контролю системі реєстрації права власності, виключно низькій транспарентності бізнес-процесів, недосконалості господарського (у тому числі корпоративного) законодавства.

Вищезазначені фактори разом із швидким загостренням корпоративних конфліктів зумовили виникнення нової форми «квазіпідприємницької» діяльності – рейдерства. Зазначена діяльність становить силове недружнє поглинання підприємства (суб'єкта господарювання) проти волі його власника або ж власника істотної участі підприємства. Зазначена проблематика стала предметом дослідження багатьох вчених, зокрема О.О. Ашуркова, О. А. Бурбело., В.А. Устименка, В.К. Мамутова та інших

Про реальну масштабність розповсюдження рейдерської активності свідчить створення в Україні Міжвідомчої комісії з питань протидії протиправному поглинанню та захопленню підприємств, що діє при Кабінеті Міністрів України.

Вирішенням проблеми активного поширення рейдерства займаються не тільки представники науки та практики, а й державні урядовці.

Так, під час зустрічі з послами країн-учасниць ЄС і деяких інших країн члени уряду України визнали, що в державі існують проблеми у галузі ведення бізнесу, зокрема незаконне захоплення підприємств – рейдерство.

За словами державних урядовців, рейдерство не тільки відлякує інвесторів від України, а й гальмує її економічний розвиток, водночас «… боротьба з цим явищем стає державним пріоритетом» [1]

Як вітчизняні, так і закордонні автори, цілком справедливо відзначають, що в умовах інтенсифікації рейдерських атак «... приватна власність розглядається як гіпотетичний об'єкт зазіхань з боку агресорів», а сама власність, «... що розглядається суспільством як приватна, є лише квазіприватною, тобто може бути експропрійована в будь-який момент»[2]. Підтвердженням зазначеної думки є те, що інститут рейдерства зумовлює виникнення нового виду господарсько-правового ризику, а також спотворення менталітету бізнес-спільноти.

Звертаючи увагу на цю обставину, В.К. Мамутов, зауважував на необхідності першочергового попередження створення сприятливих умов для рейдерства в законодавстві. Тобто на самому високому рівні держави. «Навіщо зайвий раз балансувати на грані Кримінального кодексу, коли можна створювати необхідні лазівки в законодавстві. В Україні це зробити не дуже складно. Коли рейдерство здійснюється навіть на такому рівні, діяльність правоохоронних органів стає неефективною» - зазначив вчений на слуханнях з даної тематики в Верховній Раді України[3].

Отже, нещодавно сформоване в колисці «силового підприємництва» рейдерство вже встигло перейти межі легітимності соціально-економічної поведінки. На цьому етапі свого розвитку рейдерство набуло форми вольових актів підвищеної суспільної небезпеки, що обмежують законні права й інтереси власників, персоналу підприємств. Протидія цьому феномену приречена на фіаско за межами чіткого й однозначного розуміння його економіко-правової суті та історії становлення та розвитку.

Етимологію поняття «рейдерство» пов'язують з піратством – морським розбоєм. Термін «рейдерство» походить від англійського *The*

---

[1]Привлечение и защита инвестиций станут приоритетом в работе украинского правительства [Електронне джерело] – Офіційний портал інформаційної агенції «УНІАН». – Режим доступу: http://www.unian.net/news/577585-arbuzov-poobeschal-evropeyskim-poslam-iskorenit-reyderstvo-v-ukraine.html

[2]Скиданова Лилия Алексеевна. Рейдерство как социально-экономический феномен : диссертация ... кандидата социологических наук : 22.00.03 / Скиданова Лилия Алексеевна. - Москва, 2010.- С. 23.

[3] Мамутов В. Рейдерство в законі/ В. Мамутов//Дзеркало тижня. - 2008. – No 38.

raid- набіг, раптовий напад, або *raider* - нальотчик. Рейдером в англомовних країнах називали особу, яка входила до невеликого мобільного озброєного угрупування, що пересувається, вчиняючи напади, а також морських піратів [1]. Зародилося рейдерство у Великобританії, коли британські військові кораблі поодинці виконували бойові завдання із захоплення торгових кораблів інших держав [2].

Згодом слово «рейд» в англійській мові набуло таких додаткових значень, як *несподівана атака невеликими військовими силами; вторгнення на чужу територію з метою загарбання товарів або інших цінностей; дії, спрямовані на знищення конкурента, на захоплення контролю над підприємством через придбання більшості акцій; дії спекулянтів, спрямовані на зниження цін на акції через узгоджений ними одночасний продаж* тощо[3].

В економічній науці існує думка, що саме розвиток корпоративних відносин зумовив виникнення рейдерства.

Так, відомий дослідник рейдерства та корпоративного шантажу А.Ю. Федоров безпосередньо відзначає «…рейдерство з'явилося на світ разом з акціями, коли виникла можливість поглинання компанії за межами волі її власника»[4]. Обґрунтувати таке твердження можна історичним фактом про спробу захвату французької Ост-Індської торгівельної компанії гасконським дворянином Жан-Пьером, бароном де Батц. Разом з групою фінансистів, мета яких за допомогою сумнівних фінансових операцій дискредитувати новий республіканський уряд на користь роялістів, він намагався у дні Великої французької революції (1789-1794 рр.) ліквідувати Ост-Індську торгівельну компанію. Задля реалізації цієї мети барон Жан де Батц підготував відповідну доповідь.

---

[1]Тивончук І. О. Особливості рейдерства в Україні / І. О. Тивончук, Г. Я. Глинська // Вісник Національного університету «Львівська політехніка». Менеджмент та підприємництво в Україні : етапи становлення і проблеми розвитку : зб. наук. праць. – Львів : НУ «Львівська політехніка», 2008. – № 624. – С. 146–150.

[2]Тіньова економіка: сутність, особливості та шляхи легалізації : [монографія] / [за ред. З. С. Варналія]. – К. : НІСД, 2006. – С. 6.

[3]Сметанкина Ю. Что такое рейдерство? / Ю. Сметанкина // Власть. – 2007. – № 1. – С. 37-42.

[4] Федоров А.Ю. Рейдерство и корпоративный шантаж (организационно-правовые меры противодействия) : монография / А.Ю. Федоров. – М.: Волтерс Клувер, 2010. – С. 6.

Він розраховував, що її виголошення призведе до масового продажу акцій та їх подальшого викупу за низькою ціною[1].

У контексті історичного дослідження поширення рейдерських дій заслуговують на увагу факти перерозподілу власності на теренах пострадянського простору. Так, дослідивши зазначений феномен економіко-правових відносин у давні часи, український дослідник О. Бєліков звертає увагу на чотири періоди перерозподілу власності: перший – в епоху Івана Грозного; другий – у часи правління Петра Першого; третій – після Великої Жовтневої соціалістичної революції 1917 року; четвертий – починаючи з 1990 р. й до сьогодні.

На думку автора, «… усі масові захоплення, поглинання та перерозподіли власності в будь-якій країні завжди ініціювалися державою. Досить пригадати Солона в Древній Греції, Кромвеля в Англії, «релігійні» війни в Німеччині, Велику Французьку революцію. Те саме відбувалося й у нас: від шабашів опричників до «експропріації» експропріаторів. Отже, досвіду розвитку, становлення та процвітання рейдерства як масового явища в нас більше, ніж достатньо»[2].

У сучасному, економічному контексті, тлумачення поняття «рейдерство» прийшло до нас із США, де на початку 80-х років XIX століття рейдерами називали фахівців із захоплення на замовлення підприємств або захоплення оперативного управління підприємствами. Саме в 1920-1930 роках, під час новітнього формування американської моделі організованої злочинності, рейдерство набуває кримінальних ознак. Звертаючи увагу на цю обставину, В. Овчинський зазначає, що рейдерство вже тоді стало «…найбільш ефективною формою організованої злочинності»[3].

На думку А.Ю. Федорова, «… історичний розвиток недружніх поглинань корпорацій у США починає свій відлік від відомого американського підприємця Джона Дейвисона Рокфеллера». Створивши в 1866 році через підставних осіб *Union Tank Car Company*, що спеціалізувалася на лізингу залізничного обладнання (вагони-цистерни, залізничні вагони та бункера), він створював пільгові умови для своїх конкурентів з метою надання їм змоги подальшого розвитку бізнесу. Але

---

[1] Фаенсон, М.И. Рейдерство (недружественный захват предприятий): практика современной России / М.И. Фаенсон, А.А. Пиманова. – М.: Издательство «Альфа-Пресс», 2007. – С. 5.

[2] Бєліков О. Рейдерство в Україні – реалії сьогодення // Юридичний журнал. – 2007. – № 4. – С. 105-109.

[3] Овчинский В. Рейдеромафия / В. Овчинский // Огонек. - 2007. - № 16. - С. 19.

згодом «…*Union Tank Car Company* в односторонньому порядку розривав контракти з цими компаніями. З мертвим вантажем переробленої сировини, відсутністю притоку зароблених грошей і несплаченими кредитами на розвиток виробництва ці компанії незабаром ставали банкротами, і Рокфеллер скуповував їх задешево. Так було створено найбільшу нафтову імперію»[1].

На думку деяких авторів, у тому числі Ю. Земцевої, існуюча на цей час Exxon Mobile, що за своєю суттю є правонаступником заснованої Джоном Рокфеллером Standart Oil, «… продовжує справу свого засновника та розширює сферу своєї діяльності за рахунок рейдерських поглинань, але вже не в США, а за їх межами»[2].

Активність рейдерів у США суттєво зросла в 1980-і роки, коли Майкл Мілкен почав використовувати «сміттєві облігації» для фінансування захоплень. Слід зазначити, що згідно з даними американської «Енциклопедії «білокомірцевої» та корпоративної злочинності», з 1974 до 1990 року компанія Мілкена (en: Drexel Burnham Lambert) навіть проводила щорічний кількаденний «Бал хижаків» (англ. Predator's Ball) для розваги рейдерів і зустрічей з вкладниками капіталу[3].

Між тим, професор швейцарського університету Лугано (італ. *Università della Svizzera italiana*, USI) Етторе Гроссі, зазначає, що в континентальній Європі масштабне рейдерство з'явилося лише в 1990-і роки. До цього часу аналізоване явище майже не зустрічається. Наприклад, з 1945 до 1998 року в Німеччині відбулося лише три спроби недружнього поглинання компаній поза фінансовою сферою[4].

Сьогодні рейдери – спеціалісти з перехоплення оперативного управління чи власності фірми за допомогою спеціально ініційованого

---

[1]Манахов С.А., Акжигитов Р.И., Сычев П.Г. О международном опыте по противодействию преступлениям на рынке ценных бумаг, в том числе противоправным корпоративным захватам имущественных комплексов юридических лиц // Аналитический обзор. - М.: Следственный комитет при МВД России, 2009. - С. 5.

[2]Земцова Ю. Сестрички ExxonMobile / Ю. Земцева / Слияния и поглощения. – 2006. – № 9. – С. 104-109.

[3] Lawrence M. Salinger. Encyclopedia of white-collar and corporate crime. — SAGE, 2005. — P. 263.

[4]Ettore Croci. The Market for partial corporate control in Europe: The evidence about corporate raiders. 2004.[Электронный ресурс] /EttoreCroci. – Режим доступу: http://www.eea-esem.com/papers/eea-esem/2004/185/ettore_croci_corp_raiders.pdf.

бізнес-конфлікту[1].Отже, рейдер – це суб'єкт, який агресивно захоплює підприємство, що діє переважно в організаційно-правовій формі акціонерного товариства, без згоди акціонерів (учасників), працівників, адміністрації. Термін має негативне забарвлення.

У корпоративному праві США та Західної Європи терміном «рейдер» позначають особу, яка починає активно скуповувати акції з метою отримання контрольного пакету. Рейд розглядають як операцію (спробу) з придбання значного пакету акцій певного підприємства з метою його поглинання. Використовують і такі поняття, як «рейд на світанку» (швидке скуповування акцій одразу ж після відкриття біржі з метою підготовки до поглинання) і «рейд преміальний» (неочікувана спроба поглинути підприємство шляхом пропозиції акціонерам премії, вищої за ринкову ціну їх акцій)[2].

У зарубіжній практиці одним зі складників рейдерства є «корпоративне рейдерство», яким зазвичай є фінансова установа, що не має досвіду управління виробництвом, орієнтується лише на отримання контролю над захопленим підприємством, для неї захоплене підприємство є громіздким і неефективним активом. Але навіть такі наміри «корпоративного рейдера» не свідчать про його намір здійснення злочинних дій, порушення прав акціонерів, нехтування правилами набуття корпоративного контролю. Недружнє поглинання у форматі «корпоративного рейдерства» насправді становить досить незначну частку рейдерських поглинань.

Слушною є думка переважної більшості українських і зарубіжних авторів, які звертають увагу на факт відсутності наукового та юридичного визначення таких понять, як «рейдер» і «рейдерство».

Недивно, що в науковій літературі з цього питання існує розмаїття думок. Так, в Інтернет-журналі «Юридичний лікбез» М. Макайкін зазначив, що проблематика дослідження поняття «рейдерство» полягає, передусім, у його відносній новизні[3]. Поняття, що використовуються в

---

[1]Лященко М. Загальна характеристика рейдерства в Україні [Електронний ресурс]/Ляшенко М. – Режим доступу : http://www.kspu.edu/FileDownload.ashx?id=776fad03-832a-4a02-9c9d-86404b407b25.

[2] Поняття рейдерства та його суспільна небезпечність // Юридична консультація в інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html.

[3]Макайкин М. Что такое рейдерство? [Электронный ресурс] / Михаил Макайкин // Юридический блог "Юридический ликбез" – Режим доступа : http://www.svem.ru /blog/likbez/639. html.

сучасній вітчизняній літературі з рейдерства, прийшли з інших держав, тому вони ніяк не співвідносяться ані з законодавством нашої держави, ані з реаліями захоплення підприємств.

Через відсутність законодавчо закріпленого тлумачення термін «рейдерство» в українській і російській науковій літературі трактується по-різному. І хоча відмінності у тлумаченнях незначні, вони все ж таки мають місце. Більшість авторів до поняття «рейдерство» включають і захоплення підприємств, і дружні та недружні поглинання, навіть деколи й злиття. Це порушення законів логіки. Подібний підхід відбувається через непрофесіоналізм і породжує величезну кількість суперечностей.

Отже, визначити, що таке «рейдерство» можна виключно на підставі непрямих ознак і за аналогією з тим, що називають «рейдерством» за кордоном. Слід зауважити, що рейдерством в західноєвропейській практиці корпоративних відносин називають як звичайне й абсолютно законне придбання підприємства без згоди фактичного власника і менеджменту, так і силове захоплення з метою зміни власника.

Така думку, дозволяє виділили законне і незаконне рейдерство.

Законне рейдерство або рейдерство у класичному його тлумаченні – це заволодіння майном, бізнесом, що здійснюється цілком законними методами, зокрема, за допомогою скупки (міни, дарування) акцій або часток у статутному фонді підприємства, проведення додаткової емісії акцій, скупки боргів підприємства, що поглинається, для формування конкурсної маси з метою ініціації справи про банкрутство підприємства-мети, реприватизації, сутність якої полягає в судовій відміні приватизації та подальшому перерозподілі власності.

Законне рейдерство ототожнюють з недружнім поглинанням, оскільки воно передбачає заволодіння майном, бізнесом, здійснюване повністю законними методами, наприклад, за допомогою скупки (міни, дарування) акцій або часток у статутному фонді підприємства, проведення додаткової емісії акцій, скупки боргів підприємства, що поглинається, для формування конкурсної маси з метою ініціації справи про банкрутство підприємства-мети.

До законного рейдерства належить і реприватизація, суть якої полягає в судовому скасуванні приватизації та подальшому перерозподілі власності.

На думку деяких експертів, легальне, законне недружнє поглинання в окремих випадках навіть корисне для національної економіки,

оскільки «вибиває» з ринку неефективний менеджмент і власників. Завдяки злиттям і поглинанням слабкі підприємства фактично отримують нове життя. Але законним рейдерство визнається лише за умови використання способів поглинання не заборонених чинним законодавством.

Водночас часто законне за формою, тобто за використовуваними методами, рейдерство є незаконним за суттю – отримання контролю та права подальшого розпорядження майном проти згоди та волі його власника.

Незаконне рейдерство або рейдерство, що сформувалося на пострадянському просторі, – це заволодіння майном і бізнесом за допомогою методів, які суперечать чинному законодавству.

У свою чергу, незаконне рейдерство поділяється на кримінальне й некримінальне, залежно від наявності передбаченого кримінальним законодавством країни складу злочину в діях загарбника[1].

У контексті вищезазначеного досить обґрунтованою є думка українського дослідника Н. Гуторової, яка виділяє два види рейдерства – «біле» і «чорне» – і акцентує увагу на доцільності використання терміна «рейдерство» лише для позначення фактів протиправного захоплення підприємств[2].

З іншого боку, в сучасному цивілізованому світі розповсюджений тільки легальний тип рейдерства. Ця форма рейдерства дозволена, контрольована і врегульована законом. Таким чином, поняття «рейдерство» в західноєвропейському розумінні, як правило, немає негативного значення.

У корпоративному праві США та Західної Європи терміном «рейдер» позначають особу, яка здійснює активну скупку акцій з метою отримання контрольного пакету. При цьому «рейд» розглядають як операцію (спробу) з придбання великого пакета акцій певного підприємства з метою його поглинання[3].

В умовах існуючого «теоретичного вакууму» щодо інституту рейдерства український економіст І.М. Макарчук припускає можливість трактувати поняття «рейдерство» «... за аналогією до того, що розумі-

---

[1]Понятие рейдерства. Факторы // Real Estate Development Group. – Режим доступа: http://www.red-develop.com/ru/informaciya/analitika/115.html.

[2] Гуторова Н. Щодо встановлення кримінальної відповідальності за рейдерство // Юридичний радник.– 2007. – № 2. – С. 6-9.

[3] Поняття рейдерства та його суспільна небезпечність // Юридична консультація в інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html.

ють під «рейдерством» за кордоном»[1]. Погоджуємося з думкою автора, але за певних умов. У цьому випадку мається на увазі відсутність можливості формування універсального поняття «рейдерство» в контексті існування внутрішньодержавних правових особливостей регулювання системи економічних, у тому числі корпоративних, відносин.

Необхідно взяти до уваги й наявність науково-доктринальних відмінностей у визначенні поняття «рейдерство», зумовлених належністю автора до конкретної наукової школи[2].

Кірєєв А.Ю. на рівні дисертаційної роботи, визначає рейдерство як систематичну діяльність на ринку корпоративного контролю, спрямовану на несилове правове та не правове отримання контролю над активами інших суб'єктів економічної діяльності із завданням їм економічних та інших збитків.

Нам видаються примітними й деякі спроби вітчизняних авторів, пов'язані з галузевим розмежуванням рейдерських дій.

Так, представники Національного інституту стратегічних досліджень З. Варналій та І. Мазур визначають рейдерство як «... недружнє, за межами дії цивільного законодавства, спрямоване проти волі власника захоплення чужого майна... »[3].

Подібного погляду дотримуються й інші українські дослідники. Так, на думку Б.М. Грека, «… рейдерство в сучасному розумінні – це недружнє поглинання підприємств і компаній, перерозподіл власності й корпоративних прав.

Іншими словами, рейдерство – це недружнє, поза межами дії цивільного законодавства, спрямоване проти волі власника захоплення чужого майна на користь іншої особи, установлення над майном повного контролю нового власника в юридичному і фізичному розу-

---

[1] Макарчук І.М. Рейдерство, як одна з форм тіньової економіки держави та його наслідки [Електронний рисурс] // Економічний вісник університету. Збірник наукових праць. – 2010. – № 1. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/evu/2010_15_1/Makarch.pdf

[2] Киреев А.Ю. Рейдерство в Российской экономике: сущность, тенденции и возможности противодействия. Автореф. дис. … канд. экон. наук: 08.00.05 / А.Ю. Киреев. – М., 2008. – С. 9.

[3] Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

мінні з використанням корумпованості чиновників та (або) із застосуванням сили»[1].

Розміщення інституту рейдерства виключно за межами правового поля конструктивно критикується з боку деяких авторів. Так, український дослідник М.А. Колесник акцентує увагу на можливості здійснення недружнього захоплення чужого майна, а також установлення над ним повного контролю в межах чинного законодавства[2]. Вважаємо таку критику цілком обґрунтованою.

Інші автори, досліджуючи інститут рейдерства, доходять висновку про можливість його розміщення в незаконній, законній, або так званій «напівзаконній» сферах.

До речі, прибічником такого підходу є російський дослідник Н. Лопашенко, який стверджує, що рейдерство – це методика заволодіння чужою власністю, що ґрунтується на мистецтві менеджменту та корпоративних юристів і становить ретельно сплановану систему діяльності, спрямовану на отримання чужої компанії, що здійснює підприємницьку та (або) інші види економічної діяльності. На думку автора, рейдерство, як правило, «… містить поєднання незаконних, напівзаконних (протиправних, але таких, що не знайшли законодавчої заборони і не прописаних у законі) і законних способів придбання привабливої, але чужої власності»[3].

На окрему увагу заслуговує існуюча в економічній науці думка про подвійну природу рейдерства, згідно з якою рейдерство – це спосіб перерозподілу власності, що, в принципі, є кримінальним, а за формою набуває деяких форм юридичних процедур[4].

Ще більш категоричного погляду про можливість легальних форм рейдерської діяльності дотримуються інші вітчизняні дослідники. Вони зазначають, що «рейдерство» в класичному розумінні становить

---

[1] Грек Б.М., Грек Т.Б. Поняття та історичні передумови розвитку рейдерства в Україні / Б.М. Грек, Т.Б. Грек / Адвокат. – 2010. – № 9. – С. 29.

[2]Колесник М.А. Рейдерство в Україні: Загальна характеристика та основні тенденції розвитку [Електронний ресурс] // Право і безпека. – 2011. – № 1. – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/pib/2011_1/PB-1/PB-1_16.pdf

[3]Лопашенко Н. Рейдерство/ Н. Лопашенко // Законность. - 2007. - № 4. - С. 8.

[4]Рейдерство как социально-экономический и политический феномен современной России. Отчет окачественном социологическом исследовании. Исследование центра политических технологий 20.05.2008 //сайт Компромат.ш [Электронный ресурс]. Режим доступа: http://compromat.ru/main/mixl/raiderycpt.htm.

реалізацію заходів із придбання чужого підприємства, переважно в межах чинного законодавства.

Незважаючи на цю обставину, рейдер утім діє всупереч волі керівництва й акціонерів підприємства – об'єкта рейдерського захоплення.

Така специфіка рейдерської активності зумовлює її віднесення до об'єктивних процесів, що сприяють динаміці економічного росту і побудові конкурентоспроможної економіки[1].

На окрему увагу заслуговує позиція деяких авторів, зокрема С. Симакова, про безпідставність самого віднесення поняття «рейдерство» до наукових, у тому числі економічних та юридичних категорій [2]. Підтримуючи вищезазначену точку зору, І. Головань лише обмежується асоціацією поняття «рейдерство» з «модним» терміном [3].

Такий авторський підхід аргументований відсутністю відповідальності, що передбачена чинним законодавством за здійснення рейдерських дій, а отже, й неприпустимістю нормативно-правової можливості боротьби із зазначеним негативним феноменом дійсності.

Аналіз існуючих поглядів на економіко-правову природу «рейдерства» підтверджує факт переважного застосування широкого підходу до визначення цього поняття.

Так, український правознавець О. Бєліков, використовуючи цей підхід, характеризує рейдерство як послідовний алгоритм операцій, що дозволяє «... за допомогою прогалин у законодавстві отримати у володіння певний капітал (у більшості випадків – підприємство)» [4]. Зауважимо, що реалізація подібної моделі часто супроводжується виведенням активів з володіння законних власників. Такий факт не виключає факт виведення рейдерських атак за межі легітимних суспільних відносин.

---

[1] Поняття рейдерства та його суспільна небезпечність // Юридична консультація в Інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html.

[2] Симаков С. Рейдерство по-украински (краткий очерк) // Юридичний радник. – 2006. – № 6 (14). – С. 23-25.

[3] Головань І. В. Рейдерство – модний термін чи зручна ширма? // Вісник господарського судочинства. – 2008. – № 6. – С. 127.

[4] Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

На підставі аналізу існуючих уявлень про економіко-правову суть рейдерства сформулюємо таке його визначення: рейдерство – це реалізація заходів, спрямованих на заволодіння підприємством (його активами) без згоди власника або шляхом його примусу до згоди, з використанням незаконних або формально законних дій.

При цьому, формально законні дії рейдера порушують правила «ділового обігу» і посягають на основні права і свободи суб'єктів економічної діяльності.

Використання широкого підходу до визначення рейдерства часто призводить до ототожнення рейдерства з такими поняттями, як «недружнє поглинання», «корпоративний шантаж» і «незаконне встановлення контролю над підприємством».

Зауважимо, що в економічній науці близького зарубіжжя також мають місце прецеденти повного ототожнення понять (термінів) «недружнє поглинання», «корпоративний конфлікт», «захват підприємства» та «рейдерство». Непоодинокі й випадки віднесення в пострадянській економічній науці до рейдерства процесів «грінмейлу».

До речі, в одній зі своїх робіт представник російської науки О.А. Полушкін вважає вищезазначені поняття синонімами1. Разом з тим, автор безпосередньо відносить до рейдерства шахрайство, підробку документів, реприватизацію та ініціювання банкротства. Проаналізуємо економіко-правову сутність зазначених понять і визначимо доцільність їх ототожнення.

В основу визначення економіко-правової природи поняття «недружнє поглинання» покладена британська й американська модель організації ринку корпоративного контролю.

Обидві моделі ґрунтуються на визнанні поглинання – дружнього і недружнього – позитивним явищем, що за належного регулювання сприяє швидкому й ефективному перерозподілу виробничих і фінансових ресурсів з мінімальними втратами на користь більш ефективних менеджерів. Механізм поглинання розглядається як один з найпотужніших «двигунів» американської та британської економіки.

Загроза втратити роботу внаслідок недружнього поглинання забезпечує істотну мотивацію для менеджерів підприємства, зумовлює їх працювати чесно та ефективно на користь акціонерів.

---

[1] Полушкин О.А. Рейдерство: пути решения актуальных проблем // Закон и право. – 2008. – № 2. – С. 62.

Незадовільні результати діяльності підприємства, відсутність дивідендів, нехтування інтересами акціонерів веде до того, що таке підприємство стане легкою здобиччю для загарбника, а його акціонери з готовністю продадуть свої акції, натомість менеджерам і директорам доведеться шукати нову роботу [1].

Дружнє поглинання (friendly take-over) є операцією двох юридичних осіб щодо приєднання однієї юридичної особи до іншої. Аналогією дружнього поглинання можна вважати приєднання.

Майже 95 % усіх злиттів і поглинань відбуваються за взаємною згодою сторін. У цьому випадку керівництво підприємства, що поглинається, позитивно ставиться до перспективи поглинання, погоджується не чинити опір поглинанню та рекомендує своїм акціонерам прийняти пропозицію підприємства-агресора, яке поглинає, про продаж йому своїх акцій[2].

Оскільки поглинання, в тому числі і дружнє, неминуче призводить до змін у менеджменті підприємства, то позитивне ставлення керівництва підприємства-мети до перспективи втрати ним своїх повноважень, прав і компетенцій є, радше винятком, ніж правилом.

Процедура поглинання відбувається не лише за взаємною згодою, але й з виникненням конфлікту, наприклад, усупереч бажанню менеджменту, але з відома акціонерів підприємства. Останній випадок отримав назву недружніх (або ворожих) поглинань (hostile take-over)[3].

Недружнє поглинання – це встановлення над підприємством або активом повного контролю як в юридичному, так і у фізичному сенсі всупереч волі менеджменту або власника цього підприємства, або активу[4]..

---

[1]Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

[2]Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

[3]Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

[4]Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень /

З цього визначення можна зробити висновок: недружнє поглинання відбувається проти волі власників або керівництва підприємства, але це не означає, що поглинання відбувається у незаконний спосіб. Тобто недружнє поглинання відрізняється загалом від дружнього опором менеджменту або власників підприємства-мети. Відповідно, у цьому випадку керівництво підприємства-мети налаштовано проти поглинання, намагається зірвати поглинання, зробити його невигідним для поглинача та закликає акціонерів не продавати свої акції підприємству-агресору.

В основі недружніх поглинань завжди лежить конфлікт зацікавлених осіб. Конфлікт, наприклад, може виникати через порушення прав міноритарних акціонерів або, навпаки, через їхній шантаж з метою дорожчого продажу своїх акцій (на Заході називається грінмейлом)[1].

Майнові суперечки, фактичним предметом яких є встановлення контролю над підприємствами шляхом недружнього поглинання, стали звичайною практикою підприємницького життя.

Методи, що використовують ініціатори недружніх поглинань, як правило, відносно законні, але водночас далекі від норм етики і моралі. У хід йдуть і маніпуляція громадською думкою, і лобізм, і біржові махінації, і застосування фізичної сили. Щоправда, і відповідна реакція об'єктів інтересів рейдерів часто також далека від ідеалу.

У деяких випадках мета недружніх (або ворожих) поглинань – продаж активів підприємства та його ліквідація.

Здебільшого на захоплених підприємствах проводиться реструктуризація, що спричиняє зміну менеджменту, продаж непрофільних активів підприємства, реструктуризацію боргів, скорочення витрат та оновлення основних виробничих фондів. Таким чином, контроль над підприємством переходить до ефективного власника.

На думку експертів з проблем кримінальних поглинань Торгівельно-промислової палати Російської Федерації, недружнє поглинання є нормальним ринковим механізмом.

З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

[1]Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

Класичні рейдери сприяють економічному розвитку, відсторонюючи від управління бізнесом неефективний менеджмент, перешкоджаючи зловживанням великих акціонерів і реструктуруючи неефективно працюючі підприємства[2].

До того ж, сьогодні немає чітких критеріїв, за якими те чи інше поглинання підприємства можна вважати протиправним, у тому числі й злочинним.

Способи недружнього поглинання ґрунтуються на використанні чинного законодавства і їхнє використання не передбачає його порушень або квазізаконного удавання до чинних законів (рис. 1.1).

Рис. 1.1. Види поглинання підприємства

Факт поширення під час недружнього захоплення технологій шантажу міноритарних акціонерів задля дорожчого продажу акцій зумовлює виникнення різноманітних алгоритмів корпоративного шантажу.

В економічній літературі під корпоративним шантажем розуміють дії, спрямовані на порушення нормального функціонування акціонерного товариства, що звичайно здійснюються дрібним акціонером з метою досягнення викупу належного йому пакету акцій за ціною, яка значно перевищує ринкову[1].

Деякі автори, зокрема відомий дослідник корпоративних захватів М.Г. Іонцев, безпосередньо відносять корпоративний шантаж до грінмейлу[2]. На думку представників такого теоретичного підходу, сутність будь-якого корпоративного шантажу полягає в тому, щоб шляхом різних формально законних способів змусити придбати пакет акцій, що належить грінмелеру, за завищеною ціною.

У процесі реалізації технології корпоративного шантажу його виконавці (ініціатори) використовують такі прийоми: блокування рішень : акціонер голосує проти або не бере участі в голосуванні, внаслідок чого загальні збори не мають кворуму, або утримується від голосування, беручи участь у зібранні, у результаті чого кількість голосів, необхідних для прийняття рішення, недостатня.

Звертаючи увагу на таку технологію, Н.Д. Бут, І.С. Вікторов, Д.А. Звягінцев та О.С. Опенишев зазначають, що блокування рішень – «… це приклад шантажу, коли рішення, що блокується, є вигідним для такого акціонера, але він звертається з вимогою сплатити його голосування або придбати його пакет акцій за вищою, ніж ринкова, ціною.

Метою діяльності такого акціонера є створення неможливості нормального функціонування акціонерного товариства»[3]; постійні вимоги надавати інформацію, яку, відповідно до чинного законодавства, товариство зобов'язане надавати своїм акціонерам; звернення до суду з позовами по відношенню до акціонерного товариства або великого акціонера.

---

[1]Противодействие недружественным поглощениям: Научно-практическое пособие. – М.: ОЛМА-ПРЕСС, 2006. – С. 121.

[2] Ионцев М.Г. Корпоративные захваты: слияния, поглощения, гринмэйл. — 2-е изд., перераб. и доп. — М.: Ось-89, 2005. – С. 10.

[3] Противодействие недружественным поглощениям: Научно-практическое пособие. – М.: ОЛМА-ПРЕСС, 2006. – С. 121.

Під незаконним встановленням контролю над підприємством, як правило, розуміють суспільно небезпечне, протиправне діяння, пов'язане з незаконним придбанням права володіння, та (або) використання, та (або) розпорядження активами (часткою активів) юридичної особи, або пов'язане з установленням контролю над юридичною особою шляхом незаконного придбання права володіння, та (або) використання, та (або) розпорядження частками учасників юридичної особи в уставному капіталі[1].

У будь-якому випадку незаконне встановлення контролю над підприємством асоціюється з активною діяльністю заподіяння шкоди правам або законним інтересам власників акціонерного товариства, що суперечить їх волевиявленню та загрожує безпеці особистості, суспільства та держави.

Слід вважати, що повне ототожнення рейдерства з різними варіаціями недружнього поглинання досить сумнівне. Контраргументом подібного підходу є англосаксонський підхід до визначення недружнього поглинання. Згідно з останнім, недружнє поглинання - це легітимне встановлення контролю (придбання) над контрольним пакетом акцій підприємства на ринку цінних паперів, його реорганізація або ж продаж. При цьому, зарубіжною теорією зовсім не виключаються активні дії, спрямовані на протидію встановленню зазначеного контролю (проведення реорганізації) з боку топ-менеджменту або акціонерів компанії.

Звертаючи увагу на цю обставину, О.А. Полушкін справедливо зауважує, що загалом, поглинання – це процес, у результаті якого активи компанії переходять у власність покупця, а зовсім не «загарбника»[2].

На феномен ототожнення понять «недружнє поглинання», «корпоративний конфлікт», «захват підприємства», «рейдерство» та «грінмейл» звертають увагу і деякі зарубіжні автори.

Так, К.О. Гуман у своїй дисертації пояснює факт ототожнення зазначених термінів тим, що «… в державах з розвиненою ринковою економікою не існує такого поняття, як рейдерство, а недружні захвати виявляються в зовсім інших формах, з абсолютно іншою специфікою, але російські автори переважно користуються зарубіжною термі-

---

[1] Федоров А.Ю. Рейдерство и корпоративный шантаж (организационно-правовые меры противодействия) : монография / А.Ю. Федоров. – М.: Волтерс Клувер, 2010. – С. 452-453.

[2] Полушкин О.А. Рейдерство: пути решения актуальных проблем // Закон и право. – 2008. – № 2. – С. 62.

нологією, визначають за її допомогою процеси російського рейдерства»[1].

У свою чергу, деякі автори виводять інститут недружнього поглинання з площини легітимних дій суб'єктів корпоративних відносин.

Так, С.Г. Мартинов у своїй дисертації асоціює недружнє поглинання з установленням контролю «... над господарським товариством через нелегітимну зміну органів його управління та / або використання боргових зобов'язань та / або за допомогою придбання прямо або опосередковано активів і цінних паперів товариства всупереч волі інших акціонерів»[2].

Слід вважати, що незаконний характер установлення корпоративного контролю в деяких випадках характерний саме для рейдерства, а не для інституту недружнього поглинання.

Зауважимо, що ряд авторів відносить рейдерство до незаконних дій, які здійснюються з метою заволодіння майном іншого суб'єкта. Такий погляд пропагують українські дослідники П.В. Берназ та О.О. Середа[3].

Визначаючи економіко-правову суть рейдерства, деякі російські економісти (у тому числі на дисертаційному рівні) відзначають його не правовий характер[4].

Таким чином, попри певну схожість економіко-правової природи, «рейдерство» та «недружнє поглинання» - різні поняття. Зважаючи на це, слід погодитися з фахівцями в галузі безпеки, що рейдинг (рейдерство) – це процес, а поглинання – це результат[5].

---

[1]Гуман Е.О. Развитие организационно-экономического механизма защиты предпринимательской структуры от угрозы рейдерства : диссертация ... кандидата экономических наук : 08.00.05 / Гуман Екатерина Олеговна; [Место защиты: Ин-т экономики УрО РАН].- Екатеринбург, 2010.- С. 43.

[2] Мартынов С.Г. Гражданско-правовые механизмы защиты от недружественных поглощений хозяйственных обществ : диссертация ... кандидата юридических наук : 12.00.03 / Мартынов Сергей Геннадьевич; [Место защиты: Российская академия народного хозяйства].- Москва, 2011.- 173 с.

[3]Берназ П.В. Рейдерство в Україні: визначення поняття / П.В. Берназ, О.О. Середа // Проблеми цивільного та господарського права. – 2008. – № 1. – С. 82-84.

[4] А.Ю. Рейдерство в Российской экономике: сущность, тенденции и возможности противодействия. Автореф. дис. … канд. экон. наук: 08.00.05 / А.Ю. Киреев. – М., 2008. – С. 9.

[5]Поняття рейдерства та його суспільна небезпечність [Електронне джерело] // Юридична консультація в інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html.

Доцільно відрізняти «рейдерство» від процесів злиття та поглинань, корпоративних конфліктів і грінмейлу і за іншими критеріями. Так, суттєва відмінність зазначених понять полягає у відмінності їх мети: характерною метою рейдерства є заволодіння підприємством і його майном для отримання негайного прибутку.

В свою чергу мета злиття та поглинань (процеси *M&A*), як правило, полягає в підвищенні конкурентоспроможності, у тому числі на міжнародному рівні, або в симетричній відповіді на дії конкурентів, що укрупнюються.

Не менш специфічна і мета грінмейлу, суть якої зводиться до отримання прибутку від продажу акцій за підвищеними цінами без захвату підприємства.

Не можна також применшувати і суттєву різницю досліджуваних форм бізнес-активності, яка полягає в методах її реалізації. До речі, під час реалізації більшості процесів злиття та поглинань реалізуються методи, що не суперечать сучасним вимогам чинного законодавства.

При цьому в процесі реалізації функцій грінмейлеров, попри відсутність грубих порушень законодавства, все ж таки вчиняються діяння, спрямовані на дестабілізацію роботи підприємства. Задля реалізації цієї мети нерідко очорняється ділова репутація підприємства – об'єкта грінмейлу.

Таким чином, методологія рейдерства, що спирається на використання легальних і протизаконних дій, у тому числі передбачених диспозиціями КУпАП та КК України, більш ніж специфічна.

Отже, з метою більш чіткого розуміння економічної суті рейдерства, процесів злиття та поглинань, корпоративних конфліктів і грінмейлу, їхніх спільних рис і відмінностей, вважаємо за доцільне подати порівняльну характеристику аналізованих понять у табл.1.1.

На думку більшості представників вітчизняної та зарубіжної економічної науки, формування інституту рейдерства пов'язане з недосконалістю ринкових інструментів перерозподілу власності [1231].

---

[1]Тарханова З.Э. Функционирование института рейдерства в РФ: автореферат дис.... кандидата экономических наук: 08.00.01 / Тарханова Зарина Эльбрусовна; [Место защиты: Сев.-Осет. гос. ун-т им. К.Л. Хетагурова]. - С. 9

[2] Варналій З. С., Мазур І. І. Рейдерство в Україні: Передумови та шляхи подолання / З.С. Варналій, І.І. Мазур // Стратегічні пріоритети. – 2007. – № 2 (3). – С. 129-136.

[3] Шемчук В. Рейдерство та корупція / В. Шемчук // Вісник прокуратури. – 2006. – № 11. – С. 14.

Таблиця 1.1.

Порівняння процесів M&A, рейдерства, грінмейлу та корпоративного конфлікту

Ознака	Явища, які порівнюються			
	Процеси M&A	Рейдерство	Грінмейл	Корпоративний конфлікт
Сутність явища	Одна з форм структурної перебудови юридичної особи з метою ефективного розподілу та використання всіх ресурсів підприємства	Дії спрямовані на заволодіння чужим майном, що відбуваються всупереч волі власника; витрачається менше коштів, ніж майно оцінюється за ринковою вартістю, з подальшою легалізацією цього майна	Корпоративний шантаж шляхом скупки значної кількості акцій з пропозицією продати їх за підвищеними цінами	Конфлікт інтересів власників підприємства, є частим приводом для захоплення
Мета	Підвищення конкурентоспроможності, у т.ч. на міжнародному рівні; симетрична відповідь на дії конкурентів, які укрупнюються; відсутність альтернативних джерел підвищення капіталізації	Встановлення контролю над суб'єктом господарської діяльності та його активами; збагачення, але не через господарську діяльність, а шляхом продажу активів та цінного майна	Отримання прибутку від продажу акцій за підвищеними цінами без захоплення підприємства	Різна, залежить від інтересів учасників конфлікту

[1] Федоров А. Ю. Рейдерство и корпоративный шантаж: монография. – М.: Волтерс Клувер, 2010. –480с.

Продовження табл. 1.1

Ознака	Явища, які порівнюються			
	Процеси M&A	Рейдерство	Грінмейл	Корпоративний конфлікт
Методи досягнення мети	Як правило, не суперечать законодавству	Поряд із законними використовуються й протиправні, що підпадають під статті КУпАП та КК України	Грубих порушень законодав-ства не допускається, але вичиняються діяння, спрямовані на дестабілізацію роботи підприємства, очорняється його ділова репутація	Якщо конфлікт не створений для рейдерського захоплення, методи, як правило, правові
Очікувані наслідки	Утворення нового підприємства або встановлення контролю над суб'єктом господарської діяльності	Установлення контролю над суб'єктом господарської діяльності	Отримання великих відступних та вигідний продаж акцій	Різні для кожного з учасників

Наведені відмінності процесів, що аналізуються, можна використовувати в практичній діяльності.

1.2. Передумови та особливості розвитку рейдерства в Україні

Аналіз проблеми виникнення та розвитку рейдерства дозволив дійти висновку, що рейдерство не є виключно українським феноменом в сучасних умовах. Однак інституалізація рейдерської активності в Україні має свої специфічні відмінності, пов'язані з передумовами виник-

нення й особливостями подальшого розвитку цього негативного феномену сучасного господарювання.

Пострадянські реформи, основною метою яких було формування ринкових відносин та інституту приватної власності, на жаль, спричинили зовсім не ті результати, що очікувалися. Період ослаблення державного контролю ознаменувався відторгненням адміністративних і моральних обмежень, розквітом корупції та тіньової економіки.

На фоні цих негативних тенденцій значно посилених проголошенням приватної та приватизацією державної власності, виник новий тип підприємців, які сформували згодом не тільки певний тип соціально-економічної поведінки, а й менталітет бізнес-спільноти та ділову етику країни загалом.

Досліджуючи зазначені економічні формації, Л.О. Скиданова у своїй дисертації обґрунтовано доходить висновку, що певна частина підприємців, які брали участь у безпосередньому перерозподілі державної власності, сформувала в подальшому новий вид підприємництва – рейдерство і новий тип підприємців – рейдерів[1].

Погоджуючись з подібним твердженням, необхідно акцентувати увагу на тому, що набувши форми «силового підприємництва», сучасна рейдерська діяльність трансформувалася в модель соціально-економічної поведінки щодо незаконного перерозподілу власності, а в деяких випадках і в окрему, досить резонансну форму протиправної діяльності.

За умови подальшого розвитку зазначеного сценарію перерозподілу власності приватна власність у подальшому все частіше буде розглядатися як гіпотетичний об'єкт зазіхань з боку агресора. Критикуючи подібні тенденції, дослідники справедливо зазначають: «… «привабливі» підприємства змушені перебувати в постійному страху бути захопленими, що формує не тільки новий вид підприємницького ризику, але і спотворений менталітет бізнес-співтовариства. Власність, що розглядається суспільством як приватна, є лише квазіприватною, тобто може бути експропрійована в будь-який момент»[2].

---

[1] Скиданова Л.А.Рейдерство как социально-экономический феномен: автореферат диссертации на соискание ученой степени кандидата социологических наук: специальность 22.00.03 «Экономическая социология и демография» / Скиданова Лилия Алексеевна; [Моск. гос. ун-т им. М. В. Ломоносова]. - Москва: 2010. - С. 3.

[2] Скиданова Л.А.Рейдерство как социально-экономический феномен: автореферат диссертации на соискание ученой степени кандидата социологических наук: специальность 22.00.03 «Экономическая социология и демография» / Скиданова Лилия Алексеевна; [Моск. гос. ун-т им. М. В. Ломоносова]. - Москва: 2010. - С. 4-5.

Між тим, слід погодитися з поширеною серед науковців і практиків думкою, що поведінка суб'єктів господарювання формується виходячи з двох основних передумов, а саме: економічна свідомість, яка визначає альтернативу, що мінімізує витрати та максимізує результат; норми, правила, соціальні стереотипи, або іншими словами, інститути.

Ураховуючи вищезазначену парадигму поведінки учасника економічних відносин, К.О. Гуман однією з передумов існування рейдерської поведінки виділяє економічну свідомість, тобто вибір найбільш вигідних економічних альтернатив. Саме тому, на думку дослідника, « … однією з основних попередніх умов для появи рейдерства є висока прибутковість цієї діяльності»[1]. Обґрунтовуючи таку точку зору, наводять твердження, що в сучасних умовах поширення силових захоплень підприємства, його вартість – це витрати на рейдерське захоплення підприємства, які, як показує практика, нижче, ніж витрати на легальну процедуру придбання такого підприємства.

Погоджуючись з наведеним ствердженням, зазначимо, що в умовах українських бізнес-реалій прибутковість здійснення рейдерських «атак», як правило, становить від 300 до 2000 %. Інша форма передумов поведінки суб'єктів господарювання, у тому пов'язаної зі здійсненням рейдерських дій, набуває форми норм, правил, стереотипів, або іншими словами, інститутів.

Етимологія слова «інститут» має латинське походження (лат. *institutum* – встановлення, звичай, установа). Одне з перших визначень поняття «інститут» належить американському економісту, засновнику інституційного напряму політичної економії Торстейну Бунде Веблену. Згідно з його визначенням, «інститут» – це «стійкі звички мислення, характерні для більшої спільноти людей»[2]. Характерно, що Т. Веблен досліджував походження інститутів передусім з погляду інстинктів, звичок, традицій і соціальних норм. Дещо схожого думки щодо визначення поняття «інститут» дотримується Джеффри Ходжсон – засновник Європейської асоціації еволюційної політичної економії. Відомий економіст зазначає, що інститут становить «соціа-

[1]Гуман Е.О. Развитие организационно-экономического механизма защиты предпринимательской структуры от угрозы рейдерства : диссертация ... кандидата экономических наук : 08.00.05 / Гуман Екатерина Олеговна; [Место защиты: Ин-т экономики УрО РАН].- Екатеринбург, 2010.- С. 46-47.

[2] Веблен Т. Теория праздного класса. М.: Прогресс, 1984. – С. 201.

льну організацію, яка за допомогою звички, традиції або правових обмежень формує довгострокові рутинізовані схеми поведінки»[1].

Лауреат Нобелівської премії з економіки 1993 року, американський економіст Дуглас Сесіл Норта так трактує поняття «інститут» – це «правила гри в суспільстві або, точніше, придумані людьми обмеження, що спрямовують людську взаємодію в певне русло»[2]. На думку С. Дугласа, «…інститути містять як формальні правила і неформальні обмеження (загальновизнані норми поведінки, досягнуті угоди, внутрішні обмеження діяльності), так і певні характеристики примусу до виконання тих та інших»[3].

Зазначені погляди і трактування сформували сучасне уявлення категорії «інститут». Так, Сучасний економічний словник подає таке визначення: «інститут – це сукупність стійких формальних і неформальних правил, норм, звичаїв взаємозв'язку, взаємодії між людьми, організаціями, державними органами, що мають місце в економіці та суспільстві»[4].

Отже, для економічної теорії характерне виокремлення формальних і неформальних інститутів. До формальних інститутів здебільшого належать юридичні приписи, що містяться в нормативно-правових актах. На думку Д. Норта, це правила, «придумані людьми»[5].

У свою чергу, неформальні інститути – це загальноприйняті умовності й кодекси поведінки, або іншими словами, ті, що зафіксовані в нормах моралі, звичаях, традиціях, табу тощо.

На підставі аналізу поглядів на економіко-правову природу інституту можна дійти висновку, що рейдерська поведінка зумовлена стійким поєднанням соціально-економічних інститутів та існує за рахунок руйнування основоположного базисного суспільного інституту – приватної власності. Таким чином, суспільний розвиток піддається критично небезпечним ризикам, що ставлять під сумнів існування не

---

[1] ХоджсонДж. Экономическая теория и институты. – М.: Дело, 2003. – С. 37.

[2] НортД. Інституції, інституційна зміна та функціонування економіки. – К.: Основи, 2000.- С. 11.

[3] НортД. Институциональные изменения: рамки анализа // Вопросыэкономики. - № 3 - С. 7.

[4] Современный экономический словарь [Электронный ресурс] Режим доступа: http://slovari.yandex.ru/dict/economic/article/sesl/ses-2317.htm

[5] НортД. Інституції, інституційна зміна та функціонування економіки. – К.: Основи, 2000.- С. 34.

тільки підприємницької «нормативно-позитивної» активності за соціально орієнтованим сценарієм, призводять до зростання і розвитку економіки, але й деструктивно впливають на історичні перспективи країни[1].

Аналіз економічної літератури свідчить про відсутність загальноприйнятого підходу до системного визначення ретроспективи рейдерської діяльності в Україні.

Водночас найбільш прийнятною та обґрунтованою, на наш погляд, є систематизація передумов розвитку рейдерства в Україні, що запропонована відомим українським економістом З.С. Варналієм. Учений виділяє такі основні причини поширення рейдерства в Україні: слабкість правової системи та судової влади; корумпованість органів влади; відсутність державних інститутів, що ефективно захищали б права власника; низький рівень правової культури; правовий нігілізм – як у суб'єктів господарювання, так і в представників органів влади; сумнівна передісторія приватизації певних об'єктів тощо[2].

Проте це не єдина спроба вітчизняного осмислення детермінації рейдерства в Україні.

Так, деякі автори звертають увагу не тільки на зовнішні, але й на внутрішньогосподарські передумови поширення рейдерства в Україні. Наприклад, І. Паславський аналізуючи причини виникнення рейдерства звертає увагу на «… велику кількість помилок і порушень в управлінні підприємствами, тобто наявність значного резерву формальних приводів для рейдерських атак»[3].

Проблемі визначення причин поширення рейдерства присвячені роботи представників економічної науки близького зарубіжжя. Наприклад, З.Є. Тарханова виокремлює такі передумови розвитку рейдерства: нечітка, непрозора система реєстрації прав власності; високий рівень чиновницької корумпованості; високий ступінь недосконалості ринку корпоративного контролю на фоні зростання його сумарних значень у ВВП; недооцінка активів середніх і малих ВАТ, чиї акції не є інструментом ринку корпоративного контролю, що призводить до зростання

---

[1]Гуман Е.О. Развитие организационно-экономического механизма защиты предпринимательской структуры от угрозы рейдерства : диссертация ... кандидата экономических наук : 08.00.05 / Гуман Екатерина Олеговна; [Место защиты: Ин-т экономики УрО РАН].- Екатеринбург, 2010.- С. 454-55.

[2] Варналій З. С., Мазур І. І. Рейдерство в Україні: Передумови та шляхи подолання // Стратегічні пріоритети. – 2007. – № 2 (3). – С. 129-136.

[3]Паславський І. Основні етапи протидії українському бізнесу. Роль і позиції ЗМІ / І. Паславський // Вісник Львівського університету. – 2011. – Вип.34. – С. 163-164.

конкуренції при оцінці альтернатив та рівня витрат угод активів в секторі середніх і малих ВАТ [1].

Таким чином, до основних передумов розвитку рейдерства в Україні слід віднести: низький рівень правової культури та правовий нігілізм на всіх рівнях: серед суб'єктів господарювання, представників органів влади та в суспільстві загалом; низький рівень ступеня відкритості суспільства і економіки; високий рівень корумпованості правоохоронних, судових і дозвільних структур; недосконаліть ринкових інструментів перерозподілу власності та велика кількість управлінських внутрішньогосподарських помилок («резерв формальних приводів рейдерства»);відсутність регулярної ринкової оцінки ліквідних активів підприємств; ефемерність української моделі фондового ринку, а отже, і відсутність чіткої реалізації вільного обігу акцій; нечітка і непрозора система реєстрації прав власності; низька інформаційна транспарентність підприємств; зростання корпоративних конфліктів, пов'язаних з недосконалістю законодавства у сфері корпоративних відносин; недосконаліть правової системи й відсутність державних інституцій ефективного захисту прав власності в Україні.

Заслуговують на увагу і деякі спроби ретроспективної систематизації розвитку рейдерства в Україні. Так, у своєму дослідженні, присвяченому визначенню історичних передумов розвитку рейдерства в Україні, Б.М. Грек і Т.Б. Грек, погоджуючись з класифікацією З.С. Варналія, умовно поділяють історію вітчизняного рейдерства на два періоди. Перший період - від початку 1990-х рр. до початку 2000-х – роки проголошення незалежності України, переходу економіки до ринкових відносин, визначення політичних центрів на фоні створення злочинних угрупувань. Другий період – початок 2000-х рр. і до сьогодні – характеризується напівзаконним загарбанням підприємств, більш легальними методами боротьби, активним протистоянням рейдерству[2].

Інші дослідники виокремлюють три основні етапи рейдерського «перерозподілу», зумовлені перехідними трансформаційними процесами інституційної динаміки приватної власності: перший етап – силовий «кримінальний» або «бандитський» перерозподіл власності, що

---

[1]Тарханова З.Э. Функционирование института рейдерства в РФ: автореферат дис.... кандидата экономических наук: 08.00.01 / Тарханова Зарина Эльбрусовна; [Место защиты: Сев.-Осет. гос. ун-т им. К.Л. Хетагурова]. - С. 9

[2] Грек Б.М., Грек Т.Б. Поняття та історичні передумови розвитку рейдерства в Україні / Б.М. Грек, Т.Б. Грек / Адвокат. – 2010. – № 9. – С. 29-30.

мав місце на початку 1990 років; другий етап – «олігархічний» переділ власності − середина 1990-х - 2002 рр.;третій етап класичного «рейдерського» перерозподілу власності (активізувався з 2002-2005 рр.)[1].

Лише частково погоджуємося із зазначеними вище спробами періодизації рейдерства. Вважаємо, що історія вітчизняної моделі рейдерської діяльності має такі етапи свого розвитку:

- *перший етап – стадія зародження рейдерства*: кінець 1980-х –початок 1990-х років - «бандитський» перерозподіл позитивного фінансового потоку у формі рекету (від англ. *rack* – мучити, катувати) – «… примусового стягування з підприємця постійної плати за послуги з охорони (іноді дійсно наданої)»[2].

На думку деяких дослідників, зазначений період є класичним марксистським періодом початкового («дикого») нагромадження капіталу, здійснюваного відкрито кримінальним способом, досить часто із застосуванням фізичного насильства [3][4]. В Україну рейдерство прийшло на початку 1990-х років, в епоху дикого нагромадження первинного капіталу. Як наслідок, крім типового кримінального «чорного», з'явився поділ рейдерства на «біле» і «сіре». Прагнучі захопити ласий шматок, «білі» рейдери йдуть на майже фантастичні, але цілком законні кроки, аби підірвати економічне становище підприємства і потім за безцінь заволодіти ним. «Сірі» використовують сумнівні методи, балансуючи між криміналом і законністю[5].

- *другий етап*: початок 1992 – 1996 роки – рейдерські захоплення майнових комплексів державних підприємств під егідою проголошеного курсу державної приватизації;

- *третій етап*: 1996 - середина 2000-х рр. – епоха резонансних банкрутств з їх подальшим оскарженням і застосування «методик» доведення до банкрутства з метою наступного викупу дочірньої інфраструктури підприємства (земельні ділянки, будинки, споруди).

---

[1] Тарханова З.Э. Функционирование института рейдерства в РФ: автореферат дис.... кандидата экономических наук: 08.00.01 / Тарханова Зарина Эльбрусовна; [Место защиты: Сев.-Осет. гос. ун-т им. К.Л. Хетагурова]. - С. 10.

[2] Дорошук А.А., Трибуха М.В. Система регулювання рейдерства в Україні / А.А. Дорошук, М.В. Трибуха // Економіка: реалії часу. – 2011. – № 1. – С. 171.

[3] Паславський І. Основні етапи протидії українському бізнесу. Роль і позиції ЗМІ / І. Паславський // Вісник Львівського університету. – 2011. – Вип.34. – С. 159.

[4] Рейдерство в Україні: загрози ташляхи протидії. — К., 2010. − С. 6.

[5] Грек Б.М., Грек Т.Б. Поняття та історичні передумови розвитку рейдерства в Україні / Б.М. Грек, Т.Б. Грек / Адвокат. – 2010. – № 9. – С. 29.

Починаючи з 2004 років, з'являються прецеденти зміни власника приватизованих підприємств задля подальшого захоплення майнових комплексів приватизованих об'єктів;

- *четвертий етап – стадія розквіту рейдерства*: 2004 – 2009 рр. – розповсюдження технологій злиття та поглинань у галузі чинного приватного (раніше приватизованого) бізнесу та поширення негативних наслідків глобальної фінансової кризи.

Початок глобальної фінансової кризи та банкрутство майже 20% малих підприємств на фоні «… сумнозвісної тендеризації у виразно лобістській її редакції»[1]. Характерною рисою зазначеного періоду стало послаблення підприємств, пов'язане з девальвацією національної валюти, та майже сто відсоткове блокування отримання кредитних ресурсів з подальшим поглинанням таких підприємств більш великими конкурентами.

У більшості випадків рейдерські атаки супроводжувалися конфронтацією з колишніми власниками. Для здійснення впливу на опонентів рейдери все частіше залучали сторонніх осіб: колишніх партнерів, кредиторів, представників державних регулюючих органів та інших учасників. Самі рейдери стали займати позицію зовнішніх гравців-координаторів, керуючих проектами шляхом спрямування необхідних директив особам, які діють в їх інтересах. Відбулося значне розширення числа учасників рейдерських проектів;

- *п'ятий етап – нова хвиля перерозподілу власності під час корінних політичних змін і пошуків новітніх напрямів і форм рейдерських атак:* 2010 рік – до сьогодні.

Якщо рейдерство в його класичному тлумаченні можна ототожнювати з недружнім поглинанням, то українське рейдерство не асоціюється з таким явищем ринку корпоративного контролю. Вкладання в іноземні терміни невластивого їм значення, використання цих термінів для характеристики українського рейдерства призводить до того, що в суспільному уявленні закріплюється спотворене, негативне ставлення до корпоративних поглинань.

Негативний підтекст поняття «поглинання» у зарубіжній практиці зумовлений асоціюванням з його наслідками – зі зміною менеджменту, технологічною модернізацією, змінами стратегій виробництва, зі значним скороченням працівників; натомість негативний підтекст поняття

[1] Паславський І. Основні етапи протидії українському бізнесу. Роль і позиції ЗМІ / І. Паславський // Вісник Львівського університету. – 2011. – Вип.34. – С. 162.

«рейдерство» у класичному розумінні зумовлений його наслідками – наступною ліквідацією єдиного виробничого комплексу і швидким розпродажем активів захопленого підприємства, часто – частками.

Орієнтація на швидкий перепродаж активів захопленого підприємства є тією характерною ознакою, що об'єднує «корпоративне рейдерство», яке спостерігається у США, з українським рейдерством в Україні та Росії. Єдиною відмінністю є те, що швидкість перепродажу активів різна. Легальність отримання контролю над захопленим підприємством за результатами «корпоративного рейдерства» дає змогу новому власнику не поспішати із продажем активів і тому отримати за них відповідну ціну, для чого новий власник прагне мінімізувати шкоду, що може бути завдана отриманим активам. В Україні ж рейдер здебільшого намагається найшвидше позбутися захоплених активів, продати їх за будь-яку ціну, яка хоч і ненабагато, але перевищує витрати на рейдерське захоплення. Стан активів, що продаються, рейдера майже не хвилює. Саме протиправність дій, порушення закону та прав власників, руйнування захоплених активів є найхарактернішими ознаками рейдерства в Україні.

Велике значення силового складника в рейдерстві (самоуправство, нанесення тілесних ушкоджень, перешкоджання законній господарській діяльності, захоплення державних або громадських будівель чи споруд, умисне знищення чи пошкодження чужого майна) призводить до того, що його часом зводять саме до силового захоплення під прикриттям законних або псевдозаконних підстав. Однак силове захоплення – це лише один з формальних засобів досягнення рейдером своєї мети. Більш витонченим способом є захоплення акцій підприємств шляхом судових рішень, зміни керівників, здійснення захоплення з середини [1]. За незаконним захопленням акцій підприємства, дестабілізацією його положення на ринку або відбувається перепродаж його активів частинами чи цілком, або підприємство включається в бізнес-структуру рейдера.

Рейдерством в Росії та Україні, де воно набуло найбільшого масштабу, спочатку почали називати кримінальне захоплення підприємств. На відміну від тієї ж рейдерської атаки, кримінальне захоплення підприємства є відбиранням чужої власності з порушенням законів

[1] Мухина А. Блеф, замешанный на коррупции (17 апреля 2008 года, г. Саратов) / А. Мухина // "Газета "Богатей". – 2008. – № 15 (440). – Электронный ресурс: Режим доступа: http://www. bogatej.ru/bogatej/print.php?fr=440&article=22042008120838&art_id=0.

держави. В Україні (як і в більшості пострадянських країн) злиття та поглинання підприємств часто відбувалося та відбувається не для оптимізації їхньої економічної діяльності, а радше з метою привласнення чужого майна, тобто рейдерство у класичному розумінні відбувається рідко.

У попередньому параграфі акцентувалася увага на поширеній в західноєвропейських країнах практиці здійснення рейдерства в рамках чинного законодавства. Попри цю обставину, здійснювані в Україні рейдерські захвати найчастіше тісно взаємопов'язані і (взаємодоповнювальні) з таким негативним протиправним явищем сучасності, як корупція. Це визначає одну з особливостей розвитку рейдерства в Україні.

Звертаючи увагу на цю особливість, Б.М. Грек зазначає: « … вважається, що рейдерство … – широко поширена як у світі, так і в Україні система поглинання підприємства шляхом захоплення, насильницького злиття, скуповування акцій через підставну структуру, методом винесення спірного судового рішення з подальшим силовим захопленням підприємства. Опосередкованими учасниками рейдерства, часто не з власної ініціативи, стають суди і силові структури»[1].

Зазначимо, що подібна практика «проекції» рейдерських дій на протиправну площину властива і для держав ближнього зарубіжжя. Так, звертаючи увагу на цю обставину, білоруський дослідник В.В. Пильський резонно зауважує: «Рейдерство і корупція – явища взаємопов'язані, оскільки останнє забезпечує реалізацію головних умов успіху рейдерської діяльності, якими є інформація, «швидкість і максимальна кількість дій, що підлягають легалізації»[2].

Подібні тривожні тенденції характерні і для російського бізнесу. Російський дослідник М.І. Фаєнсон зауважує, що незважаючи на рейдерську активність, яка повинна в кінцевому підсумку опинитися в правовому полі, «... дії рейдерів ніколи не бувають прозорими і … завжди конфіденційні. Інформаційно-правова атака планується рейдерами за каскадним методом («інформаційний», «міліцейський», «прокурорський», «податковий», «реєстраційний» та інші «каскади»), створюючи обтяження відразу за кількома напрямами. Така атака

---

[1] Грек Б.М., Грек Т.Б. Поняття та історичні передумови розвитку рейдерства в Україні / Б.М. Грек, Т.Б. Грек / Адвокат. – 2010. – № 9. – С. 30-31.

[2] Пыльский В.В. Рейдерство: место и значение коррупции / В.В. Пыльский / Наука-2010 : сб. науч. ст. В 2 ч. Ч. 1 / ГрГУ им. Я. Купалы ; редкол.: А.Ф. Проневич (отв. ред.) [и др.]. – Гродно : ГрГУ, 2010. –С. 117-119.

схожа на комп'ютерний спам, коли система інформаційної безпеки вже не справляється з потоками атак і дає пробій»[1].

Аналіз вітчизняної практики рейдерства у зв'язку з використанням корупційних схем свідчить, що найчастіше до цієї сфери протиправної активності залучаються з ініціативи обох сторін корпоративного конфлікту (рейдера і власників об'єкта захоплення) різноманітні силові структури. До числа останніх можуть належати правоохоронні органи (МВС, СБУ, прокуратура), податкові органи, органи судової влади, органи у сфері дозвільної діяльності, органи державного управління з природних ресурсів і охорони навколишнього середовища, органи й установи, що здійснюють державний санітарний нагляд, органи державного управління охороною праці, фонди соціального захисту населення, органи нотаріальної юрисдикції.

Таким чином, специфіка розвитку рейдерства в Україні характеризується систематичним залученням до цих форм корпоративного конфлікту чотирьох основних категорій державних органів, а саме: правоохоронних, судових, моніторингових і дозвільних.

Корупційне пособництво рейдерським захопленням переважно зводиться до реалізації таких функцій в інтересах рейдерів: збір інформації про компанію-мету; тиск на власників, топ-менеджерів компанії-мети; легалізація дій рейдера; маніпуляції з доказової базою (втрата, псування, легалізація); моніторинг дій власника; забезпечення перехоплення управління без кримінальних ризиків для рейдера; блокування дій власника з перехоплення контролю і розпорядження юридичною особою активами; затягування, покривання незаконних дій рейдера; прискорення дій, пов'язаних з профільною діяльністю державного органу.

При цьому дії корупціонерів в інтересах компанії-об'єкта рейдерського захоплення можуть зводитися до такого: прискорення отримання необхідних документів для вчинення розпорядчих дій з нерухомістю; легалізація раніше скоєних дій власника, менеджменту; приховування наявних фактів податкових, фінансово-облікових та інших правопорушень; перешкоджання вчиненню виконавчого провадження.

На думку деяких авторів, у тому числі представників ближнього

[1] Фаенсон, М.И. Рейдерство (недружественный захват предприятий): практика современной России / М.И. Фаенсон, А.А. Пиманова. – М.: Издательство «Альфа-Пресс», 2007. – С. 10.

зарубіжжя[1], основними групами корупційних послуг, що надаються на всіх стадіях рейдерської атаки є: в інтересах рейдера – збір інформації, тиск на компанію-ціль, покривання та легалізація незаконних дій рейдера, реєстрація переходу прав на об'єкт захоплення; в інтересах компанії-жертви – блокування дій рейдера, тиск на загарбника, відновлення прав.

Аналіз найбільш поширених форм рейдерських дій, деталізації яких буде присвячено наступний розділ, свідчить про стрімке розширення учасників цього процесу. Так, разом з основними учасниками в процесі рейдерства все частіше беруть участь приватні охоронні підприємства, злочинні співтовариства і спеціально сформовані для захоплення агресивні групи, професійні консультанти цього сегменту бізнес-активності, компанії, що спеціалізуються тільки на організації та здійсненні рейдерських захоплень, засоби масової інформації. Подібна практика залучення до рейдерських процесів широкого кола учасників характерна для всього постсоціалістичного простору, у тому числі й для РФ [2].

Дослідники в галузі економіки акцентують увагу на тривожних аспектах виходу української моделі рейдерства за будь-які межі. Так, В. Мамутов звертає увагу на «шокуючі» факти нормативно-правового лобіювання інтересів рейдерів. На його переконливу думку, у вищих ешелонах законодавчої влади створюється законодавство сформоване для полегшення рейдерських схем привласнення чужого майна. Вчений безпосередньо підкреслює факт «переходу рейдерства зі стадії захоплення окремих об'єктів у стадію захоплення всього правового поля у сфері економіки»[3].

Не менш специфічна й характерна для української моделі рейдерської діяльності яскраво виражена асинхронність рейдерських хвиль захоплення між центром і регіонами, різними мотивами рейдерства: у центрі – інвестиційного, а в регіонах – ліквідаційного рейдерства. Хвилі рейдерських атак з центру переходять в регіони з певним запізнен-

---

[1] Пыльский В.В. Рейдерство: место и значение коррупции / В.В. Пыльский / Наука-2010 : сб. науч. ст. В 2 ч. Ч. 1 / ГрГУ им. Я. Купалы ; редкол.: А.Ф. Проневич (отв. ред.) [и др.]. – Гродно : ГрГУ, 2010. –С. 118.

[2] Гуман Е.О. Развитие организационно-экономического механизма защиты предпринимательской структуры от угрозы рейдерства : диссертация ... кандидата экономических наук : 08.00.05 / Гуман Екатерина Олеговна; [Место защиты: Ин-т экономики УрО РАН].- Екатеринбург, 2010.- С. 42.

[3] Мамутов В. Рейдерство в законі / В. Мамутов // Дзеркало тижня. – 2008. – № 38.

ням і диверсифікованою технологією захоплень підприємств, готуючи підґрунтя для входу на регіональний ринок більших гравців.

Проблема дослідження особливостей розвитку рейдерства становить значний інтерес і для науковців близького зарубіжжя. Так, представник російській науки С. Анісімов виділяє кілька груп особливостей рейдерства. На думку автора, перша група особливостей зумовлена відмінностями причин цих процесів. Істотний вплив таких чинників, як постприватизаційний перерозподіл власності, експансія і реорганізація великих груп, фінансові кризи.

Друга група, на думку автора, зумовлена специфікою пострадянського фондового ринку, який ще спочатку розвивався як ринок корпоративного контролю, і для якого характерні зниження обсягу операцій, що формують портфельні інвестиції, і збільшення масштабів викупу акцій з метою перерозподілу власності.

Третя група особливостей пов'язана з такою специфікою структури власності російських компаній, як: незначна роль міноритарних акціонерів; вплив особистої мотивації керівництва; непрозора структура власності компаній; поширення форм неформального контролю; поширеність прецедентів поглинань через банкрутство та боргові схеми; поширеність адміністративно-силових і судових методів захисту[1].

Вважаємо, що зазначені вище особливості розвитку рейдерської діяльності певною мірою характерні і для української практики ворожих поглинань.

Проведений аналіз економіко-правої сутності вітчизняної моделі рейдерських атак дозволяє деяким авторам виокремлювати й такі їх особливості: нерозбірливість компаній-агресорів у виборі способів нападу; наявність компаній, що спеціалізуються в галузі недружніх злиттів і поглинань; неможливість розмежувати корпоративний шантаж (міноритарія, що захищає свої права) та недружнє поглинання з боку компанії-агресора[2].

Залежно від сегмента ринку, де діє підприємство-мета та підприємство – агресор, виділяють такі види рейдерства, що зумовлюють його вітчизняну специфіку.

---

[1] Анисимов С. Рейдерство в России. Особенности национального захвата. СПб.: Невский проспект, «Вектор», 2007. –С.51-54.

[2]Котляр Э. Гринмейл: русская версия [Електронне джерело]// Журнал «Консультант». −2005.−№ 5. − Режим доступу: http://www.cfin.ru/investor/ao/prevent_ greenmail.shtml?printversion.

Горизонтальне, мета якого – створення інтегрованої структури підприємств зі схожими видами діяльності, що забезпечує економію за рахунок ефекту масштабу та синергії. Зазвичай такі поглинання відбуваються між підприємствами, що працюють в одному сегменті ринку (в одній галузі) та спеціалізуються на виробництві подібної продукції або наданні подібних послуг.

Метою рейдера є горизонтальне поглинання – збільшення сегменту ринку, а отже, ступеня концентрації в галузі і, як наслідок, витіснення з ринку конкурентів[1].

Горизонтальні поглинання бувають двох видів:

а) поглинання, що розширюють географію ринку збуту підприємства-агресора, проводяться за допомогою придбання підприємства-мети, яке виробляє ідентичну з підприємством-метою продукцію, але працює на інших географічних сегментах ринку;

б) поглинання, що розширюють асортимент підприємства-агресора, проводяться за допомогою придбання підприємства-мети, яке виробляє подібну, але неабсолютно ідентичну продукцію.

Вертикальне, мета якого - створення інтегрованої структури підприємств з різними рівнями технологічних переділів, що зменшує трансакційні витрати [2]. Обмежує цей вид рейдерства вимога стійкості технологічних зв'язків і ймовірність економічної невигідності інтегрування. Також технологічні зміни можуть зробити якусь ланку інтегрованої структури непотрібною або менш ефективною, ніж передбачалося. Прикладом вертикальних поглинань є захоплення сталеливарною компанією підприємства з видобутку залізної руди, вугілля, або нафтовидобувною компанією нафтопереробного підприємства.

Споріднене (або концентричне), що зазвичай визначають як захоплення підприємств «подібних за природою та діями». Під час цих захоплень підприємство-агресор і підприємство-мета пов'язані між собою базовою технологією, виробничим процесом або через ринкову нішу [3];

---

[1]Криничанский К. В. Рынок слияний и поглощений как среда реализации функции стимулирования предпринимателей и менеджеров / К. В. Криничанский // Менеджмент в России и за рубежом. – 2007. – № 3. – С. 115 – 118.

[2]Борисов Ю. Корпоративное рейдерство как социально-экономическое явление в мировой экономике : аналитический доклад. – М. : Первый институт корпоративного права, 2007. – С. 6.

[3]Лазуренко В. И. Рейдерство : слияния и поглощения : монография / В. И. Лазуренко, Я. Н. Лоиакин, Ю. В. Лазуренко. – М. : ТУКБИ, 2009. − С. 41.

родинні (або концентричні) поглинання значно підвищують рівень монополізації відповідного сектору ринку та стримують його розвиток.

Конгломеративне, за якого захоплюється підприємство, що ніяк не стикається з діяльністю підприємства-агресора як на сегменті ринку, так і у виробничо-постачальницьких зв'язках. Конгломерат є об'єднанням технологічно непов'язаних виробництв, для якого характерні частий продаж і покупка активів різного виду. Зазвичай підприємство-агресор переслідує мету диверсифікації своєї діяльності [1].

У літературі, що висвітлює проблему рейдерства в Україні, описано чимало випадків захоплення підприємств, бездіяльності влади та прокуратури, несправедливих ухвал суддів і схем рейдерського захоплення. Але на противагу швидкому поширенню рейдерства виникло та зміцніло явище антирейда – професіональної протидії рейдерству.

Як правило, антирейд містить комплекс заходів з повернення колишньому власникові втрачених прав на управління підприємством. Цей комплекс не може бути універсальним, а його складники часто незначною мірою відрізняються від заходів, вжитих самими рейдерами для захоплення. Здійснюють антирейд, як правило, певні організації.

Антирейд є двоїстим явищем: з одного боку, його суб'єкти можуть допомогти повернути власність, а з іншого − антирейд є прихованим способом сприяння рейдерству, закріпленню його результатів. Рейдери доволі майстерно використовують антирейд як спосіб отримання інформації про підприємство, про лінію його захисту, яку підприємство, що захищається, на умовах конфіденційності надає антирейдеру для того, щоб завести судові процеси в глухий кут. Наприкінці судової процедури антирейдер, насправді пов'язаний з рейдером, а то і створений ним, для пояснення програшу посилається на недосконаліть законів, корумпованість влади, судейської системи тощо. І такі пояснення антирейдера є доволі переконливими, адже несправедливість судових рішень і їхнє невиконання набули тотального масштабу.

Завершаючи дослідження передумов та особливостей розвитку рейдерської діяльності, вважаємо за доцільне акцентувати увагу на певному парадоксі, влучно визначеному А.Ю. Киреєвим: «… починаючи з моменту зародження, рейдерство перебуває в безперервному розвитку. Рейдери знаходяться в постійному пошуку нових проектів, що характеризуються високою прибутковістю. Це неминуче призво-

[1]Там само. – С. 41.

дить до того, що з'являються нові лідери, нові більш сильні гравці, які вже можуть становити небезпеку для самого рейдера»[1].

1.3. Вплив загроз рейдерства на економічну безпеку підприємства

Ефективність розвитку системи економіко-правових відносин безпосередньо залежить від безпеки діяльності окремих суб'єктів господарювання. При цьому в якості однієї з найбільш значущих складових безпеки виступає економічна безпека, яка, згідно сучасним теоретичним уявленням «... нерозривно пов'язана з економічною ефективністю функціонування господарських об'єктів, з економічною незалежністю, стабільністю та безпекою суспільства»[2].

Аналіз існуючих теоретичних поглядів щодо поняття «економічна безпека» свідчить про відсутність загальновизнаного підходу до визначення її економіко-правової сутності.

У контексті відсутності універсального визначення поняття «економічна безпека», вбачаємо за доцільне, звернути увагу на окремі етимологічні аспекти даної проблематики.

Згідно деяким літературним джерелам (тлумачний словник Роберу – англ. *The Collins-robert French Dictionary*), перша згадка поняття «безпека» мала місце в 1190 році. Зокрема, професор Попов О.І. відзначає, що згідно наведеної редакції поняття «безпека», воно означало «... спокійний стан духу людини, що рахувала себе захищеною від будь-якої небезпеки» [3]. Примітно, що усвідомлення сутності поняття «безпека» зазнавало істотних зміни протягом часу.

Так, в XVII-XVIII столітті, визначення поняття «безпека» значно змінилося, і в більшості випадків застосовувалося не з позиції стану захищеності, а з погляду необхідності реалізації державою функції забезпечення безпеки суспільства. Подібне трактування поняття «безпека» мало місце і в законі Російської імперії від 14 серпня 1881 року

---

[1]Киреев А.Ю. Рейдерство в Российской экономике: сущность, тенденции и возможности противодействия. Автореф. дис. … канд. экон. наук: 08.00.05 / А.Ю. Киреев. – М., 2008. – С. 11.

[2] Матвеев Н. Экономическая безопасность предприятия : дисс. ... канд. экон. наук. –М. : Изд-во "Лотос", 1999. – С. 12.

[3] Попов А.И. Экономическая теория: Учебник для вузов. 4-е изд. – СПб.: Питер, 2006. – С. 465.

«Положення про заходи щодо охорони державного порядку і суспільного спокою». У контексті аналізованої етимологічної проблематики, цей закон визначав «безпеку» з позиції державних заходів, спрямованих на розширення меж влади адміністративно-поліцейських органів на певних територіальних одиницях в цілях досягнення стану посиленої і надзвичайної охорони.

Зміна в природі розуміння суті «безпека» (у тому числі і економічна безпека) мало місце і в пострадянський період. Так, академік Абалкін Л., одним з перших визначив економічну безпеку як стан економічної системи, що дозволяє їй динамічно розвиватися і ефективно вирішувати соціальні завдання. Вказаний учений справедливо помічав, що перебування держави в умовах подібного стану сприяє розробці і реалізації в життя незалежної економічної політики[1].

Вельми схожим вбачається підхід до визначення поняття «Економічна безпека» професора Тамбовцева В.Л. Зокрема, даний вчений відносить економічну безпеку кожної системи до сукупності здібностей стану її виробничої підсистеми, що забезпечує можливість досягнення цілей всієї системи[2].

У подальшому, поняття економічна безпека було дещо розширено. Так, в колективній монографії, присвяченій питанням забезпечення економічної безпеки, Шлемко В.Т. та Бінько І.Ф. асоціюють економічну безпеку зі станом національної економіки, який дозволяє зберегти стійкість до внутрішніх і зовнішніх погроз і здатній задовольнити потреби особи, сім'ї, суспільства, держави[3].

Подібний підхід до визначення поняття «Економічна безпека» демонструється і професором Р. Пастернак-Таранушенко. Зокрема, даним вченим в якості економічної безпеки запропоновано розуміти стан стабільного існування держави, завдяки чому забезпечені найкращі умови для життя його мешканців, функціонування і розвитку самої держави [4]. При цьому, суть поняття економічна безпека держави зазначеним

---

[1] Абалкин Л. И. Экономическая безопасность России: угрозы и их отражение / Л. И. Абалкин // Вопросы экономики. – 1994. – № 12. – С. 4.

[2]Тамбовцев В. Л. Экономическая безопасность хозяйственных систем : структура проблемы / В. Л.Тамбовцев // Вестник МГУ. Сер. 6. Экономика. – 1995. –С. 14.

[3]Шлемко В.Т., Бінько І.Ф. Економічна безпека України: сутність і напрямки забезпечення. – К.: НІСД, 1997. – С. 3.

[4] Пастернак-Таранушенко Г.А. Економічна безпека держави. – К.: Інститут державного управління і самоврядування при Кабінеті Міністрів України, 1994. – С. 7.

автором асоціюється із станом гарантованого і стабільного розвитку економіки, причому, як в сьогоденні, так і в майбутньому[1].

Вельми примітний підхід до визначення сутності економічної безпеки, запропоновано доктором економічних наук Предборським В.А. Зазначений вчений переконаний, що безпека є результатом певної свідомості, соціальній діяльності щодо забезпечення безпеки особи, сім'ї, суспільства, держави. Розвиваючи вказану точку зору, Предборський В.А. зазначає, що діяльність із забезпечення безпеки виникає як соціальний феномен, який спрямований на подолання суперечностей між об'єктивною реальністю - небезпекою і потребами особи, соціальних груп, суспільства і держави на принципах попередження»[2].

Аналіз вищезазначених дефініцій поняття «економічна безпека» свідчить про доцільність виділення ключових рівнів економічної безпеки. Так, акцентуючи увагу на цієї обставині, відомий вітчизняний економіст Жаліло Я. виокремлює три основні рівні національної економічної безпеки, а саме: економічна безпека держави, економічна безпека суб'єкта господарювання, та економічна безпека фізичних осіб[3].

При цьому подібна диференціація рівнів економічної безпеки, неодноразово опинялася в епіцентрі наукової критики з боку економістів. Зокрема, український економіст Васильцев Т.Г. справедливо звертає увагу на необхідності розширення переліку рівнів економічної безпеки такими компонентами, як регіон, галузь, сектор економіки [4]. Погоджуючись з подібним висловлюванням автора, слід зазначити, що реалізація широкого підходу до виокремлення рівнів економічної безпеки сприяє більш глибокому розумінню її економіко-правової природи, а також детальному дослідженню галузевих і територіальних аспектів економічної безпеки.

В контексті зазначеного вище, вельми переконлива точка зору, згідно якої «... системне усвідомлення змісту економічної безпеки держави

---

[1]Пастернак-Таранушенко Г. А. Економічна безпекадержави. Статики процесузабезпечення / ГеннадійАдольфович Пастернак-Таранушенко ; за ред. Б. Кравченка. – К.: Кондор, 2002. – С. 29.

[2] Предборський В.А. Економічна безпека держави: Монографія. – К.: Кондор, 2005. – С. 13.

[3] Жаліло Я. А. Економічна стратегія держави: теорія, методологія, практика / Ярослав Анатолійович Жаліло. – К. : НІСД. 2003. – С. 24.

[4]Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – С. 11.

вимагає обґрунтування визначення процесу її забезпечення і функціонування взаємозв'язків її елементів (як системи) в динаміці: існуючий рівень і захищеність інтересів в майбутньому; здібність до розвитку»[1].

Певною специфікою характеризується і визначення поняття «економічна безпека» сучасних представників російської економічної думки. Так, академік Сенчагов В.К., резюмуючи усе різноманіття підходів до визначення поняття економічна безпека, прийшов до наступного висновку. Суть економічної безпеки визначається ним як «... такий стан економіки та інститутів влади, при якому забезпечується гарантований захист національних інтересів, соціально направлений розвиток країни в цілому, достатній оборонний потенціал навіть за найбільш несприятливих умов розвитку внутрішніх і зовнішніх процесів»[2].

При цьому заперечення Сенчаговим В.К. необхідності співвідношення економічної безпеки до якоїсь абстрактної теоретичної конструкції більш ніж виправдано. Подібний теоретичний підхід може бути аргументований готовністю, а головне реальною здібністю публічних органів влади до захисту інтересів суб'єктів економічних відносин, а також інтересів національної економіки в цілому.

Специфічний підхід до визначення поняття «економічна безпека» демонструється й іншим представником російської економічної науки - академіком Вечкановим Г.С. Погоджуючись у загальних рисах з визначенням «економічна безпека», що було запропоновано академіком Сенчаговим В.К., Вечканов Г.С. вбачає необхідність розширення даного поняття наявністю сформованого в державі рівня створених правових норм, законодавчих і інших органів, а також засобів і методів забезпечення захисту національних інтересів[3].

Аналіз існуючих підходів до визначення сутності економічної безпеки держави дозволяє зробити висновок щодо багаторівневої природи її розбудови. У контексті узагальнення існуючих теоретичних поглядів на природу економічної безпеки держави, вельми доцільним, вбачається висновок, щодо її багаторівневої системи організації. Вказана система гостро потребує захисту власних структурних складових (компонентів) на різних рівнях ієрархії управління економікою.

---

[1]Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – С. 11.

[2] Сенчагов В.К. Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. 2-е изд. – М.: Дело, 2005. – С. 72.

[3] Вечканов Г. С. Экономическая безопасность : учеб. / Григорий Сергеевич Вечканов. – СПб. : Питер, 2007. – С.31-32.

Звертаючи увагу на цей факт, український економіст Васильцев Т.Г. справедливо асоціює зазначені рівні ієрархії управління економікою з державою, регіонами, галузями, секторами економіки, окремими підприємствами, особою тощо[1].

З позиції універсальності поняття «національна економічна безпека», що знаходить свій прояв в захищеності соціально-економічних відносин на мега-, макро-, мезо- і мікрорівнях економіки, однією із найважливіших її структурних складових виступає «економічна безпека підприємства».

Досить широкого поширення набув теоретичний підхід, відповідно до якого, зміст поняття «економічна безпека підприємства» асоціюється з особливим станом підприємства, що характеризує здатність протистояння несприятливим зовнішнім впливам.

Звертаючи увагу на цю обставину Козаченко А.В., Пономарев В.П. і Ляшенко А.Н. на монографічному рівні справедливо характеризують подібний підхід як розширений. На думку зазначеного авторського колективу, застосовуючи даний підхід економічна безпека підприємства повинна розглядатися як: «... можливість забезпечення його стійкості в різноманітних, у тому числі і в несприятливих умовах, які складаються в зовнішньому середовищі, незалежно від характеру її впливу на діяльність підприємства, масштабу і характеру внутрішніх змін»[2].

Подібна точка зору вельми поширена в сучасній російській економічній науці і пропагується рядом її представників, зокрема: Олейниковим Є.А. [3], Забродським С.Т., Капустіним Н. [4], Шликовим В.В.[5]

Схожої позиції у визначенні економічної безпеки підприємства дотримується й український економіст Ніжник В.М.

Згідно усвідомленням цього автора, економічна безпека підприємства - це захищеність його діяльності від негативних дій зовнішнього середовища, а також здатність швидко усувати різні погрози або

---

[1] Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – С. 5.

[2]Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения / А. В.Козаченко, В. П. Пономарев, А. Н. Ляшенко. – К. : Либра,2003. – С. 36.

[3] Основы экономической безопасности. (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. М., 1997. − С. 138.

[4] Забродский В., Капустин Н. Теоретические основы оценки экономической безопасности отрасли и фирмы // Безнес-информ. – 1999. – № 15-16. – С. 35-37.

[5]Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. — СПб, 1999. − С. 36.

адаптуватися до існуючих умов, що негативно позначаються на його діяльності [1].

З урахуванням зазначених поглядів на економічну безпеку підприємства, вважаємо за необхідне, визначити в якості її найважливішого елементу - визнання ключових інтересів суб'єкта господарювання. При цьому зазначені інтереси є об'єктивним проявом, як внутрішньо корпоративних взаємозв'язків підприємства, так і зв'язків підприємства з іншими суб'єктами господарювання і суспільством в цілому.

Важливо підкреслити, що «економічні інтереси підприємства» ініціюються фактично усіма структурними складовими суб'єкта господарювання.

У даному зв'язку, слід погодитися з думкою Петрова Ю.В., який акцентує увагу в своїй дисертації на тому, що «... структура економічних інтересів підприємства включає сукупність особистих, колективних і суспільних інтересів, які виявляються у вигляді прямих і непрямих виробничих економічних інтересів поточного, середньо- і довгострокового характеру» [2].

Аналіз існуючих теоретичних підходів до визначення сутності поняття «економічна безпека», а також дослідження економіко-правової природи рейдерства дозволяє асоціювати погрози рейдерства з можливістю нанесення збитку (шкоди) суб'єктам господарювання.

У даному зв'язку вельми переконлива точка зору, згідно якої боротьба із загрозою рейдерства безпосередньо граничить з поняттям економічної безпеки підприємства. Зокрема, в ході обґрунтування подібної точки зору Радванська Н.В. розглядає рейдерські захоплення як реальні «погрози порушення цілісності підприємства» [3].

Ще більш категоричним вбачається вислів Добровольського В.І., згідно якого в ході рейдерських захоплень об'єктом посягання є не суто економічні відносини, як при шахрайстві, а економічна діяльність підприємств, як складову економічної безпеки держави. Подібна точка зору до визначення сутності рейдерського захоплення власності

---

[1] Нижник В.М. Економічна дипломатія та економічна безпека України: Навчальний посібник / В.М. Нижник. – Хмельницький: ХНУ, 2007. – С. 93.

[2] Петров Юрий Владимирович. Особенности реализации экономических интересов предприятия (фирмы) в транзитарной экономике России : Дис. ... канд. экон. наук : 08.00.01. Тамбов, 2000. – С. 45.

[3] Радванська Н.В. Рейдерство як загроза економічній безпеці підприємства та держави // Вісник Хмельницького національного університету. – 2011. – № 2. – С. 204.

підприємств, дозволяє Добровольському В.І. асоціювати рейдерство з «економічним тероризмом» [1].

Вважаємо за доцільне визнати часткову істинність подібної думки. Так, вельми переконливою вбачається теоретична позиція, згідно якої як родовий об'єкт будь-якого рейдерського захоплення власності (з позиції правопорушення) виступає економічна безпека держави. При цьому безпосереднім об'єктом подібного акту протиправної вольової активності є економічна безпека підприємств і «чужа власність у вигляді її майнових комплексів» [2]. З іншого боку, вельми сумнівне заперечення можливості посягання рейдерів на корпоративні права власників захоплюваного підприємства, що породжують складні різновиди внутрішньогосподарських економіко-правових відносин.

Проблематика прямого взаємозв'язку погроз рейдерства з економічною безпекою підприємства неодноразово потрапляла в епіцентр полеміки вітчизняних економістів. Зокрема, в одній зі своїх монографій Васильцев Т.Г. звертає увагу, що проблеми здійснення підприємницької діяльності, які існують на сьогоднішній день, спотворюють систему мотивації як підприємців, так і пересічних громадян до підприємництва. В результаті цього, в суспільстві відбувається спотворення правової культури такого типу економічного порядку, який орієнтується на закриту конкуренцію і дозволяє досягати успіху особам, які вміють якнайкращим способом «обходити закони» і мають добре налагоджені корупційні зв'язки з органами державного управління, а не тим, хто може ефективніше використовувати обмежені економічні ресурси. При цьому автор справедливо відзначає, що існування «... кримінальних, рейдерських, дискримінаційних дій щодо суб'єктів підприємницької діяльності є прямою (фізичною) загрозою належному функціонуванню і відповідно економічній безпеці підприємництва» [3].

Примітним є те, що найбільш великі підприємства, які здійснюють прибуткову господарську діяльність на території нашої держави, найчастіше, не створюються в ході прозорих форм конкурентної боротьби, а переходять у власність за наслідками приватизаційних процесів. В деяких випадках, подібні підприємства переходять у власність

---

[1] Добровольский В.И. Ответственность рейдера по российскому законодательству / В.И. Добровольский. – М.: Волтерс Клувер, 2010. – С. 33.

[2] Там само. – С. 33.

[3] Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – С. 39-40.

унаслідок вторинного перерозподілу раніше приватизованих об'єктів державної власності. У даному зв'язку, цілком закономірна думка, що домінує в кругах фахівців, згідно якій навіть наявність власності - вже достатня причина для того, щоб хтось побажав її привласнити або придбати з мінімальними витратами. Подібний феномен сучасної моделі здійснення господарської діяльності обумовлює специфічну закономірність, унаслідок якої, одним із засобів протидії рейдерству є ефективність збереження інформації про власне підприємство.

При цьому завдання підсистеми інформаційного забезпечення економічної безпеки підприємства, в умовах погроз рейдерських атак, полягає у зборі, накопиченні і оцінці інформації про потенційні джерела небезпеки з метою максимального зниження невизначеності стратегічних ризиків.

Звертаючи увагу на цю обставину, дослідник проблематики забезпечення економічної безпеки підприємства Шаваєв А.Г [1], визначає низку вимог до інформації, відповідно до яких, інформація повинна: свідчити про дійсні наміри потенційних і діючих партнерів; містити відомості про сильні і слабкі сторони конкурентів; дозволяти здійснювати вплив на позиції зацікавлених осіб в процесі переговорів; сигналізувати про можливі протиправні посягання на діяльність суб'єкта; дозволяти контролювати хід реалізації і дотримання партнерами, раніше досягнутих домовленостей; виявляти несанкціоновані канали витоку конфіденційної інформації.

Враховуючи особливу актуальність збору і обробки інформації для забезпечення економічної безпеки в умовах існуючих рейдерських погроз, вбачається за доцільне, зобразити даний процес схематично (Рис. 1.2).

Таким чином, в умовах реально існуючих погроз рейдерського захоплення збір, аналіз і обробка відповідної інформації є найбільш відповідальною ланкою не тільки системи забезпечення безпеки, але і маркетингу, оскільки на її основі формується стратегія здійснення господарської діяльності підприємства.

Аналіз існуючих підходів до розуміння сутності погроз функціонування підприємств пов’язаних з реалізацію рейдерських атак дозволяє сформулювати низку висновків:

---

[1]Шаваев А.Г. Система борьбы с экономической разведкой. М.: Изд-во «Правовое просвещение». 2000.-240с.; С. 67.

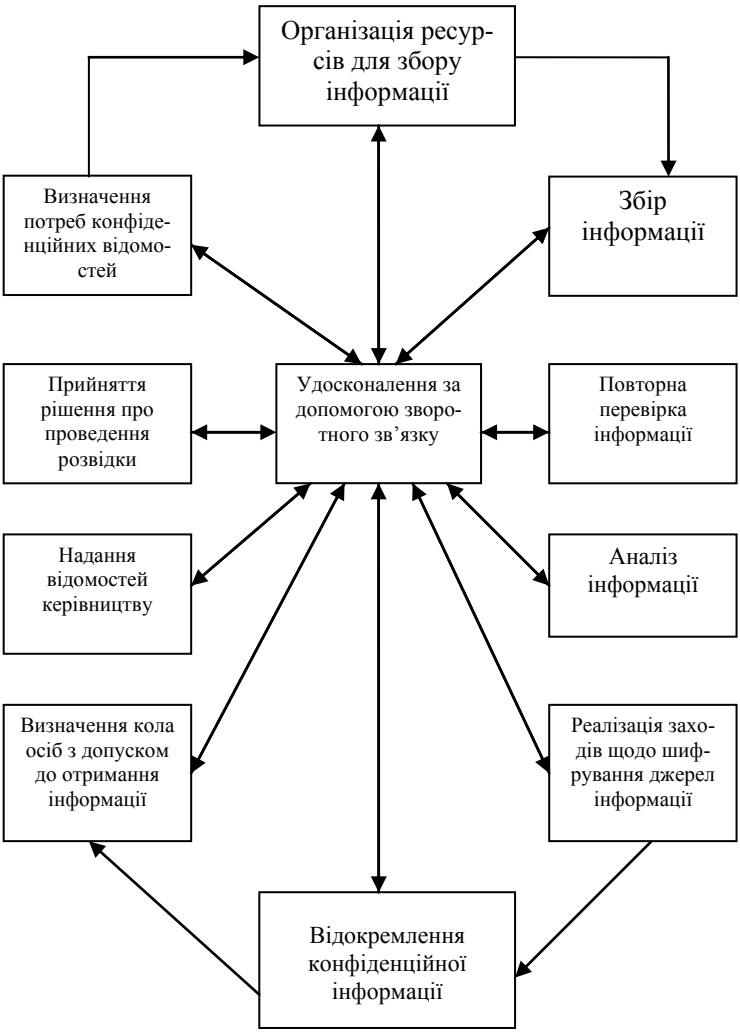


Рис.1.2. Схема збору і обробки інформації для забезпечення економічної безпеки підприємства

1. Загрози рейдерства знаходяться в тісному взаємозв'язку з детермінантами і безпосередніми фактами здійснення низки правопорушень (зокрема злочинів), що посягають на безпеку функціонування підприємства. Так, відмова власника крупного пакету акцій (паїв) у продажу своєї частки контролю бізнесу, часто, обумовлює здійснення рейдерами таких протиправних, зокрема кримінальних, дій: навмисне доведення до банкрутства з корисливих мотивів шляхом укладення завідомо збиткових, економічно необґрунтованих зобов'язань, надання гарантій, поруки, надання в заставу майна.

Одним із загальновідомих методів захоплення підприємств є ініціація банкрутства обраної жертви шляхом створення штучної кредиторської заборгованості або навмисної скупки боргів із одночасним пред'явленням їх до сплати. Класична схема рейдерського захоплення виглядає таким чином. Після створення на підприємстві штучної кредиторської заборгованості кредитори ініціюють процедуру банкрутства даного підприємства та виведення з штату топ-менеджменту, перерозподіл активів підприємства і його ліквідацією (або ж існування без активів).

При цьому, згідно з аналітичними даними «... до реалізації подібних схем долучають кваліфікованих юристів, арбітражних керуючих, суддів, працівників податкових органів і державних реєстраторів». фальсифікація договорів про відступлення частки (акції) або договорів купівлі продажу оспорюваних в судовому порядку істотних часток захоплюваного підприємства; фальсифікація протоколів загальних зборів учасників, рішень «не легітимно уведених» в структуру топменеджменту осіб про відчуження директорату; відкриття в асоційованому з рейдерами банку додаткового рахунку підприємства і акумулювання на ньому грошових коштів з інших рахунків цього підприємства; продаж майна підприємства або продаж підприємства в цілому фізичним і юридичним особам, не обізнаним про злочинний характер його відчуження («добросовісному набувачеві»); загрози на адресу акціонерів (учасників); фізичне захоплення підприємств.

Реалізація даної мети часто, як і у випадках доведення до банкрутства, як правило, супроводжується примусовим виконанням державною виконавчою службою рішень судів, для чого притягуються приватні охоронні фірми і (або) правоохоронні органи; ініціація необґрунтованих перевірок контролюючими органами або порушення відносно керівників підприємства кримінальних справ; перешкоджання

учасникам товариства у здійсненні ними права голосу на зборах і (або) в наданні інформації про його діяльність[1]; публікація в засобах масової інформації замовлених матеріалів на користь «рейдерів-загарбників»; реєстрація підставних фірм для подальшого оформлення на них продажів і перепродажів захопленого підприємства і його майна; виготовлення підробленої печатки підприємства;; примушування акціонерів всупереч їх волі до продажу акцій.

2. Погрози рейдерства, в переважній більшості випадків, знижують ступінь ефективності функціонування підприємства - об'єкту рейдерського посягання. Наочним підтвердженням вказаної думки є офіційна статистика Міністерства економіки України. Зокрема, тільки в 2006 році, за даними вказаної установи, сумарний обіг рейдерських атак склав 3,5 млрд. доларів США[2].

У той же час, на фоні зазначеної статистики, державні витрати у тому ж році, спрямовані на підтримку підприємництва склали еквівалент 1,8 млн. грн., що на думку Васильцева Т.Г. свідчить про низьку ефективність державної політики в досліджуваній сфері [3]. Іншими словами, фінансові втрати підприємців, що опинилися в епіцентрі рейдерських захоплень, більш ніж в 9 тис. разів перевищують реальні витрати державного бюджету на підтримку підприємництва.

Згідно сучасним уявленням щодо природи забезпечення економічної безпеки підприємства[4], реалізація рейдерських дій із захоплення підприємства обумовлює виникнення низки негативних наслідків, зокрема: створення украй несприятливих умов для ефективного функціонування підприємства; зниження інвестиційної і інноваційної активності; зниження конкурентоспроможності виробленої продукції або ж послуг, що надаються, створення вкрай несприятливих умов для їх реалізації; активізація посягань на співробітників підприємства з боку конкурентів (або рейдерських груп); «витік» кваліфікованого персоналу; нераціональне використання власності підприємства, а в

---

[1] Добровольский В.И. Ответственность рейдера по российскому законодательству / В.И. Добровольский. – М.: Волтерс Клувер, 2010. – С. 1.

[2] Вакханалия стоп : украинским рейдерам светят новые перспективы [Електронне джерелео]. – Інтернет видання Інформаційної агенції « ЛІГАБізнесінформ». – № 103 (744). – 2008. – Режим доступу: www.times.liga.net//articles/gs013450.html.

[3] Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – С. 181-182.

[4] Ларина И.Е. Экономика защиты информации : Учебное пособие. – М.: МГИУ, 2007. – С. 6.

деяких випадках і її втрата; зниження прибутків підприємства; зниження внутрішньої і зовнішньої стабільності підприємства.

3. У разі істотного загострення рейдерських загроз підприємства повинні негайно реалізовувати заходи, які спрямовані на їх нейтралізацію або відшкодування понесених збитків.

Слід зазначити, що ідея повного усунення існуючих загроз рейдерських захоплень вельми утопічна.

Тим часом, їх загостренню сприяють так звані індикатори «рейдерської придатності», до яких в сучасній економічній літературі[1], як правило, відносять: відсутність в Україні єдиної державної політики у сфері протидії корупції; високий рівень корупції в державних, правоохоронних, контролюючих і судових органах; можливість отримання відповідного судового рішення, як правило, спірного; практика «розташування» дрібних пакетів акцій між акціонерами підприємства; численні зміни керівництва на всіх рівнях влади, безкарність при здійсненні ними владних повноважень; вкрай низька ефективність практиці оцінки активів підприємства; організаційні та правові проблеми здійснення господарської діяльності; суперечливість статутної документації приписам чинного законодавства; системні порушення порядку придбання активів і акцій; прорахунки в юридичній фіксації правоволодіння активами та акціями; неефективність внутрішньогосподарської системи розподілу функцій і повноважень органів управління суб'єкта господарювання; прорахунки у внутрішньогосподарській (статутній) документарній фіксації порядку організації та здійснення корпоративних відносин; порушення організаційно-правових аспектів порядку проведення зборів акціонерів і ради директорів; порушення чинних нормативно-правових приписів статутної фіксації функціональних обов'язків (компетенції) керівних органів; введення і наступне перебування номінальних осіб («проліскив») в системі топменеджменту підприємства; слабкий рівень організації захисту комерційної таємниці, а також документації з обмеженим доступом користування; прорахунки в юридичному оформленні легітимізації угод; порушення при роботі з поштою і прийомом кореспонденції; ефемерність функціонування служби безпеки підприємства, так само, як і

[1]Дульський О.О. Рейдерство – нова загроза державній та економічній безпеці України // Боротьба з організованою злочинністю і корупцією. – 2009. – № 11. – С. 90.; Радванська Н.В. Рейдерство як загроза економічній безпеці підприємства та держави // Вісник Хмельницького національного університету. – 2011. – № 2. – С. 204-205.

відсутність налагодженої внутрішньогосподарської взаємодії між моніторинговими підрозділами суб'єкта господарювання.

Аналіз існуючих думок щодо природи загроз економічній безпеці[1] дозволяє акцентувати увагу на прямому взаємозв'язку рейдерства з наступними загрозами економічної безпеки: зростання корумпованості органів державної влади, представників судового апарату і правоохоронних органів; зменшення сумарних надходжень до бюджету держави через прогресуючу динаміку ухилення від сплати податків; монополізація окремих галузей виробництва або сфер надання послуг; створення сприятливого підґрунтя розповсюдження негативної практики доведення до банкрутства і ворожих захоплень; погіршення інвестиційного клімату; значне зниження конкурентоспроможності окремих галузей виробництва або сфер надання послуг; збільшення об'ємів операцій щодо легалізації (відмивання) доходів, придбаних злочинним шляхом; падіння виробництва в різних галузях господарювання; підвищення рівню безробіття. Підсумовуючи дослідження економіко-правової суті загроз рейдерства економічній безпеці підприємства, вбачається за доцільне, сформулювати висновки щодо їх типології за методами реалізації рейдерських захоплень.

Не дивлячись на існуюче різноманіття способів рейдерських захоплень підприємств, усі зазначені діяння можна класифікувати відповідно до трьох основних методів їх реалізації, а саме: загрози рейдерства економічній безпеці, засновані на формально законній методології рейдерських дій; загрози рейдерства економічній безпеці, засновані на протиправній методології рейдерських дій; загрози рейдерства економічній безпеці, засновані на комбінованій методології рейдерських дій, що характеризується можливістю комбінування формально законних і протиправних погроз рейдерського захоплення. Вважаємо за доцільне, наочно продемонструвати типологію загроз

---

[1]Предборський В.А. Економічна безпека держави: Монографія. – К.: Кондор, 2005. – 391 с.; Шлемко В.Т., Бінько І.Ф. Економічна безпека України: сутність і напрямки забезпечення. – К.: НІСД, 1997. – С. 3.; Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – 384с.; С. 54.; Федоров А.Ю. Рейдерство и корпоративный шантаж (организационно-правовые меры противодействия) : монография / А.Ю. Федоров. – М.: Волтерс Клувер, 2010. – 480 с.; С. 32-33; Акимов В.А. Оценка и прогноз стратегических рисков России: теория и практика / Право и безопасность. – 2004. – № 1. – С. 17.; Потапов В.Я. Оценка и прогноз опасностей и угроз современной России // Право и безопасность. – 2003. – № 3-4. – С. 11.; Экономическая безопасность Российской Федерации: учеб. для вузов: в 2 ч. – СПб., 2001. – С. 72-73.

рейдерського захоплення, засновану на методології його здійснення, за допомогою відповідного малюнка (Рис.1.3).

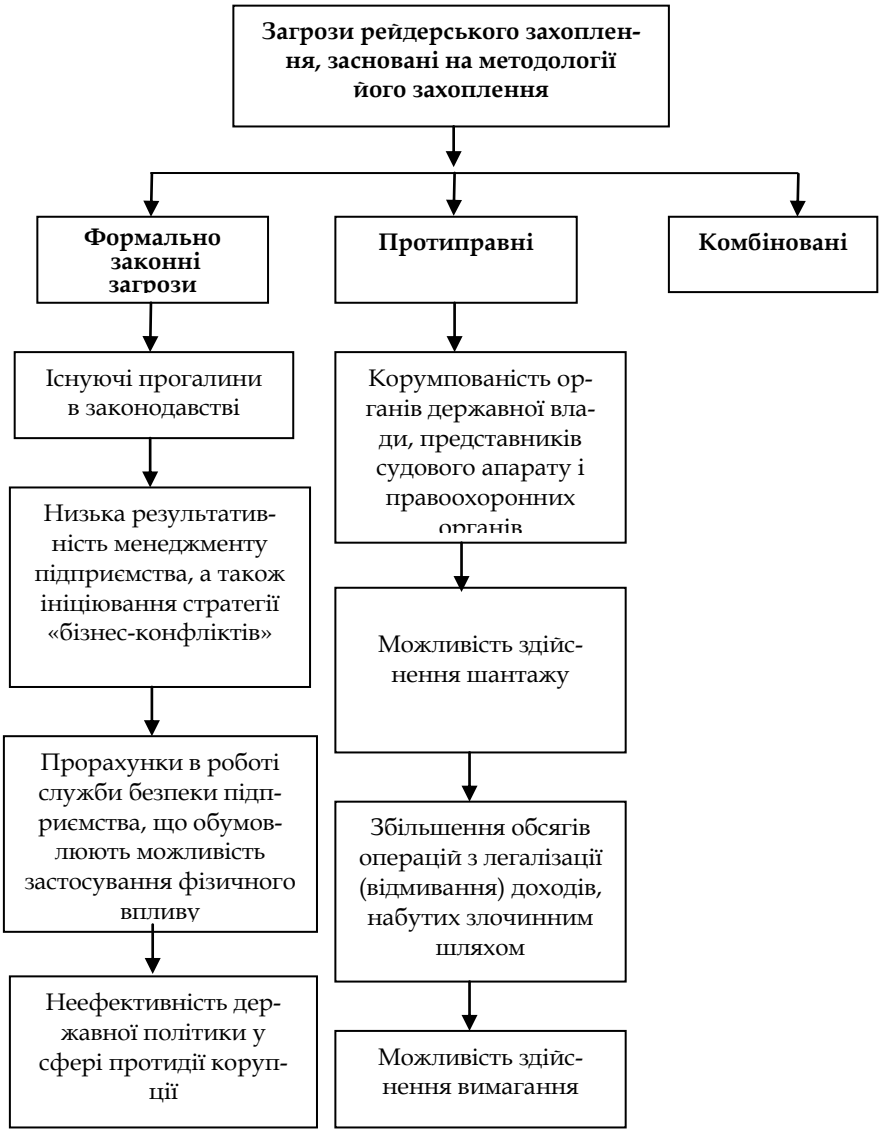


Рис 1.3. Класифікація загроз рейдерства економічної безпеки підприємства залежно від методу його реалізації

В контексті формально законних загроз рейдерського захоплення особливе місце посідає і методика боротьби за голоси акціонерів.

До боротьби за голоси акціонерів підприємство-агресор удається у тому випадку, якщо в неї немає реального корпоративного контролю над підприємством-метою. Підприємство-агресор переконує акціонерів, як правило, міноритарних, передати за довіреністю їхньому представнику голоси на загальних зборах акціонерів, сподіваючись зібрати достатню кількість голосів для демократичної, на перший погляд, зміни складу органів корпоративного управління (правління, наглядової ради).

На перший погляд, боротьба за голоси акціонерів підприємства-мети є нескладним способом недружнього (або ворожого) поглинання, але «обробка» міноритарних акціонерів потребує індивідуального підходу, подолання консервативності міноритарних акціонерів, збереження у таємниці істинних намірів представників підприємства-агресора і подолання опіру менеджменту підприємства-мети, у якого є дієві способи «оборони». Боротьба за голоси акціонерів підприємства-мети як спосіб недружнього (або ворожого) поглинання підприємства-мети може дати результати за певних умов: кількість акцій є великою; акції підприємства-мети сильно розосереджені (велика питома вага міноритарних акціонерів); в акціонерів підприємства-мети є підстави (реальні або штучно створені) бути впевненими в ефективності її менеджменту; в менеджменті підприємства-мети є приховані (або навіть явні) прихильники поглинання.

Рейдерська атака за суттю схожа з боротьбою за голоси акціонерів підприємства-мети – йдеться про скупку акцій, але на відзнаку від боротьби, яка може тривати певний час, відбувається дуже швидко, іноді – блискавично. Акції підприємства-мети скуповуються на фондовій біржі або у позабіржовому обігу в максимально короткий термін. Якщо процес скупки акцій затягується, виникає ризик збільшення ринкової ціни акцій підприємства-мети. Крім того, про ведення боротьби за голоси акціонерів підприємство-мета часто знає і обороняється, тоді як рейдерська атака відбувається дуже швидко, і часто підприємство-мета узнає про неї вже по завершенню (часто вдалому) атаки.

Рейдерство ініціюється і бізнес-конфліктом або корпоративним конфліктом для встановлення повного контролю над бізнесом, результатом якого є не позитивний економічний і соціальний ефект, а отри-

мання короткострокової користі. Мотивом рейдерських дій можуть бути не лише матеріальні цінності, а й такі спонукання як особиста неприязнь, помста, незадоволені амбіції, намагання знищити конкурента. Правилом є скерованість не на ефективний розвиток виробництва, збільшення прибутковості підприємства-мети і досягнення конкурентних переваг, а отримання негайного прибутку будь-якою ціною [1].

Корпоративний конфлікт – це конфлікт інтересів власників підприємства. Проблематичність даного конфлікту в тому, що корпоративний конфлікт може перетекти у захоплення підприємства з підробкою документів та перехопленням управління підприємством. Часто корпоративний конфлікт є елементом рейдерських дій, але він не завжди прямо пов`язаний із рейдерством. Корпоративний конфлікт можна урегулювати і без відчуження підприємства.

На відміну від формально-законних загроз та методів рейдерських захоплень, незаконне рейдерство або рейдерство у його тлумаченні, що сформувалося на пострадянському просторі – це заволодіння майном, бізнесом методами, що суперечать чинному законодавству. У свою чергу, незаконне рейдерство поділяється на кримінальне та некримінальне, залежно від наявності передбаченого кримінальним законодавством країни складу злочину в діях загарбника [2].

Резюмуючи вищезгадане, вважаємо за доцільне зазначити, що загострення загроз рейдерства економічній безпеці підприємства, що виходять від зовнішніх і внутрішніх джерел небезпеки, повинно зумовлювати характер і напрямок діяльності по забезпеченню безпеки підприємства. У даному зв'язку, вельми переконливою є думка, згідно якої«... в основі організації, планування та реалізації заходів забезпечення безпеки в різних сферах є аналіз і оцінка характеру реальних і потенційних внутрішніх і зовнішніх загроз, кризових ситуацій, а також інших несприятливих чинників, що перешкоджають досягненню поставлених цілей і становлять небезпеку для життєво важливих інтересів»[3].

Отже, дослідження комплексу питань, що стосуються економічної характеристики рейдерства, в контексті визначення його понять та

---

[1] Бироваш М. Силовой прием / М. Бироваш // Бизнес. – 2007. – № 6. – С. 24-27.

[2] Понятие рейдерства. Факторы [Электронный ресурс]. - Real Estate Development Group. – Режим доступа: http://www.red-develop.com/ru/informaciya/analitika/115.html.

[3] Экономика и организация безопасности хозяйствующих субъеков, 2-е изд. – СПб.: Питер, 2004. – С. 70-71.

передумов впливу на економічну безпеку підприємства, дозволило дійти таких висновків:

1. Нещодавно сформоване «в колисці» силового підприємництва рейдерство вже встигло перейти межі легітимності соціально-економічної поведінки. На цьому етапі свого розвитку рейдерство набуло форми вольових актів підвищеної суспільної небезпеки, що обмежують законні права й інтереси власників, персоналу підприємств, що зазнали протиправної активності рейдерів.

2. Рейдерство – це реалізація заходів, спрямованих на заволодіння підприємством (його активами) без згоди власника або шляхом його примусу до згоди, з використанням незаконних або формально законних дій. При цьому, формально законні дії рейдера порушують правила «ділового обігу» і посягають на основні права і свободи суб'єктів економічної діяльності.

3. Попри певну схожість економіко-правової природи, «рейдерство» та «недружнє поглинання» – різні поняття. Зважаючи на це, слід погодитися з фахівцями в галузі безпеки, що рейдинг (рейдерство) – це процес, а поглинання – це результат [1].

Доцільно відрізняти «рейдерство» від процесів злиття та поглинань, корпоративних конфліктів і грінмейлу за низкою критеріїв. Суттєва відмінність зазначених понять полягає у відмінності їх мети: характерною метою рейдерства є заволодіння підприємством і його майном для отримання негайного прибутку.

В свою чергу мета злиття та поглинань (процеси *M&A*), як правило, полягає в підвищенні конкурентоспроможності, у тому числі на міжнародному рівні, або в симетричній відповіді на дії конкурентів, що укрупнюються.

Не менш специфічна і мета грінмейлу, суть якої зводиться до отримання прибутку від продажу акцій за підвищеними цінами без захвату підприємства.

4. Історія вітчизняної моделі рейдерської діяльності має такі етапи свого розвитку:

- *перший етап – стадія зародження рейдерства*: кінець 1980-х – початок 1990-х років – «бандитський» перерозподіл позитивного фінансового потоку у формі рекету (від англ. *rack* – мучити, катувати)

---

[1]Поняття рейдерства та його суспільна небезпечність [Електронне джерело] // Юридична консультація в інтернеті Pozov.com.ua. – Режим доступу : http://www.pozov.com.ua/ua/rejderstvo_ua.html.

– «… примусового стягування з підприємця постійної плати за послуги з охорони (іноді дійсно наданої)» ;

- *другий етап*: початок 1992 – 1996 роки – рейдерські захоплення майнових комплексів державних підприємств під егідою проголошеного курсу державної приватизації;

- *третій етап*: 1996 – середина 2000-х рр. – епоха резонансних банкрутств з їх подальшим оскарженням і застосування «методик» доведення до банкрутства з метою наступного викупу дочірньої інфраструктури підприємства (земельні ділянки, будинки, споруди).;

- *четвертий етап – стадія розквіту рейдерства*: 2004 – 2009 рр. – розповсюдження технологій злиття та поглинань у галузі чинного приватного (раніше приватизованого) бізнесу та поширення негативних наслідків глобальної фінансової кризи.

5. До основних передумов розвитку рейдерства в Україні слід віднести: низький рівень правової культури та правовий нігілізм на всіх рівнях: серед суб'єктів господарювання, представників органів влади та в суспільстві загалом; низький рівень ступеня відкритості суспільства і економіки; високий рівень корумпованості правоохоронних, судових і дозвільних структур; недосконаліть ринкових інструментів перерозподілу власності та велика кількість управлінських внутрішньогосподарських помилок («резерв формальних приводів рейдерства»); відсутність регулярної ринкової оцінки ліквідних активів підприємств; ефемерність української моделі фондового ринку, а отже, і відсутність чіткої реалізації вільного обігу акцій; нечітка і непрозора система реєстрації прав власності; низька інформаційна транспарентність підприємств; зростання корпоративних конфліктів, пов'язаних з недосконалістю законодавства у сфері корпоративних відносин; недосконаліть правової системи й відсутність державних інституцій ефективного захисту прав власності в Україні.

6. Аналіз існуючих підходів до розуміння сутності погроз функціонування підприємств пов'язаних з реалізацію рейдерських атак дозволяє сформулювати наступні висновки: по-перше, загрози рейдерства знаходяться в тісному взаємозв'язку з детермінантами і безпосередніми фактами здійснення низки правопорушень (зокрема злочинів), що посягають на безпеку функціонування підприємства; по-друге, погрози рейдерства, в переважній більшості випадків, знижують ступінь ефективності функціонування підприємства - об'єкту рейдерського посягання; по-третє, у разі істотного загострення рейдерсь-

ких загроз підприємства повинні негайно реалізовувати заходи, які спрямовані на їх нейтралізацію або відшкодування понесених збитків.

7. Не зважаючи на існуюче різноманіття способів рейдерських захоплень підприємств, усі зазначені діяння можна класифікувати відповідно до трьох основних методів їх реалізації, а саме: загрози рейдерства економічній безпеці, засновані на формально законній методології рейдерських дій; загрози рейдерства економічній безпеці, засновані на протиправній методології рейдерських дій; загрози рейдерства економічній безпеці, засновані на комбінованій методології рейдерських дій, що характеризуються можливістю комбінування формально законних і протиправних погроз рейдерського захоплення.

В наступному розділі наведено більш детальне дослідження впливу різноманітних факторів небезпеки, в тому числі рейдерських загроз, на діяльність підприємств.

Р О З Д І Л 2

ДОСЛІДЖЕННЯ ЗАГРОЗ РЕЙДЕРСЬКИХ ПОСЯГАНЬ НА ПІДПРИЄМСТВО

2.1. Виявлення факторів небезпеки підприємства

Важливе місце в дослідженні факторів небезпеки займає їх аналіз, під яким розуміють – процедури виявлення факторів небезпеки і оцінки їх значимості. По суті, це аналіз ймовірності того, що відбудуться певні небажані події, що негативно вплинуть на досягнення цілей проекту. Аналіз небезпек включає виявлення, оцінку факторів небезпек та управління небезпекою (зниження небезпеки або зменшення пов'язаних із ним несприятливих наслідків).

Забезпечення економічної безпеки підприємства, наприклад харчової промисловості, вимагає ухвалення ефективних рішень, пов'язаних з виявленням, обліком і знаходженням способів запобігання або ослаблення погроз.

Одні погрози можна передбачати, інші виникають раптово. Передбачати можна ті, які виникають в певних умовах, відомі з досвіду попередньої економічної діяльності. Непередбачені погрози можуть виникнути у зв'язку з несподіваними діями партнерів, конкурентів або форс-мажорними обставинами.

Загроза небезпеки – об'єктивний тренд, подія, що спричиняє за собою небезпеку втрат, збитку, шкоди або сприймане як таке.

Економічна небезпека – це об'єктивно-суб'єктивна категорія у діяльності суб'єктів господарювання, що пов'язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору[1]. Вона відображає міру відхилення від цілей, від очікуваного результату, міру невдачі (збитків) з урахуванням впливу керованих і некерованих чинників, прямих та зворотних зв'язків стосовно об'єкта керування.

Це визначення ґрунтується на системному підході до категорії економічної небезпеки і вказує на необхідність аналізу впливу на

[1] Рахматуллин Р.К. Особенности ценообразования на продукцию сельского хозяйства в условиях развитой рыночной экономики // ИНИОН РАН «Новая литература по социальным и гуманитарным наукам. Депонированные научные работы», раздел «Экономика». − № 11. − 1999.

об'єкти управління множини внутрішніх і зовнішніх чинників та надсистеми, а також ставлення до суб'єктів небезпеки.

Об'єктом небезпеки називають економічну систему, ефективність та умови функціонування якої наперед точно невідомі.

Під суб'єктом небезпеки розуміють особу (або колектив), яка зацікавлена в результатах управління об'єктом ризику і має компетенцію прийняття рішень щодо об'єкта небезпеки.

Джерело небезпеки — це чинники (явища, процеси), які спричиняють невизначеність результатів, конфліктність у широкому сенсі цього поняття.

Під інформаційною ситуацією розуміють певний ступінь градації невизначеності навколишнього середовища в одному з можливих станів із заданої множини, якою володіє суб'єкт управління на момент прийняття рішення.

Якісний аналіз небезпеки вимагає ґрунтовних знань, досвіду, інтуїції в тій чи іншій сфері економічної діяльності. Його головна мета — визначити фактори і зони небезпеки, після чого ідентифікувати всі можливі ризики. Характерними для цього аналізу зокрема, є наступні аспекти[1].

Перший аспект пов'язаний з необхідністю порівнювати очікувані позитивні результати з можливими економічними, соціальними (як сьогоденними, так і майбутніми) несприятливими наслідками. У зв'язку з цим необхідно ідентифікувати причини виникнення небезпеки, виявити її чинники, види невизначеності та конфліктності, які зумовлюють небезпеки. Необхідно також здійснити класифікацію небезпеки.

Другий аспект якісного аналізу небезпеки пов'язаний з виявленням впливу рішень, які приймаються в умовах невизначеності та конфліктності, на інтереси суб'єктів господарювання. Коли немає зацікавленості в результатах економічних рішень, то немає й небезпеки. Ситуація результату може бути охарактеризована, зокрема, такими рисами: наявність невизначеності та (чи) конфліктності; наявність альтернатив (стратегій) та необхідність вибору однієї з них (уникнення того, щоб здійснити вибір, є різновидом вибору); можливість оцінити наявні альтернативи та прийняти рішення. Спочатку суб'єкт небезпеки усвідомлює ризикованість ситуації, прогнозує можливі потенціальні втрати (збитки), причому не лише у формі грошей, а й прес-

[1] Савицкая Г.В. Анализ хозяйственной деятельности предприятий. – М.: Экоперспектива, 2007. – 301 с.

тижу, злагоди з керівництвом, роботодавцями, постачальниками тощо. Усвідомивши ситуацію як таку, що обтяжена небезпекою, вона оцінює її прийнятність для себе. На відміну від теорії прийняття рішень, вихідний пункт якої − гіпотеза, що суб'єкт вже перебуває в ризикованій ситуації, людина (керівник) вирішує, як її уникнути. Пристосуватися до небезпеки можуть допомогти дії, що знижують ймовірність небажаних подій чи величину потенційних збитків або впливають на розподіл наслідків небезпеки серед суб'єктів господарської діяльності чи суспільства в цілому.

Для кожної стадії прийняття ризикованого рішення характерні свої закономірності. Так, на стадії усвідомлення і попереднього оцінювання (вимірювання) небезпеки, його суб'єкт фокусує свою увагу на одній-двох найважливіших, на його думку, характеристиках. Найчастіше зосереджуються на величині очікуваного доходу (наприклад, коли питання торкається інвестицій) і майже не замислюються над імовірністю збитків. Здебільшого інформація про конкретну ситуацію формується у суб'єкта небезпеки в два етапи: спочатку обирається одна з характеристик як деяке обмеження, а іншу вважають за мету. При цьому відкидають усі альтернативи, що не відповідають обраним обмеженням. Далі з тих альтернатив, що залишилися, обирають ту, яка забезпечує найвищий рівень характеристики, обраної за мету. Зазвичай, характеристику («ймовірність одержання не меншого від деякого заданого значення прибутку») розглядають як обмеження, а «величину сподіваного прибутку» − як мету.

Зовнішнє пристосування (інтравертність) до небезпеки полягає в спробі суб'єкта ризику певним чином модифікувати зовнішнє середовище, щоб дістати деякі переваги. Йдеться про маневрування ресурсами, маніпулювання поводженням контрагентів (партнерів) при укладенні угод тощо.

Внутрішнє пристосування (екстравертність) до небезпеки є характерним для осіб, які не дуже вірять у можливість контролю над зовнішнім середовищем та безпосереднього впливу на нього. Їх основний інструмент, − це збір додаткової інформації, виграш у часі, підключення своїх керівників до процесу прийняття відповідальних рішень, генерація нових альтернатив.

Так, приймаючи рішення стосовно великих інвестицій, деякі особи, що відповідають за прийняття рішень, намагатимуться торгуватися з банком щодо умов позики, ставок відсотків, графіків виплат

або будуть прагнути залучити банк до справ своєї фірми на правах співучасника (зовнішнє пристосування до небезпеки). Інші особи більше уваги приділятимуть збиранню інформації про можливості банку та його заінтересованість у наданні кредиту фірмі чи обмірковуванні проблеми обхідних шляхів на випадок провалу операції і падіння авторитету фірми (внутрішнє пристосування до небезпеки).

Слід мати на увазі, що під час прийняття певного рішення доцільно виявити інтереси основних учасників подій: хто яку позицію займає, хто і як ставиться до вашої ініціативи. В результаті заздалегідь складеться певне уявлення про можливий перебіг подій (пов'язані з цим суперечності та перешкоди, що зумовлюють ризик). Для ведення переговорів це досить важливий чинник, який дає змогу здійснити аналіз ситуації, обтяженої небезпекою, та вжити відповідних заходів щодо її переведення в більш сприятливу.

Поводження підприємця в умовах небезпеки має орієнтуватися: на пошук «рушійної пружини» ризикової ситуації (осмислення проблеми, формування управлінської задачі, розстановка сил), використовуючи ситуаційний (сценарний) аналіз; на відшукання зв'язку даної ризикованої ситуації з попередніми обставинами (історичний метод) та прогнозування загроз щодо різних ускладнень, які можуть призвести до збитків; на зіставлення ризикової задачі з розвитком цілісної системи управління (системний підхід); на обґрунтування і використання технологій розв'язання управлінських задач, адекватних ситуацій; на формування адекватного стилю управління (нова тактика в нових обставинах, обтяжених ризиком). В. В. Вітлінський пропонує таку багатокрокову процедуру (алгоритм) якісного аналізу небезпеки та поведінки його суб'єктів щодо прийняття рішень у ситуації, обтяженій небезпекою (рис 2.1).

В основу цього підходу покладено зміну ставлення до споживачів товарів (послуг), торгових партнерів, працівників підприємств. Ці стосунки насправді, а не лише декларативно, прагнуть зробити менш конфронтаційними (суперечливими), конкурентні стратегії доповнюються стратегіями співпраці.

По-перше, суб'єкт управління (небезпеки) може бути сам соціально-економічною системою. Його цілі (множина цілей) можуть не збігатися і мати суперечливий характер. Слід зазначити, що далеко незавжди цілі можна відносно легко відобразити в кількісній формі,

тому оцінка різноманітних ситуацій і варіантів (стратегій, проектів) може виявитися неоднозначною.

Рис. 2.1. Узагальнена формалізована процедура аналізу небезпеки та поведінки його суб'єктів[1]

По-друге, моделі, що описують поведінку об'єктів управління (небезпеки), нездатні, і в цьому, як правило, немає потреби, відображати всі його властивості. По-третє, наявна інформація не завжди відображає усі суттєві моменти, бо їх врахування здійснюється опосередковано, насамперед через систему економічних показників. Вони

[1] Вітлінський В. В., Верченко П. І. Аналіз, моделювання та управління економічним ризиком: Навч.-метод. посібник для самост. вивч. дисц. – К.: КНЕУ, 2000 – С. 12.

ж, у свою чергу, відображають якісні чинники в кількісно вираженій формі, а це призводить до втрати частини інформації.

Небезпеки, як звісно, можна класифікувати на зовнішні і внутрішні. Під зовнішніми чинниками слід розуміти ті умови, які підприємці, як правило, не в змозі змінити, але повинні їх прогнозувати та враховувати, бо вони істотно впливають на стан справ.

Згідно із загальною теорією менеджменту зовнішні чинники доцільно розподілити на дві групи: чинники безпосереднього впливу та чинники опосередкованого впливу. Основні з цих чинників наведено на рис. 2.2.

Рис. 2.2. Система зовнішніх чинників небезпеки

В економічній літературі, присвяченій проблемам підприємництва, виокремлюють такі чотири групи чинників, які належать до внутрішніх факторів небезпеки: стратегія фірми; принципи діяльності фір-

ми; ресурси та їх використання; якість і рівень використання маркетингу.

Динамічна небезпека — це небезпека, пов'язана з непередбачуваними (недетермінованими) змінами вартості основного капіталу внаслідок прийняття управлінських рішень або непередбачуваними зсувами у ринкових чи політичних реаліях. Такі зміни можуть призвести як до збитків, так і до додаткових прибутків.

Статична небезпека — це небезпека, пов'язана зі скороченням реальних активів внаслідок втрати частки власності, а також із скороченням доходу через недієздатність організації. Ця небезпека може призвести лише до збитків.

Видове різноманіття небезпек дуже велике — від пожеж і стихійних лих до міжнаціональних конфліктів, змін у законодавстві, що регулює економічну та підприємницьку діяльність, інфляційних коливань тощо. Виявлені небезпеки підприємства описані нижче були взяті у економічного відділу підприємства, де в свою чергу вони були отримані використовуючи метод мозкового штурму.

Проаналізуємо види небезпек, з якими пов'язана діяльність одного з аграрних підприємств Донецької області.

Виробнича небезпека - небезпека пов'язана з виробництвом продукції, товарів і послуг; із здійсненням будь-яких видів виробничої діяльності, в процесі якої підприємці стикаються з проблемами неадекватного використання сировини, підвищенням собівартості, збільшенням втрат робочого часу, неефективним використанням нових методів виробництва. На підприємстві, що досліджувалося, були виявлені таки головні фактори виробничої небезпеки: використання неякісної сировини, простій устаткування при поломці тощо.

До основних причин, що зумовлюють економічну небезпеку, можна віднести: зниження намічених обсягів виробництва та реалізації продукції; відсутності в потрібний момент часу необхідної кількості матеріалів та комплектуючих, підвищення відсотка браку; зниження цін, згідно з якими планувалося реалізовувати продукцію та послуги, у зв'язку з їхньою недостатньою якістю, несприятливими змінами у ринковій кон'юнктурі тощо; збільшення питомої ваги затрат матеріальних, енергетичних, паливних ресурсів, зростання транспортних витрат, торговельних накладних та інших побічних витрат.

Сюди ж можна віднести зростання фонду оплати праці з причин перевищення очікуваної чисельності працюючих чи внаслідок пере-

вищення рівня заробітної плати окремим працівникам; зростання податків та інших відрахувань внаслідок змін ставки оподаткування тощо; низький рівень дисципліни постачання, зокрема, збої в постачанні палива, електроенергії тощо; фізичне та моральне зношення основних фондів (обладнання) тощо[1]

Виявлено, що найважливішими факторами економічної небезпеки підприємства – об'єкта дослідження є: зниження обсягів реалізації внаслідок зниження попиту або витіснення товарів конкуруючими товарами (замінниками) або запровадження обмежень на продаж товарів тощо; підвищення закупівельної ціни на зерно; фізичне та моральне зношення основних фондів (обладнання) тощо.

Головні фактори соціальної небезпеки цього підприємства – це небезпека втрати ділової репутації та недобросовісна діяльність партнерів і конкурентів. Під фінансовою небезпекою розуміють небезпеку, що виникає під час здійснення фінансового підприємництва чи фінансових угод. До фінансової небезпеки належать: валютна, кредитна та інвестиційна небезпека. Для цього підприємства актуальними є кредитна та інвестиційна небезпеки.

Кредитна небезпека - можливість того, що підприємство не зуміє погасити свої борги вчасно та небезпека часткового або повного непогашення дебітором своєї заборгованості перед підприємством. Фактор кредитної небезпеки є актуальним для підприємства, тому що воно фінансово нестійке через недостатність власного капіталу, тож має високу потребу в кредитуванні. Можливі наслідки здійснення загрози кредитного ризику невиплати кредиту підприємством взятого в банку - банкрутство. Небезпека не погашення дебітором своєї заборгованості перед підприємством може спричинити за собою часткову або повну втрату виділених кредитних грошей.

Фактор інвестиційної небезпеки також є вельми актуальним для підприємства, тому що він зумовлюється і залежить від специфіки вкладення підприємницькою фірмою коштів на свій розвиток. Нерідко в економічній літературі інвестиційними небезпеками вважають лише небезпеки, зумовлені вкладенням коштів у цінні папери. Насправді під цими небезпеками слід розуміти різноманітні суттєві небезпеки, що можуть виникнути при використання коштів на розвиток підприємства.

[1] Ястремський О.І. Моделювання економічного ризику. – К.: Либідь, 1992. – 176 с.

Інноваційна небезпека — це міра можливих збитків, які можуть виникнути у разі вкладення підприємницькою фірмою коштів у виробництво нових товарів, технологій, послуг, що не відразу сприймаються ринком або не знаходять свого споживача взагалі.

Вибір перспективних проектів розвитку підприємства є вкрай важливим для діяльності підприємства і його стабільного росту. Основні небезпеки на підприємстві, які належать до групи інвестиційних, наведено в табл. 2.1.

Можливими наслідками загроз інвестиційної небезпеки на підприємстві є втрата капіталу, знецінення реальної вартості капіталу, зниження ліквідності активів.

Таблиця 2.1

Основні види інвестиційної небезпеки підприємства

Види небезпеки	Пояснення
Капітальна	Загальна небезпека, що стосується усіх інвестиційних вкладень. Небезпека полягає у тому, що при нераціональному використанні засобів на розвиток підприємство буде не в змозі повернути інвестовані засоби без збитків
Селективна	Ризик спрямованого вибору об’єкта для інвестування в порівнянні з іншими варіантами
Відсоткова	Небезпека збільшення витрат по сплаті відсотків або зниження доходу від використання коштів на розвиток підприємства до рівня нижче очікуваного із-за коливань загального рівня процентних ставок
Небезпека ліквідності	Небезпека труднощів продажу активів підприємства (наприклад небезпека збитків унаслідок нездатності підприємства забезпечити виконання своїх зобов'язань поставок товару в повному об'ємі)
Небезпека інфляції	Ризик полягає у тому, що через високі темпи інфляції доходи, які надійдуть від вкладених у розвиток підприємства коштів, можуть знецінитися у реальних цінах

Окремою фінансовою небезпекою можна виділити зниження фінансової стійкості. Ця небезпека генерується недосконалістю струк-

тури капіталу (надмірною часткою використовуваних позикових коштів), що породжує незбалансованість позитивного і негативного грошових потоків підприємства за обсягами[1]. Наслідком цієї небезпеки може бути банкрутство підприємства, тому небезпека зниження фінансової стійкості є важливим фактором для оцінки рівня економічної безпеки підприємства.

Слід зазначити, що різноманітні небезпеки нерідко взаємопов'язані, зміни одних викликають зміну інших. Більшість з них впливають на результати економічної діяльності і вимагають як аналізу на якісному, так і на кількісному рівнях. Виявлені загрози підприємству та їх можливі наслідки наведені в табл. 2.2.

Таблиця 2.2

Основні виявлені загрози підприємству та їх можливі наслідки

Тип небезпеки	Назва фактору небезпеки	Можливі наслідки	Характер джерела небезпеки
Економічна	Зниження обсягів реалізації через зниження попиту	Зниження прибутку, низька ефективність праці	Зовнішня
Соціальна	Зношення основних фондів	Зниження якості продукції, поломки обладнання	Внутрішня
Фінансова	Підвищення закупівельної ціни на зерно	Збільшення витрат виробництва	Зовнішня
Виробнича	Втрата ділової репутації	Зниження попиту на продукцію і послуги	Зовнішня

Перелік загроз може бути використано у діяльності підприємств при розробці відповідних заходів.

[1] Бочарников В.П., Релецкий С.М., Захаров К. В. и другие. Риски во внешнеэкономической деятельности предприятий. – К.: ИНЭКС, 1997. — 170 с.

2.2. Діагностика рівня економічної безпеки підприємства та оцінка їх захищеності

Діагностика рівня економічної безпеки – це визначення кількісним або якісним способом величини (ступеня) небезпеки. Отже кількісний аналіз та моделювання є тими інструментальними засобами, які дають змогу оцінити, виокремити, нехай і наближено, суттєві ризики з несуттєвих (надуманих). Однак у більшості випадків одного лише якісного аналізу недостатньо для ідентифікації та виокремлення суттєвих чинників ризику й нехтування несуттєвими (надуманими). З цією метою необхідно здійснювати кількісний аналіз небезпеки. А це потребує здобуття відповідної інформації.

Методи експертних оцінки включають комплекс логічних і математико-статистичних методів і процедур, пов'язаних з діяльністю експерта по переробці необхідної для аналізу і прийняття рішень інформації.

Центральною «фігурою» експертної процедури є сам експерт – фахівець, який використовує свої здібності (знання, вміння, досвід, інтуїцію і т.п.) для знаходження найбільш ефективного ня[1].Експерти, що залучаються для оцінки небезпеки, повинні: мати доступ до всієї наявної в розпорядженні розробника інформації про проект; володіти достатнім рівнем креативності мислення та необхідними знаннями у відповідній предметній області; бути вільним від особистих переваг щодо проекту (не лобіювати його).Можна виділити наступні основні методи експертних оцінок, що застосовуються для аналізу небезпеки: запитальники; SWOT-аналіз; роза і спіраль ризиків; оцінка ризику стадії проекту; метод Дельфі.

Метод Дельфі дозволяє за допомогою декількох послідовних голосувань прийти до найкращого з даного питання рішення. При цьому голосування анонімні, що "виключає вплив натовпу". Метод реалізується таким чином (рис. 2.3).

1. Ставиться завдання – питання, на які потрібно відповісти. При цьому відповідь повинна виражатися чисельно.

2. Відбирається експертна група - група людей (зазвичай 10 або більше), які є фахівцями в цій сфері і будуть голосувати.

3. Проводиться перший тур голосування. При цьому експерти:

---

[1] Ковалев В.В., Волкова О.Н. Анализ хозяйственной деятельности предприятия. – М.: ТК Велби, 2002. – 34 с.

- виставляють оцінку собі (чисельне значення із заздалегідь визначеного діапазону, яке показує наскільки об'єктивною або аговитою вважає свою думку експерт); дають чисельну оцінку з питання голосування. Оцінка може бути як з якогось діапазону, так і без обмежень. Експерт повинен як можна детальніше обґрунтувати свою думку, чому він поставив саме цю оцінку в коментарі.

Рис. 2.3. Алгоритм методу Дельфі

4. Після цього аналітична група проводить аналіз даних. Обчислюються: середньогрупова оцінка − число, рівне середньоарифметичному всіх самооцінок; проста оцінка − середньоарифметичне усіх поставлених оцінок; середньозважена оцінка − обчислюється як сума творів оцінки експерта на його самооцінку і поділена суму всіх самоо-

цінок; медіана - для обчислення медіани упорядковуються всі оцінки по зростанню і вибираються дві середні за номером оцінки, вираховується їх середньоарифметичне.

Вираховується довірчий інтервал. Для цього вважаються так звані квартилі − 1/4 від різниці між максимальною оцінкою і мінімальною. Нижньою межею довірчого інтервалу буде мінімум-квартиль, верхньою максимум-квартиль.

5. Далі всім експертам розсилаються результати. Вони вивчають їх, зокрема коментарі інших експертів. Проводиться другий тур, в якому експерт може як залишитися при своїй думці, так і поміняти її. Свою нову оцінку експерт повинен прокоментувати.

6. За новими даними знову обчислюються всі характеристики з пункту 4. пункти 4-6 повторюються до тих пір, поки експерти не прийдуть до спільної думки. Критерієм цього може бути, наприклад, довжина довірчого інтервалу - як тільки він стане менше, ніж заздалегідь задана величина голосування припиняється.

Метод аналогій використовують для кількісного аналізу небезпеки, якою може бути обтяжений, скажімо, новий проект, доцільно виявити дані про наслідки впливу несприятливих чинників небезпеки якихось близьких за сутністю до раніше виконуваних проектів. Під час використання аналогів застосовують бази даних та знань щодо чинників ризику. Ці бази будуються на матеріалах літературних джерел, пошукових робіт, моніторингу, опитувань фахівців тощо[1]

Одержані дані обробляють, використовуючи відповідний математичний апарат та обчислювальну техніку для виявлення залежностей та з метою врахування потенційного ризику.

Проте навіть у відносно простих і широко відомих випадках невдалого завершення проектів досить важко створити передумови, у яких ситуації повторювали б минулий досвід, яким можна було скористатися для нових проектів. Тому метод аналогій може виявитися достатнім лише в простих випадках, а в основному він використовується як допоміжний у низці інших методів. Аналіз небезпеки збитків можна здійснювати також з точки зору можливих (ймовірних) збитків, що

[1] Мельник Т. Кількісний аналіз оцінки ризику // Фінанси України. - 2000. - № 9. - С. 63-67

є характерними для будь-якого об'єкта (проекту). Для здійснення цього аналізу вводиться поняття областей (зон) небезпеки[1].

Виділяють такі зони небезпеки (рис. 2.4)

Рис. 2.4. Схема зон небезпеки і характерних точок

Безпечна зона — це область, у якій випадкові збитки не очікуються. Їй відповідають нульові збитки чи перевищення прибутку над сподіваним значенням. Ця область — область виграшу підприємця.

Зона допустимої небезпеки — це область, у межах якої зберігається економічна доцільність підприємницької діяльності, тобто випадкові збитки можуть мати місце, але вони менші сподіваного прибутку від підприємницької діяльності.

Зона критичної небезпеки — це область, де є наявною можливість збитків, які перевищують величину (обсяг) очікуваних прибутків аж до величини повної обчисленої (розрахункової) виручки від підприємницької діяльності. Величина можливих (ймовірних) збитків у цій зоні перевищує сподіваний прибуток і може призвести до втрати всіх коштів, вкладених підприємцем у справу.

Зона катастрофічної небезпеки — це область можливих збитків, які за своєю величиною (обсягом) перевершують критичний рівень і можуть досягати величини (обсягу) майнового стану підприємця. Катастрофічна небезпека може призвести до краху, банкрутства компанії (фірми), її закриття і розпродажу майна. До категорії катастрофічної небезпеки слід віднести також небезпеку, пов'язану з безпосередньою загрозою для життя чи екологічною катастрофою.

[1] Підскунова О. В. Аналіз та оцінка фінансових ризиків діяльності малих підприємств // Фінанси України. − 2007 . − № 8 . −С. 119-129

Оцінка факторам небезпеки на підприємстві була здійснена наступним чином. Головні фактори соціальної небезпеки підприємства — небезпека втрати ділової репутації та недобросовісна діяльність партнерів і конкурентів були оцінена експертним методом Дельфі з використанням опитувальників на основі попередніх даних про операції з контрагентами як фактори слабкої небезпеки.

Керівництво вживає достатніх заходів для виявлення недобросовісних контрагентів до проведення операцій з ними, а також недопущення нанесення шкоди діловій репутації підприємства.

На підприємстві були виявлені таки головні фактори виробничої небезпеки: використання неякісної сировини, простій устаткування при поломці.

Фактор використання неякісної сировини був оцінений експертним методом Дельфі з використанням опитувальників на основі попередніх даних звітності підприємства про закупівлі зерна і реалізацію борошномельних товарів виготовлених з цього зерна. Цей фактор належить до слабкої небезпеки.

Для оцінки фактора небезпеки простою устаткування при поломці була використана статистика спостереження поломок розмельного обладнання з поломки якого за даними виробничого відділу в середньому найчастіше трапляються простої при поломці на підприємстві.

Для оцінки надійності обладнання обраний метод оцінки Каплана-Мейера функції ризику[1].

Оцінка Каплана-Мейера функції ризику обчислюється за формулою

$$H\left(t \geq t_j\right) = H\left(t_j\right) = \sum_{i=1}^{j} \frac{d_i}{r_i}, \quad j = 1, 2, ..., K,$$

де di - кількість спостережень, моменти припинення яких спостерігалися з тривалістю t_i, i= 1,2, ..., K,

K - число моментів припинення,

r_i - кількість спостережень, незакінчених або цензурованих до моменту ti, i = 1,2, ..., K, причому

$$r_j = \sum_{i=j}^{K} (m_i + d_i), \; j = 1, 2, ..., K,$$

[1] Barber S., Jennison C. Symmetric tests and confidence intervals for survival probabilities and quantiles of censored survival data // Biometrics – 1999. − vol. 55. − pp. 430-436.

де m_i – кількість постережень, цензурованих між моментами t_i, it_{i+1}.

Дисперсія оцінки Каплана-Мейера функції ризику обчислюється за формулою

$$DH(t_j) = \frac{DS(t_j)}{S(t_j)},\ j = 1, 2, \ldots, K,$$

$DS(t_j), j = 1, 2, \ldots, K,$ - дисперсія функції надійності,

$S(t_j)$, $j = 1, 2, \ldots, K$ - оцінка Каплана–Мейера функції надійності.

Довірчий інтервал оцінки функції ризику обчислюється як

$$I_H(t_j) = \left(H(t_j) - \Psi((1+\beta)/2\sqrt{DH(t_j)}; H(t_j) + \Psi((1+\beta)/2)\sqrt{DH(t_j)} \right)$$

де Ψ- зворотня функція стандартного нормального розподілу,

β - довірчий рівень, виражений в частках.

Функція ризику зазвичай зображується або у вигляді ступеневого графіка, або у вигляді ламаної лінії, що сполучає задані точки, які відповідають моментам припинення[1].

Для оцінки надійності обладнання був використаний програмний продукт AtteStat. Програма аналізу даних AtteStat призначена для професійної статистичної обробки даних в різних областях діяльності. Вона виконана у вигляді надбудови до популярних електронних таблиць Microsoft Excel під управлінням операційної системи Microsoft Windows.

Для аналізу надійності обладнання був використаний модуль програми під назвою «Аналіз виживання».

Скріншот цього модуля наведено на рис. 2.5, скріншот таблиці Excel, де здійснюється введення і виведення даних,- на рис. 2.6 зображено графік отриманий в результаті оцінки функції ризику поломки обладнання підприємства. Відомо, що час напрацювання розмельного устаткування підприємства на відмову дорівнює 83 дням.

[1] Aalen O.O., Murka C., Gjessing H.K. Survival and event history analysis: A process point of view. – New York, NY: Springer, 2008.

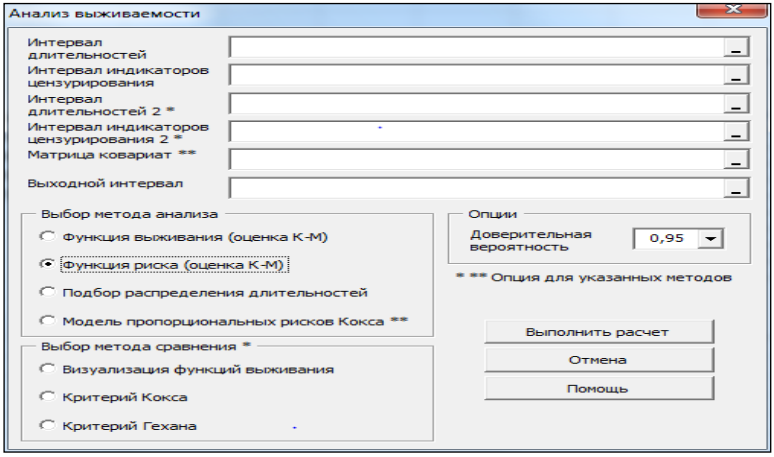
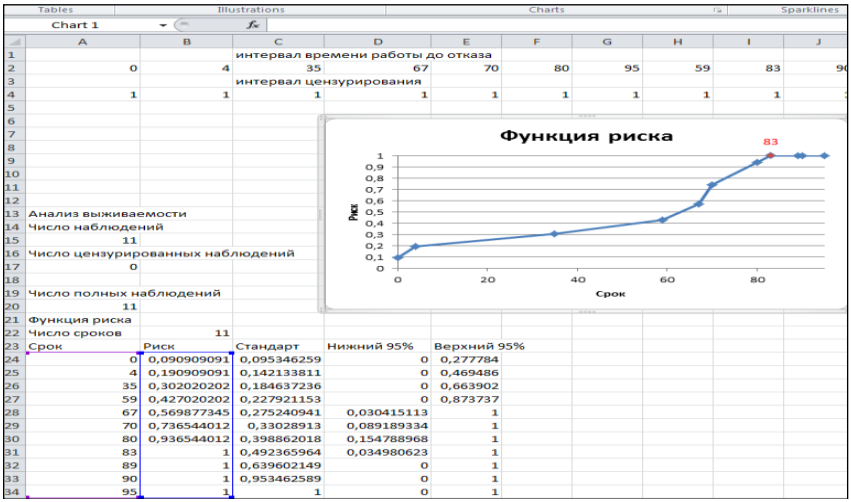


Рис. 2.5.Модуль програми AtteStat «Аналіз виживання»

Розглянемо кількісні показники надійності виробів(Н),які визначаються набором показників. Для кожного з типів виробів існують рекомендації по вибору показників Н.



	A	B	C	D	E	F	G	H	I	J
1			интервал времени работы до отказа							
2	0	4	35	67	70	80	95	59	83	90
3			интервал цензурирования							
4	1	1	1	1	1	1	1	1	1	
13	Анализ выживаемости									
14	Число наблюдений									
15	11									
16	Число цензурированных наблюдений									
17	0									
19	Число полных наблюдений									
20	11									
21	Функция риска									
22	Число сроков	11								
23	Срок	Риск	Стандарт	Нижний 95%	Верхний 95%					
24	0	0,090909091	0,095346259	0	0,277784					
25	4	0,190909091	0,142133811	0	0,469486					
26	35	0,302020202	0,184637236	0	0,663902					
27	59	0,427020202	0,227921153	0	0,873737					
28	67	0,569877345	0,275240941	0,030415113	1					
29	70	0,736544012	0,33028913	0,089189334	1					
30	80	0,936544012	0,398862018	0,154788968	1					
31	83	1	0,492365964	0,034980623	1					
32	89	1	0,639602149	0	1					
33	90	1	0,953462589	0	1					
34	95	1	1	0	1					

Рис. 2.6. Скріншот таблиці MSExcel, де здійснюється введення і виведення даних

Для оцінки Н. виробів, які можуть знаходитися в двох можливих станах - працездатному і відмовному, застосовуються такі показники: середній час роботи до виникнення відмови Тср - напрацювання до першої відмови; середній час роботи, що припадає на одну відмову, Т - напрацювання на відмову; λ (t) - інтенсивність відмов; імовірність безвідмовної роботи за час t - P (t). Закон розподілу напрацювання до відмови визначає кількісні показники Н. невідновних виробів. Закон розподілу записується або в диференціальній формі щільності ймовірності f (t), або в інтегральній формі F (t)[1].

Існують наступні співвідношення між показниками Н. і законом розподілу:

$$P(t) = 1 - F(t) = e^{\left(-\int_0^\infty \lambda(t)dt\right)};$$

$$T_{cp} = \int_0^\infty tf(t)dt = \int_0^\infty P(t)dt;$$

$$\lambda(t) = \frac{f(t)}{P(t)} = \frac{1}{T}.$$

Для відновлюваних виробів вірогідність появи n відмов за час t в разі найпростішого потоку відмов визначається законом Пуассона:

$$P_n(t) = \frac{(\lambda)^n}{n!} e^{\lambda t}$$

З нього випливає, що ймовірність відсутності відмов за час t дорівнює (експонентний закон надійності).

$$P(t) = e^{(-\lambda t)}$$

Обчислимо ймовірність відсутності відмов розмельного обладнання підприємства за місяць використання:

$$T = 83; \lambda = 1/83; t = 30$$

$$P(30) = e^{-(1\backslash 83)(30)} \approx 0,7$$

Звідси можна отримати ймовірність відмови за період часу - Q(t):

---

[1] Бруевич Н. Г. Количественные оценки надежности изделий, в сборнике: Основные вопросы теории и практики надежности - М.,1971 – 122 с.

$$Q(t) = 1 - P(t)$$

Ймовірність відмови розмельного обладнання підприємства за місяць дорівнює:

$$Q(30) = 1 - P(30) = 0,3$$

Згідно з нормативами виробничого відділу підприємства ймовірність поломки розмельного обладнання за місяць 0,3 в межах норми, тобто ступінь небезпеки простою устаткування при поломці низька.

Оцінку економічних факторів небезпеки здійснено наступним чином. У практиці роботи підприємств зустрічаються приклади використання коефіцієнта зносу як індикатора ризику виникнення збоїв у виробничому процесі. При високих значеннях коефіцієнта зносу аналітик робить відмітку про досить високий ризик збоїв у виробничому процесі та необхідність модернізації виробництва[1]. Для підприємства, що застосовує механізм прискореної амортизації по значній частці основних засобів, розрахунковий коефіцієнт зносу не буде відображати фактичний стан майна підприємства. Для підприємств, де не використовують механізм прискореної амортизації прийнято вважати, що значення коефіцієнта зносу більш ніж 50% є небажаним. Більш об'єктивну оцінку даного показника можна отримати, порівнявши його значення по конкретному підприємству зі значенням даного коефіцієнта зносу в галузі.

Розрахунки свідчать, що коефіцієнт зносу в 2012 році зростав на 6,72% з 2,23% до 8,95%, в 2013 році до 11,62%, тобто ще на 2,67%. Це обумовлено тим, що в 2011 році було закуплено нове обладнання, а також проведена модернізація старого. Тому коефіцієнт має низькі значення в 2011 і 2012 роках і поступово зростає. За даними бухгалтерії підприємство не використовує механізм прискореної амортизації, а значення коефіцієнта зносу в галузі в середньому становить 50-55%. Таким чином порівнявши показник зносу основних засобів підприємства за 2013 рік з середнім по галузі можна зробити висновок про те що показник зносу основних фондів значно нижче середнього показника по галузі (що обумовлено покупкою нового обладнання та модернізацією та ремонтом старого в 2011 році). Це означає, що небезпека

[1]Кольцова И. В., Рябых Д. А. Практика финансовой диагностики и оценки проектов. – М.: ООО «И.Д. Вильямс», 2007. – С. 102-103.

зносу основних фондів не є реальною загрозою за даними на 2013 рік, тобто підприємство у безпеці на найближчих 2 роки якщо темпи зростання зносу основних фондів збережуться на рівні 2013 року та оскільки показник зносу основних фондів підприємства значно нижче середнього показника по галузі.Фактор зниження обсягів реалізації (внаслідок зниження попиту або витіснення товарів конкуруючими товарами або запровадження обмежень на продаж товарів тощо) був оцінений експертним методом з використанням опитувальників на основі попередніх даних звітності про попит на товари та реалізацію товарів. Доцільно на прикладі цього чинника розглянути обробку експертних даних за допомогою методу Дельфі.

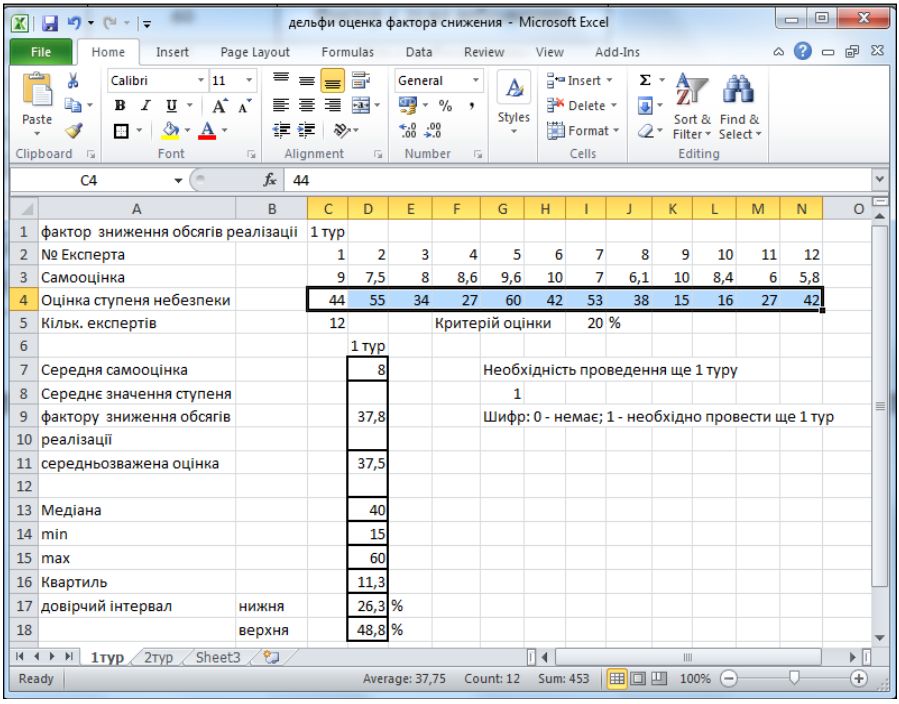
Запрошено 12 експертів, кожному з яких була дана анкета з проханням оцінити рівень небезпеки фактору зниження обсягів реалізації. Експерт ставив собі індивідуальну самооцінку в балах (від 0 до 10), оцінював рівень небезпеки фактору зниження обсягів реалізації у відсотках (0т 0 до 100). Робота проводилась індивідуально і анонімно. Критерієм оцінки було обрано довжину інтервалу не більше 20%. Результати після першого туру мали вигляд(табл.2.3).

Таблиця 2.3.

Результати після першого туру методу Дельфі

№ експерта	Коефіцієнт самооцінки	Рівень небезпеки	Коментар
1	9	44	Він несе значну небезпеку
2	7,5	55	Цей фактор небезпечний
3	8	34	Слабка небезпека
4	8,6	27	Фактор допустимоїнебезпеки
5	9,6	60	Фактор є дуже небезпечним
6	10	42	Він є небезпечним
7	7	53	Це фактор критичної небезпеки
8	6,1	38	Небезпека несуттєва
9	10	15	Майже не небезпечний
10	8,4	16	Небезпека дуже низька
11	6	27	Допустима небезпека
12	5,8	42	Значна небезпека

Для аналізу даних був використаний MS Excel(рис.2.7).



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	фактор зниження обсягів реалізації		1 тур											
2	№ Експерта		1	2	3	4	5	6	7	8	9	10	11	12
3	Самооцінка		9	7,5	8	8,6	9,6	10	7	6,1	10	8,4	6	5,8
4	Оцінка ступеня небезпеки		44	55	34	27	60	42	53	38	15	16	27	42
5	Кільк. експертів		12			Критерій оцінки			20 %					
6				1 тур										
7	Середня самооцінка			8			Необхідність проведення ще 1 туру							
8	Середнє значення ступеня						1							
9	фактору зниження обсягів			37,8			Шифр: 0 - немає; 1 - необхідно провести ще 1 тур							
10	реалізації													
11	середньозважена оцінка			37,5										
12														
13	Медіана			40										
14	min			15										
15	max			60										
16	Квартиль			11,3										
17	довірчий інтервал	нижня		26,3	%									
18		верхня		48,8	%									

Рис. 2.7. Скріншот MS Excel аналізу даних 1 туру методу Дельфі

Нижня межа довірчої області – 26,3%, верхня – 48,8%. Відповідно довірчий інтервал складав від 26,3% до 48,8%, тобто дорівнює 22,5%, і перший тур не відповів поставленому критерію.

Необхідно було провести другий, тобто відправити експертам анкети повторно з проханням переголосувати і вказати причину зміни своєї думки.

Нижня межа довірчої області – 21,75%, верхня – 35,25%. Відповідно довірчий інтервал склав: від 21,75% до 35,25%, тобто дорівнює 13,5%, й другий тур відповідає поставленому критерію.

За результатами аналізу був зроблено висновок що це фактор допустимої небезпеки.

Результати після другого туру мали вигляд (табл.2.4).

Таблиця 2.4.

Результати після першого туру методу Дельфі

№	Коефіцієнт самооцінки	Рівень небезпеки	Коментар
1	9	37	Небезпека нижче ніж я думав
2	7,5	25	Хворів, помилився з оцінкою
3	8	34	Слабка небезпека
4	8,6	27	Фактор допустимої небезпеки
5	9,6	40	Переоцінив небезпеку фактору
6	10	23	Передумала, фактор допустимої небезпеки
7	7	33	Небезпека не критична
8	6,1	38	Небезпека несуттєва
9	10	15	Майже не небезпечний
10	8,4	16	Небезпека дуже низька
11	6	27	Допустима небезпека
12	5,8	42	Значна небезпека

На рис. 2.8 наведено результати аналізу даних 2 туру.

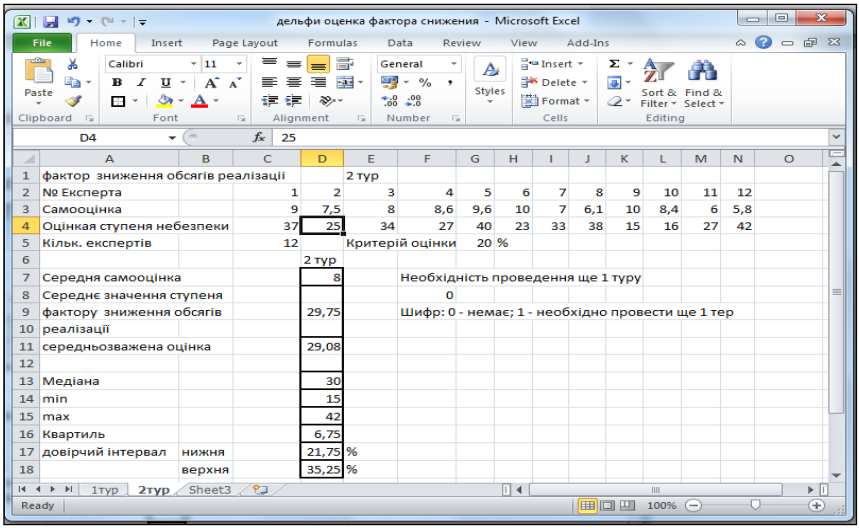


Рис. 2.8. Скріншот MS Excel аналізу даних 2 туру

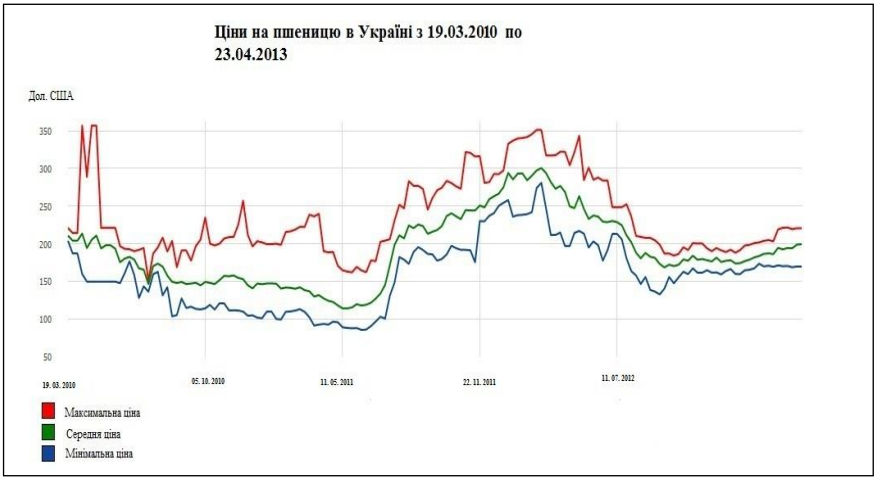


Рис. 2.9. Ціни на пшеницю в Україні з 2010 по 2013 рік. Джерело – веб-сайт www.grainboard.ru.

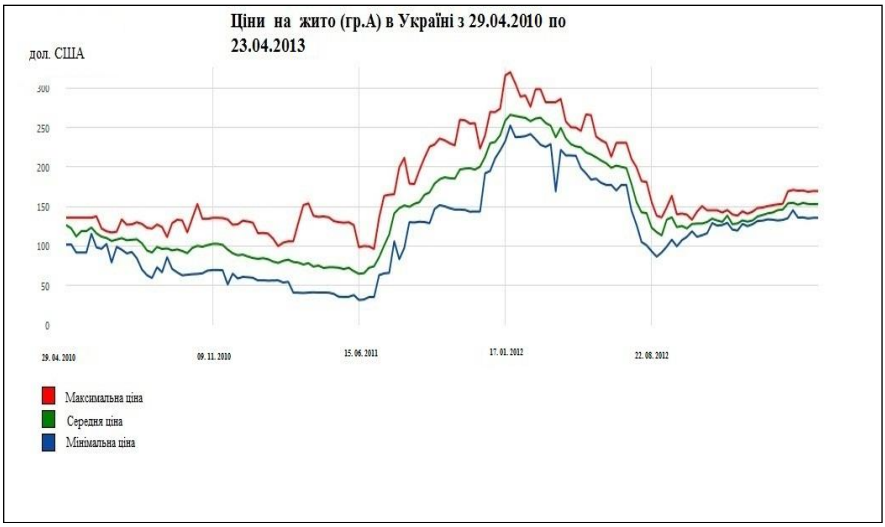


Рис. 2.10. Ціни на жито в Україні з 2010 по 2013 рік.
Джерело – вебсайт www.grainboard.ru.

Для оцінки небезпеки фінансової нестійкості проаналізуємо ймовірність банкрутства підприємства.

Найбільш відомою моделлю діагностики банкрутства є розроблена Е. Альтманом на основі проведення мультидискримінантного аналізу модель «Z–рахунку», яка також часто називається «модель Альтмана», тому саме вона взята в якості основної для проведення аналізу[1].

При обчисленні значення показника, який використовується для оцінки фінансової стійкості підприємства, вірогідності його банкрутства за цією моделлю, до уваги приймається п´ять факторів. Вони включаються до інтегрального показника шляхом множення на відповідні коефіцієнти.

В узагальненому вигляді формула розрахунку «Z–рахунку» має вигляд:

$$Z = A \cdot X\,1 + B \cdot X\,2 + C \cdot X\,3 + D \cdot X\,4 + E \cdot X5,$$

де змінні X і являють собою коефіцієнти, які обчислюються за даними фінансової звітності конкретного досліджуваного підприємства й оцінюють різні аспекти його фінансового стану, а саме:

X1 – це відношення суми власного оборотного капіталу до загальної суми активів, що може бути проінтерпретоване як міра ліквідності підприємства;

X2 – відношення нерозподіленого прибутку до загальної суми активів;

X3 – відношення прибутку до сплати відсотків та податків до загальної суми активів, яке можна інтерпретувати як міру доходності підприємства;

X4 – відношення власного капіталу до позичкового капіталу;

X5 – відношення виручки від реалізації до загальної вартості активів, що можна інтерпретувати як коефіцієнт оборотності активів.

Значення коефіцієнтів при змінних X і вважаються заданими.

Як правило, модель Альтмана формується з конкретними значеннями цих коефіцієнтів. Проте в літературі зустрічається декілька варіантів значень цих коефіцієнтів, основні з яких наведені в табл. 2.5.

---

[1] Економіко-математичні моделі оцінки фінансового стану суб'єктів господарювання: монографія / О.М. Тридід, О.Г. Тижненко, Л.О. Тижненко. – К.: УБС НБУ, 2009. – 213 с.

Таблиця 2.5

Варіанти значень коефіцієнтів в моделі Альтмана

Варіант	A	B	C	D	E
Варіант 1	1,2	1,4	3,3	0,6	1,0
Варіант 2	0,012	0,033	0,014	0,006	0,999
Варіант 3	0,717	0,847	3,107	0,42	0,995

Наявність різних варіантів коефіцієнтів не є помилкою, а лише відображає специфіку побудови та застосування моделі Альтмана. Справа в тому, що коефіцієнти в моделі Альтмана обчислюються на основі статистичного аналізу даних про фінансовий стан збанкрутілих підприємств за певний період часу. Перший і другий варіанти коефіцієнтів обчислені на основі даних підприємств, акції яких котирувалися на біржі. Особливість третього варіанту полягає в тому, що він розроблений для компаній, акції яких не котирувалися на біржі. Тому оцінка вартості власного капіталу для цього варіанту показника здійснюється на основі даних балансу, а не ринкової оцінки, що більше підходить для оцінки підприємства.

Результати обчислень наведені на рис. 2.11.

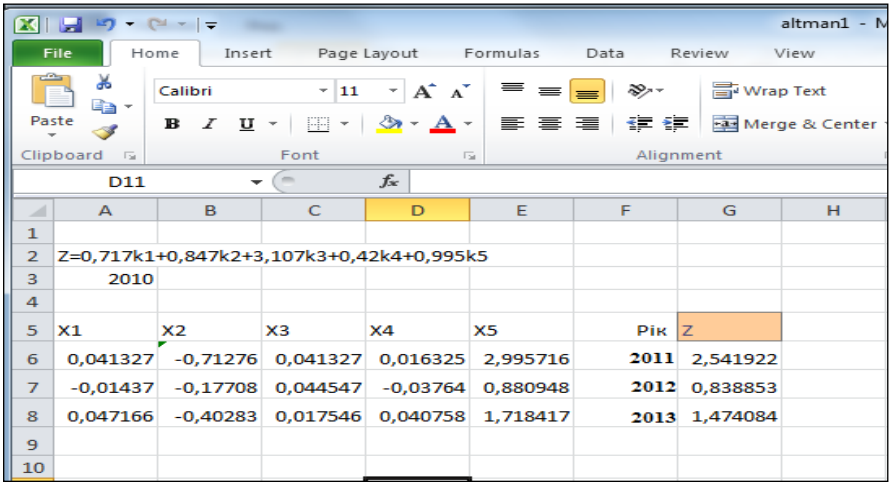


Рис. 2.11. Результати обчислень Z – показника моделі Альтмана.

Так коефіцієнт забезпеченості власними коштами КЗ. в 2013 році склав - 0,28 що нижче рекомендованої норми 0,1. З цього можна зробити висновок, що підприємство не забезпечено, в необхідному обсязі, власними коштами.

Коефіцієнт автономії КАв 2013 році значно нижче норми, за розрахунками він склав 0,05 тоді як норма для коефіцієнта автономії - більше 0,6.

Коефіцієнт маневреності КМ власного капіталу в 2013 році - 4,42, тобто також поза рекомендованої норми 0,5.Коефіцієнт фінансової стійкості КС в 2013 році він склав 0,98, тобто значно відхиляється від норми по якій він повинен бути менше 0,6.

Коефіцієнт покриття (поточної ліквідності) КЛв 2012-2013 рр.. коефіцієнт набагато вище норми і становив відповідно 44,9 і 43,9. Однак в 2011 році він був нижче рекомендованої норми і склав 0,5.

На основі відхилення від норми на 4 з 5 наведених коефіцієнтів можна зробити висновок про те, що підприємство є фінансово нестійким. З цього випливає, що фактор фінансової нестійкості несе високу небезпеку підприємству.

Під фінансовою небезпекою розуміють небезпеку, що виникає під час здійснення фінансового підприємництва чи фінансових угод. До фінансової небезпеки належать: валютна небезпека; кредитна небезпека; інвестиційна небезпека.

Для підприємства є актуальними кредитна та інвестиційна небезпеки.

Для оцінки кредитної небезпеки обчислимо вірогідність уникнення банкрутства при отриманні кредиту. За теоретичну базу обрана нерівність Чебишева:

$$P(|X - m| > \delta) \le V / \delta^2 = \sigma^2 / \delta^2,$$

де m — математичне сподівання випадкової величини X,

V— варіація деякої випадкової величини R,

σ —дисперсія,

δ — заданий допуск.

$p = V / \delta^2 \leq 1$, оскільки величина ймовірності не перевищує одиниці[1].

Розглянемо сценарій один з проектів внутрішнього розвитку, для здійснення якого необхідно узяти кредит. Банк надає кредит підприємству під відсоток r_s= 17% на впровадження нових технологій під заставу нерухомості. За даними бізнес плану проекту норма сподіваних прибутків від вкладень m_0 = 18%. При цьому експерти оцінюють, що ризик, пов'язаний з коливанням сподіваних прибутків, становить 3%. Ймовірність того, що підприємство не зможе повернути свій борг і позбудеться своєї нерухомості, це ймовірність того, що випадкова величина R набуде свого значення, яке відповідає умові $R < r_s$,або– $(R – m) > m – r_s$.Отже, одержимо:

$$P(R < r_s) = P(– (R – m) > m – r_s)$$
$$\leq P(|R — m| > m — r_s) \leq (V/(m – r_s))^2.$$

Звідси маємо, що шанс збанкрутувати не перевищує величини $V/(m – r_s)^2$. Коли задані умови (гіпотези) виконуються, то для того щоб шанс збанкрутувати був не більшим, ніж 1/9, достатньо виконати умову (правило трьох сігм)$V \leq 1/9(m – r_s)^2$, або $m \geq r_s + 3\sigma$.

Оцінимо рівень сподіваних прибутків, щоб уникнути банкрутства. Оскільки r_s = 20%, σ = 3%. Скориставшись правилом трьох сігм, одержимо: m ≥17% + 3*3% = 26%,тобто рівень (норма) сподіваних прибутків повинен бути не меншим, ніж 26% щоб шанс підприємства збанкрутувати був не більшим, ніж 1/9 при отриманні кредиту.

Оскільки норма сподіваних прибутків проекту $m_0 \leq m$, то отримання кредиту буде супроводжуватися невиправдано високим ризиком. Фактор інвестиційної небезпеки також є актуальним для підприємства. Під цією небезпекою слід розуміти різноманітні суттєві небезпеки, що можуть виникнути при використання коштів на розвиток підприємства.

Вибір перспективних проектів розвитку підприємства є вкрай важливим для діяльності підприємства і його стабільного росту. Фактор інвестиційної небезпеки був оцінений експертним методом з ви-

[1]Вітлінський В. В., Верченко П. І. Аналіз, моделювання та управління економічним ризиком: Навч.-метод. посібник для самост. вивч. дисц. – К.: КНЕУ, 2000 – 15 с.

користанням опитувальників на основі попередніх даних звітності про використання коштів на розвиток підприємства як фактори високої небезпеки. Нижче наведена табл. 2.6 оцінених факторів небезпеки підприємства.

Таблиця 2.6

Оцінка факторів небезпеки підприємства

Назва фактору небезпеки	Можливі наслідки	Норматив ний показник	Числова оцінка або зона небезпеки	Лінгвістична оцінка
Зниження обсягів реалізації	Зниження прибутку,низька ефективність праці	Зона допустимої небезпеки	Зона допустимої небезпеки	Низька небезпека
Зношення основних фондів	Зниження якості продукції, поломки обладнання	<50 - 55%.	= 11,62%	У безпеці
Підвищення закупівельної ціни на зерно	Збільшення витрат виробництва		Зона критичної небезпеки	Висока небезпека
Втрата ділової репутації	Зниження попиту на продукцію і послуги		Зона допустимої небезпеки	Низька небезпека
Недобросовісна діяльність контрагентів	Втрата капіталу, зрив поставок або виробництва продукції		Зона допустимої небезпеки	Низька небезпека
Назва фактору небезпеки	Можливі наслідки	Норматив ний показник	Числова оцінка або зона небезпеки	Лінгвістична оцінка
Кредитна	Банкрутство через отримання кредиту	m ≥ 26%	m_0= 18%	Висока небезпека

Продовження таблиці 2.6

Інвестіційна	Втрата капіталу, знецінення реальної вартості капіталу, зниження ліквідності активів		Зона критичної небезпеки	Висока небезпека
Фінансової нестійкості	Банкрутство, втрати репутації, партнерів, неплатоспроможність	$К_З$> 0,1 $К_А$> 0,6 $К_М$>0,5 $К_С$< 0,6 $К_Л$< 2	$К_З$= 0,28 $К_А$ = 0,05 $К_М$= -4,42 $К_С$= 0,98 $К_Л$ = 43,9	Висока небезпека
Використання неякісної сировини	Зниження якості продукції, поломки обладнання		Зона допустимої небезпеки	Низька небезпека
Простій устаткування	Зниження обсягів виробництва	Q(30) < 0,35	Q(30)=0,3	Низька небезпека

Наведена вище оцінка факторів може бути використана на практиці.

2.3. Методи управління безпекою підприємства

Управління безпекою покликане забезпечити оптимальне для підприємця співвідношення прибутку та безпеки, його прийнятний (допустимий) рівень. Для цього слід провести збір, обробку та аналіз інформації про зовнішнє середовище, про внутрішні показники фінансової, виробничої, комерційної діяльності фірми в минулому та в поточному періоді, здійснювати прогнози щодо майбутнього[1].

Інформація швидко старіє, а тому суб'єкт прийняття рішення повинен оперативно, динамічно реагувати на її надходження, водночас оцінюючи якість інформації й здійснюючи її моніторинг. Обираючи стратегію та тактику управління небезпекою, підприємець повинен

[1] Румянцев В., Путятина Л. Методологические проблемы адаптации товаропроизводителей к рынку // Проблемы теории и практики управления. − 1994. − №6. − С. 69-73.

дотримуватись таких основних принципів: недоцільно ризикувати більшим заради меншого; недоцільно ризикувати більше, ніж це дозволяють власні засоби; необхідно здійснювати прогноз відносно можливих наслідків небезпеки.

Складові процесу управління безпекою визначаються залежно від сфери діяльності фірми, притаманних їй ризиків, наявних ресурсів, особистої майстерності, професіоналізму, схильності до ризику управлінця (суб'єкта прийняття рішення). Для підприємства, що досліджувалося, запропоновано вживати процес управління безпекою про який згадує В.В. Вітлінський[1]. Узагальнено процес управління безпекою представлено у вигляді блок-схеми на рис.2.12.

В результаті ґрунтовного якісного та кількісного аналізу підприємець, спираючись на отримані дані, обирає один із засобів або суперпозицію засобів управління безпекою: уникнення; попередження; прийняття (збереження чи навіть збільшення); зниження ступеня безпеки (оптимізація). Доцільно розглянути ці засоби.

Уникнення ризику означає просте ухилення від певного заходу, обтяженого надмірним (катастрофічним) ризиком. Однак уникнення ризику для підприємця нерідко означає відмову від прибутку, а це пов'язано з небезпекою невикористаних можливостей. Підприємство може уникнути кредитної небезпеки відмовившись від отримання кредитів, які будуть супроводжуватися невиправдано високим ризиком підприємств.

Попередження небезпеки – це досить ефективний засіб, який однак лише в окремих випадках дає змогу зменшити (уникнути) небезпеку в управлінні. На підприємстві створюються безпечні умови праці і проводиться інструктаж робітників з техніки безпеки праці для попередження травм, для попередження травматизму при роботі. Для попередження цієї небезпеки використання неякісної сировини створена лабораторія, ефективність роботи якої становить 98%, тобто існує ймовірність порядку 2%, що неякісна сировина все-ж буде використовуватися.

Для попередження небезпеки втрати ділової репутації доречно приймати відповідні управлінські рішення, спрямовані на усунення зайвого впливу зовнішніх і внутрішніх факторів репутаційного ризику. Наприклад, зміна політики в області підбору і розстановки кадрів,

[1] Вітлінський В. В., Верченко П. І. Аналіз, моделювання та управління економічним ризиком: Навч.-метод. посібник для самост. вивч. дисц. – К.: КНЕУ, 2000 – 15 с.

у першу чергу керівників служб, посилення вимог до окремих посадах; більш ретельний розподіл повноважень між органами управління, посадовими особами та службами підприємства; проведення внутрішніх навчальних заходів з працівниками підрозділів, зайнятих обслуговуванням клієнтів (з метою уникнення відпливу клієнтури).

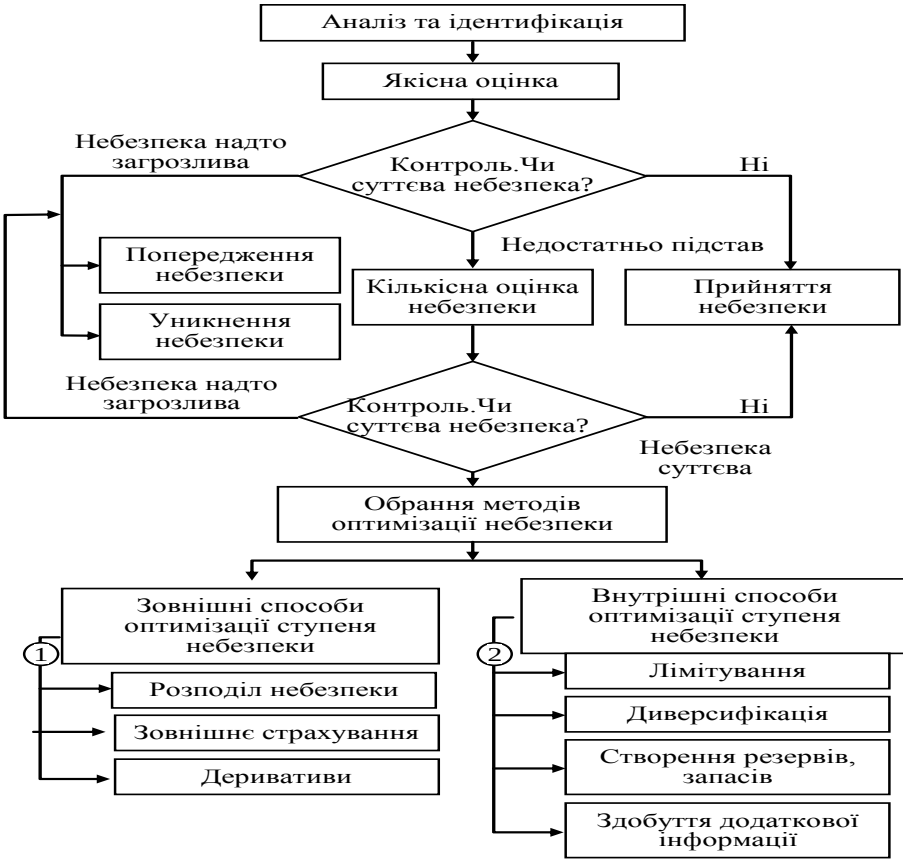


Рис. 2.12. Узагальнена блок-схема процесу управління безпекою

Сюди слід віднести організацію відвідин працівниками зовнішніх семінарів; вдосконалення системи внутрішнього контролю, у тому числі в галузі запобігання легалізації доходів, отриманих незаконним

шляхом, в першу чергу методів ідентифікації клієнтів; організацію роботи із засобами масової інформації, інших форм взаємодії з громадськістю.

Щоб попередити небезпеку пов'язану з фактором недобросовісної діяльності контрагентів, ТОВ доцільно проводити аналіз фінансово-господарської діяльності контрагентів за допомогою бухгалтерської звітності та уникати взаємодії з ненадійними, а також з такими контрагентами, які викликають підозру або відмовляються надавати про себе інформацію, по якій можна провести цей аналіз.

Прийняття ступеня небезпеки – це залишення небезпеки за підприємцем, тобто на його відповідальність. Вкладаючи засоби в певну справу, підприємець має бути впевненим, що є можливості покриття можливих збитків або ж що вони йому не загрожують**.**

Наприклад, якщо підприємство вважає, що майбутні коливання цін на пшеницю 1 класу будуть сприятливими, то воно може погодитися на прийняття практично будь-якої небезпеки щодо цієї пшениці без спроб застрахуватися від збитків (на певний період).

У той же час підприємство може застрахуватися від ризику несприятливих коливань цін на іншу пшеницю, де ймовірність збитків є значно вищою, якщо підприємство немає коштів на придбання пшениці. Оскільки фактор підвищення цін на зерно несе високу небезпеку для економічної безпеки підприємства, рекомендується розробити модель прогнозування ціни на зерно та управління сировинними запасами.

Небезпека простою устаткування при поломці на 2013 рік на підприємстві несуттєва, оскільки коефіцієнт зношення основних фондів в цьому році становив 11,62% (норма по галузі – не більш 50-55%). Підприємство вживає необхідних заходів щодо технічного забезпечення обладнання та своєчасної модернізації та купівлі нового, тому рекомендовано прийняти ступень цієї небезпеки.

Зниження ступеня небезпеки може здійснюватися або шляхом його передачі, тобто зовнішніми засобами, або за допомогою внутрішніх ресурсів (самострахування), розподілу фінансових, матеріальних коштів з урахуванням принципів лімітування, диверсифікації, тобто

внутрішніми засобами. До внутрішніх засобів зниження небезпеки відносять також здобуття додаткової інформації з цього питання[1].

При використанні зовнішніх засобів зниження ступеня небезпеки передача її здійснюється або шляхом його розподілу, або через механізм зовнішнього страхування. Розподіл ризику полягає в тому, щоб, наприклад, покласти певну частку відповідальності за ризик на того співучасника реального інвестиційного проекту, який здатний його контролювати краще від інших. Передача ризику може здійснюватися також шляхом укладення ф'ючерсного контракту. Ф'ючерси дають змогу передавати ризик несприятливої зміни цін у майбутньому протилежній стороні торговельної угоди.

Найпоширенішою формою передачі ризику є страхування. Суть зовнішнього страхування ризику виражається в тому, що інвестор ладен відмовитися від частини доходів аби уникнути ризику, тобто він взмозі заплатити за зниження рівня ризику до нуля.

Якщо поняття вартість ризику розглядати як суму фактичних збитків підприємця від реалізації цього ризику і витрат на відшкодування таких збитків та їх наслідків, то страхування дає змогу зменшити цю суму (вартість страхового ризику) до розміру страхової премії.

Сьогодні витрати на страхування підприємств у розвинутих промислових країнах варіюють від 1 до 20% обсягу щорічних продаж залежно від галузі, місцезнаходження фірми тощо. Менеджер підприємства може передати на утримання страховій компанії такі види ризиків:

ризик пошкодження/знищення майна внаслідок пожежі, стихійного лиха, технологічної аварії тощо; ризик повної/часткової (тимчасової) втрати працездатності співробітником підприємства під час виконання службових обов'язків внаслідок нещасного випадку; ризик, пов'язаний з необхідністю відшкодування збитків, що їх зазнала третя особа внаслідок певних дій (відсутності необхідних заходів) з боку підприємства, його співробітників, а також ризик збитків, спричинених даному підприємству некваліфікованими (нечесними) діями його співробітників; фінансово-комерційні ризики, які можуть реалізуватися у вигляді недоотримання прибутку, збільшення періоду кругообігу коштів тощо в результаті дії зовнішніх непередбачуваних чинників.

---

[1] Ковальчук К.Ф. Методи інтелектуальної підтримки прийняття економічних рішень // Автореф. дис. д-ра екон. наук. — К.: НАН України ІК ім. В.М.Глушкова, 1996. — 32с.

Слід підкреслити, що страхування компенсує збитки (їх частину) у грошовій формі, а не відшкодовує товарно-матеріальні цінності, а тому не може повністю усунути небезпеку затримки відтворювального процесу. У той же час в рамках дії превентивної функції страхування ймовірність реалізації небезпеки може бути зменшена, наприклад, в результаті встановлення страховиком протипожежного обладнання на підприємстві, що страхує в нього своє майно. Інформація, що її отримує потенційний страхувальник під час оцінки ризику страховиком, може бути використана для прийняття подальших рішень щодо управління ризиком (наприклад, слугувати сигналом, що роботи в цьому напрямі слід припинити, що цей вид майна абсолютно небезпечно зберігати на даній виробничій дільниці). До методів, що за своєю суттю близькі до страхування, можна віднести також деривативи (опціони, ф'ючерси, свопи тощо).

Розглянемо внутрішні способи зниження ступеня ризику.

Лімітування передбачає обмеження потоків (грошових, товарних, кредитних, інвестиційних), спрямованих у зовнішнє (по відношенню до підприємства) середовище. Підприємство може застосовувати цей засіб під час продажу товарів у кредит, наданні позичок, при прийнятті рішень щодо визначення обсягу коштів, які спрямовуються на інвестування.

Диверсифікація є процес розподілу інвестованих коштів між різними об'єктами вкладання, які безпосередньо не пов'язані між собою. На принципі диверсифікації може базуватися діяльність вкладення грошей у проекти внутрішнього розвитку. Диверсифікація дає змогу уникнути частини небезпеки при розподілі капіталу між різноманітними видами діяльності. Так вкладення грошей у декілька проектів внутрішнього розвитку замість одного збільшує ймовірність одержання ним середнього доходу і знижує рівень небезпеки.

Створення резервів, запасів на покриття ймовірних непередбачуваних витрат у майбутньому також є внутрішнім засобом зниження небезпеки, свого роду самострахуванням. Це дозволяє оперативно усувати тимчасові ускладнення у виробничій, фінансово-комерційній діяльності.

Для підприємства створення власних грошових, товарно-матеріальних резервів є альтернативою страхуванню і доцільне тоді, коли вартість майна, що наражається на певну небезпеку, відносно невелика порівняно з майновими та фінансовими параметрами усього проекту. Самострахування шляхом резервування коштів також може

застосовуватись відносно однотипного обладнання, майна підприємства, коли ймовірність пошкодження незначна.

Здобуття додаткової інформації є одним з важливих способів щодо зниження небезпеки. Під час використання неточних економічних даних виникає питання щодо доцільності їх уточнення.

Що стосується планованих заходів, особливо інноваційних проектів, то постає питання: чи необхідно терміново почати їх впровадження, чи є сенс провести ще якийсь додатковий експеримент для уточнення економічних показників.

З одного боку, додатковий експеримент дозволив би знизити економічну небезпеку, що обтяжує певний інноваційний проект, зменшити можливі збитки. Але, з іншого боку, експеримент, в свою чергу, пов’язаний з певними затратами та збитками, і якщо впровадження інноваційного проекту відкладається, то економічні збитки збільшуються. Вони особливо великі у разі проведення довгострокового експерименту. У цьому випадку впровадження заходів і одержуваний в результаті цього економічний ефект відсуваються. Отже, для оцінки доцільності добування додаткової інформації необхідно порівняти економічні результати обох варіантів. Природно, що коли б у підприємця є більш повна інформація, він може зробити кращий прогноз й знизити ступінь небезпеки.

Зниження ступеня небезпеки фінансової стійкості може здійснюватись або шляхом його передачі, тобто зовнішніми засобами, або за допомогою внутрішніх ресурсів (самострахування), розподілу.

Можливі стратегії зниження небезпеки втрати фінансової стійкості: факторинг, банківський кредит, податковий кредит, самострахування. Особливу увагу приділено самострахування ринкової діяльності підприємства як ефективного методу демпфування сукупної небезпеки і зниження загрози банкрутства.

Можливим методом самострахування є формування в пасивах підприємства резерву грошових коштів, що дозволяє покривати недолік виробничого капіталу при несприятливих змінах ринкової кон'юнктури, пов'язаних з негативним впливом факторів макроекономічного оточення. Отже, вважається за необхідне розробити модель розрахунку оптимального резерву грошових коштів підприємства.

Оскільки фактор інвестиційної небезпеки несе високу небезпеку для підприємства (під цією небезпекою слід розуміти різноманітні суттєві небезпеки, що можуть виникнути при використання коштів на розви-

ток підприємства), то управління інвестиційною небезпекою і зниження інвестиційної небезпеки повинно стати одним із головних завдань системи управління економічної безпеки підприємства (табл. 2.7).

Таблиця 2.7

Пропозиції щодо управління небезпекою підприємства

Назва фактору небезпеки	Можливі наслідки	Оцінка	Пропозиції щодо управління небезпекою
Зниження обсягів реалізації	Зниження прибутку, низька ефективність праці	Низька небезпека	Прийняття ступеня небезпеки
Зношення основних фондів	Зниження якості продукції, поломки обладнання	У безпеці	Проводити аналіз зносу основних фондів щороку
Підвищення закупівельної ціни на зерно	Збільшення витрат виробництва	Висока небезпека	Розробити модель прогнозування ціни на зерно та управління сировинними запасами підприємства
Втрата ділової репутації	Зниження попиту на продукцію і послуги	Низька небезпека	Попередження небезпеки шляхом прийняття рекомендованих управлінських рішень
Недобросовісна діяльність контрагентів	Втрата капіталу, зрив поставок або виробництва продукції	Низька небезпека	Щоб попередити небезпеки пов'язану з фактором недобросовісної діяльності контрагентів підприємства може проводити аналіз фінансово-господарської діяльності контрагентів
Кредитна	Банкрутство через отримання кредиту	Висока небезпека	Підприємство може уникнути кредитної небезпеки відмовившись від отримання кредитів, які будуть супроводжуватися невиправдано високим ризиком.

Продовження Таблиці 2.7

Назва фактору небезпеки	Можливі наслідки	Оцінка	Пропозиції щодо управління небезпекою
Інвестиційна	Втрата капіталу, знецінення реальної вартості капіталу, зниження ліквідності акт.	Висока небезпека	Розробити модель інвестиційної стратегії підприємства
Фінансової нестійкості	Банкрутство, втрати репутації, неплатоспроможність	Висока небезпека	Користуватися наведеною моделлю Альтмана, проводити аналіз фінансової стійкості підприємства. Запропоновано розробити модель розрахунку оптимального резерву грошових коштів підприємства
Використання неякісної сировини	Зниження якості продукції, поломки обладнання	Низька небезпека	Для попередження створена лабораторія, ефективність роботи якої - 98%, тобто існує ймовірність порядку 2%, використовування неякісною сировини
Простій устаткування при поломці	Зниження обсягів виробництва	Низька небезпека	Попередження поломок обладнання проводячи оцінку ймовірності відмови обладнання використовуючи аналіз виживання.

Обираючи інвестиційну стратегію підприємства доцільно враховувати, що основувати її лише на можливих прибутках небезпечно, а лише на факторі небезпеки – нераціонально, тому що це може перешкодити розвитку підприємства.Відповідно до цього для формування інвестиційної стратегії підприємства з можливо більшою очікуваною прибутковістю і можливо меншою небезпекою пропонується обрати двокритеріальну задачу Марковіца, на основі якої можна розробити відповідну модель.

Таким чином, в результаті проведеного аналізу факторів небезпеки підприємства стало відомо, що в ході фінансового-господарської діяльності (ФГД) підприємство зустрічається з наступними небезпеками ЕБ підприємства: інвестиційна; підвищення закупівельної ціни на товари; фінансової нестійкості; кредитна; зносу основних фондів; недобросовісної діяльності партнерів і конкурентів; використання неякісної сировини; простою устаткування при поломці; зниження обсягів реалізації; втрата зовнішніх ринків збуту.

2.4. Визначення детермінантів, які сприяють здійсненню рейдерських атак на підприємство

У вітчизняній економічній науці проведено низку досліджень теоретико-прикладного характеру, що прямо або опосередковано торкалися питань протидії рейдерським атакам. Запропоновані науковцями висновки та конструктивні пропозиції дозволили уточнити окремі теоретичні поняття, спростувати низку консервативних догм, розвіяти ілюзії щодо рівня, стану та динаміки цього явища в Україні.

Проте, ставши своєрідним епіцентром прикладання дослідницьких зусиль, проблема протидії рейдерству й дотепер містить певну кількість нерозглянутих питань, а деякі розроблені концепції, як виявилось, не мають чіткої практичної перспективи. Численні спроби реально впровадити напрацьовані наукою рекомендації в розробку цільових програм зниження рівня рейдерських захоплень, як втім і корумпованості у галузях економіки та державного управління сферою господарювання, в нашій державі або її окремих регіонах, підтвердили, що характер отриманих науковцями відомостей, через фрагментарність та безсистемність, не дозволяє їх ефективно використовувати для вирішення конкретних практичних завдань.

Задовольнити нагальну потребу в побудові ефективного механізму протидії протиправним захопленням здатен, на нашу думку, лише такий підхід, який би враховував у єдиному контексті усі чинники господарської сфери, які так або інакше сприяють рейдерським захопленням. При цьому вказані чинники повинні розглядатися як загрозливі елементи єдиної системи факторів, що уможливлюють рейдерське захоплення.

Річ у тому, що безпека підприємства не означає його функціонування без загроз. Різноманітні суб'єктивні та об'єктивні фактори можуть перешкоджати його функціонуванню, розвитку, руйнувати структуру ззовні або зсередини. Для підприємницької діяльності вони не лише неминучі, але змушують підприємство удосконалювати систему захисту власних інтересів від зовнішнього або внутрішнього впливу, зокрема від рейдерських атак. В цьому сенсі наріжним каменем наукової дискусії має стати, на нашу думку, структурно-системне бачення комплексу зазначених факторів як квінтесенції прогнозування потенційних загроз рейдерських захоплень. Функціонування підприємства ускладнюється постійною зміною факторів зовнішнього й внутрішнього середовища, тому результати діяльності суб'єкта господарювання важливо проводити на комплексно-динамічній основі. Констатуючи необхідність широкомасштабного висвітлення різноманітних детермінантів досліджуваного явища, слід обрати й адекватне методологічне підґрунтя, яким здатен виступити системний аналіз.

В сучасному розумінні системний аналіз – один з фундаментальних принципів усебічного дослідження соціальних явищ та процесів як певної цілісності, в якій кожен з елементів структури має специфічне призначення, а й відповідно й зовнішній прояв. Вважаємо, що тріумфальна хода системно-структурного аналізу в науковому середовищі й пояснюється саме тією гнучкістю, з якою він може бути використаний для потреб пізнання тих або інших об'єктів, у тому числі й системи чинників, що уможливлюють рейдерське захоплення.

У вітчизняній економічній теорії та теорії економічної безпеки системний підхід, незважаючи на очевидний пізнавальний потенціал та беззаперечну користь, здобуту суміжними галузями знань через його застосування, використовується дослідниками не часто. Переважна більшість науковців продовжує віддавати перевагу усталеним, перевіреним та традиційним для економічної науки підходам: інституційному, біхевіоральному та інструментальному.

Прибічники інституціоналізму в теорії економічної безпеки зосереджують увагу на певній державній установі, службі або внутрішньому підрозділі підприємства, які протидіють рейдерству, розглядаючи їх ізольовано як від аналогічних служб та інституцій, так і від самого протиправного середовища, якому цим інституціям належить протистояти. Подібна ізоляція призводить до перебільшення ролі певної інституції у справі протидії рейдерству, що часто не відповідає

дійсності, та, врешті-решт, спричиняє ігнорування можливостей системної взаємодії, веде до нераціонального використання сил та засобів забезпечення безпеки від рейдерських захоплень, розпорошення ресурсів у протидії цьому явищу тощо.

Біхевіоральний (поведінковий) підхід у дослідженнях з питань протидії рейдерству зорієнтований переважно на висвітлення механізму протиправної діяльності й часто обмежується лише вивченням особливостей протиправної поведінки досліджуваного виду. Маючи безсумнівну користь, такий підхід менш придатний у стратегічному вимірі та довгостроковій перспективі, адже через постійне удосконалення рейдерами форм і методів протиправної діяльності, а також трансформацію суспільних відносин, це не приносить очікуваних результатів у справі оптимізації системи протидії протиправним захопленням та поглинанням. Узагальнення вже викритих рейдерських схем в межах біхевіорального підходу за своєю гносеологічною природою є звичайною ретроспективою, що не враховує, по-перше, мобільності, яка притаманна сучасній злочинності економічної спрямованності, та, по-друге, залишає поза увагою протиправну поведінку з високим рівнем латентності. Негативними сторонами подібного підходу є надмірна залежність підприємств від шаблонів та розробка слабоскоординованих рекомендацій протидії рейдерству.

Прибічники інструментального підходу часто зосереджуються лише на певному методі протидії рейдерським атакам або організаційному заході забезпечення безпеки, віддаляючись таким чином від принципу комплексності в застосуванні засобів і заходів безпеки. Такий підхід, до речі, пропонується у роботі В.Л. Диканя та М.В. Куркіна «Роль конкурентної розвідки у боротьбі з недружніми поглинаннями в Україні», в якій автори у протидії рейдерству надають перевагу конкурентній розвідці — постійному процесу 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[1].

[1] Дикань В.Л. Куркін М.В. Роль конкурентної розвідки у боротьбі із недружніми поглинаннями в Україні // Вісник економіки транспорту і промисловості. − 2009. – №28. − С. 32.

Шніт А.В. у роботі «Про посилення законодавчої бази антирейдерської спрямованості»[1] віддає перевагу правовим засобам та інструментам протидії рейдерству. Проте такі підходи, вважаємо, ведуть до штучного розділення мети певного заходу (оптимізація кадрової роботи, конкурентна розвідка або удосконалення співпраці з контрагентами) чи застосування певного методу забезпечення безпеки від загальної мети – системної протидії рейдерству, а інколи навіть і протиставляючи їх. Дослідники, що віддають перевагу інструментальному підходу, часто приречені на розв'язання лише дріб'язкових (у порівнянні з масштабами усієї системи забезпечення економічної безпеки) завдань, залишаючи невирішеними загальні питання стратегії протидії протиправним захопленням і поглинанням.

Багатьох із зазначених методологічних недоліків структурно-системний підхід у контексті протидії рейдерству позбавлений, оскільки націлює на більш масштабне та широке бачення тих проблемних аспектів, які характеризують наявний стан функціонування підприємства, сприяє усуненню пізнавальних бар'єрів на шляху визначення оптимальної моделі господарської діяльності підприємства.

З іншого боку, застосування структурно-системного аналізу, який оперує поняттями «структура», «система», «елемент», «функція» потребує адекватної уваги та екскурсу до зазначених наукових категорій, вимагає опанування ними та їх адаптації відповідно до теми дослідження.

У загальнотеоретичному аспекті термін «система» традиційно визначається як наявність об'єднаної єдиними засадами певної цілісності. Відповідно до тлумачного словника, система – це «сукупність яких-небудь елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням», або «будова, структура, що становить єдність закономірно розташованих та функціонуючих частин»[2]. У буквальному перекладі з грецької мови «система» означає «ціле, складене з частин».

У світлі сучасної науки система це не лише механічний набір елементів, не лише їх звичайна комбінація, а така їх сукупність, яка характеризується їх структурованою взаємозалежністю. «Система, - вважає С. Е. Віцин, - така структурно-функціональна єдність елемен-

[1] Шніт А.В. Про посилення законодавчої бази антирейдерської спрямованості // Європейські перспективи. – 2011. - № 1. – Ч.1. – С. 117-121.

[2] Великий тлумачний словник сучасної української мови / Укл. і голов.ред. В.Т. Бусел. – К., 2002. – С.1126.

тів, цілісна єдність структурно розчленованих, але взаємопов'язаних елементів, які реалізують певні функції в умовах конкретного зовнішнього середовища[1]».

З урахуванням наведеного визначення, яке варто прийняти як базове, зазначимо, що розгляд будь-якої системи без урахування функціонального аспекту не відображає в повній мірі її сутності й спрямованості. З цих міркувань не можна оминути увагою й той зміст, який вкладається в категорію «функція». Вказаний термін має латинське походження («functio») і у перекладі означає «здійснення», «виконання». У тлумачному словнику, наприклад, поняття «функція» визначається як робота кого-небудь або чого-небудь, обов'язок, коло діяльності, призначення, роль[2]. Взагалі ж, зміст цього поняття є різноманітним і багатогранним, оскільки знаходить використання в різноманітних науках та галузях знань. У суспільно-політичному вимірі, на нашу думку, більш прийнятним вбачається розглядати функцію як «роль, яку певний соціальний інститут або соціальний процес виконує відносно потреб суспільної системи більш високого рівня організації або інтересів класів, які її складають, соціальних груп та індивідів»[3].

З'ясувавши ці базові для структурно-системного підходу категорії, варто визначитися з напрямами подальшого наукового пошуку в контексті визначення цілісної єдності розрізнених, але взаємопов'язаних та функціонально наближених факторів, які сприяють та уможливлюють здійснення рейдерських атак. Вважаємо, що висвітлення системи зазначених чинників передбачає одержання відповідей на наступний блок питань:1) які внутрішні та зовнішні фактори впливають на стан захищеності підприємства від рейдерських захоплень? 2) яким чином керувати ризиками реалізації планів рейдерського захоплення підприємства та впливати на їх мінімізацію? 3) якими є шляхи удосконалення протидії рейдерству з урахуванням визначених факторів та чинників?

Питання про систему факторів, які сприяють та уможливлюють здійснення рейдерських атак, займаючи центральне, провідне місце в презентованому дослідженні, є одночасно й першим ускладненням,

---

[1] Вицин С.Е. Системный подход и преступность / Академия МВД СССР. – М., 1980. - С. 13.

[2] Великий тлумачний словник сучасної української мови / Укл. і голов.ред. В.Т. Бусел. – К., 2002. – С.1335.

[3] Большая Советская Энциклопедия. Гл.ред. А.М. Прохоров. Изд. 3-е. В 30 т. Т. 28. – М.: Советская Энциклопедия, 1978. – С. 138.

яке зустрічається на цьому шляху, оскільки спеціальна література з досліджуваного питання не містить чіткого та зрозумілого переліку цих чинників або детермінантів. Існування такої розбіжності у визначенні чинників, ознак та видів складових економічної безпеки підприємства створює труднощі у встановленні напрямів загроз та небезпек, подвійне урахування або неврахування окремих напрямів. Як наслідок – несвоєчасна реакція та послаблення конкурентної позиції підприємства, його економічної безпеки за всіма напрямами.

Надаючи відповідь на перше з поставлених питань, варто акцентувати увагу на тому, що об'єктом рейдерської атаки може стати будь-яке підприємство, що володіє цінними активами, стійкою позицією на ринку, а також відзначається високою рентабельністю та конкурентоспроможністю.

Водночас, окремі підприємства, допускаючи ряд помилок під час стратегічного планування, а також оперативного управління фінансово-господарською діяльністю самі наражають себе на небезпеку недружнього поглинання. Адже чим менше зусиль рейдеру необхідно докласти для організації недружнього поглинання, тим вищою буде прогнозована рентабельність рейдерської атаки, і тим більш привабливішими стануть активи підприємства для рейдера[1].

Отже, вкрай потрібним є визначення системи детермінантів рейдерства в Україні, які дозволять виробити адекватні заходи з протидії їх впливу та забезпечити адресність в їх мінімізації та нейтралізації.

Ідентифікація факторів екзо- та ендогенного середовища суб'єкта господарювання стає необхідною передумовою побудови і створення цілісної картини економічної безпеки підприємства від рейдерських захоплень. У такій площині система факторів впливу має розглядатись не як детальний перелік її елементарних частин, а як структурована сукупність взаємопов'язаних компонентів[2].

Поширення рейдерства в Україні в дечому зумовлено приватизаційним процесом, який відбувався в Україні останніми роками. Здебільшого приватизація суб'єктів господарської діяльності проводилася не цілком законним шляхом. Сумнівна передісторія приватизації об'є-

[1]Вірченко В.В. Передумови та методи недружнього поглинання суб`єктів господарювання / В.В. Вірченко // Теоретичні та прикладні питання економіки. – 01/2011. – Вип.24 . – С. 236-244.

[2] Яременко О.Ф. Аспекти побудови паспорта загроз підприємства // Вісник Хмельницького національного університету. – 2011. - №2. – Т.1. – С. 15-16.

ктів, практично повна відсутність ринкової інфраструктури сприяла появі незадоволених міноритарних акціонерів, які для рейдерів можуть стати дієвим інструментом захоплення підприємства.

Детермінантами, що визначають розвиток сфери переділу власності, обумовлюють такий розвиток національного ринку злиття і поглинань, для якого характерна гіпертрофована роль інституту рейдерства, Ю.С. Нєхорошев називає комплекс елементів, зокрема: своєрідність економічного розвитку, особливості національного менталітету, недосконаліть ринкових інструментів перерозподілу власності, відсутність регулярної ринкової оцінки ліквідних активів підприємств, нечітка і непрозора система реєстрації прав власності, зростання корпоративних конфліктів, пов'язаних з недосконалістю корпоративного законодавства[1].

Вважаємо, що в запропонованих авторами концепціях йде мова про об'єктивні чинники, які, здебільшого, не контролюються підприємством. У той же час не менш важливим є уявлення про внутрішні, так звані суб'єктивні чинники, що уможливлюють рейдерське захоплення. В цьому сенсі становить інтерес позиція В.В. Вірченко та В.В. Вірченко[2], які серед основних передумов недружнього поглинання визначають такі фактори:

1. Відсутність контрольного пакету, а також недостатній рівень консолідації статутного капіталу підприємства. Наявність значної кількості міноритарних акціонерів надає можливість рейдеру придбати у них акції на вигідних для них умовах і отримати у такий спосіб пакет акцій, що дозволяє скликати позачергові збори акціонерів або включати питання на порядку денного.

2. Наявність у відкритому доступі конфіденційної інформації щодо акціонерів та фінансово-господарської діяльності підприємства. З одного боку акціонерні товариства зобов'язані оприлюднювати наступну інформацію: статут, засновницький договір, свідоцтво про державну реєстрацію; інформацію про загальні збори, наглядову раду,

---

[1] Нехорошев Ю.С. Экономика России в XXI веке: Сборник научных трудов VII Все-российской научно-практической конференции «Фундаментальные проблемы модернизации экономики России» / Под ред. Г.А. Барышевой, Л.М. Борисовой; Национальный исследовательский Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2010. – С. 153-156.

[2] Вірченко В.В. Передумови та методи недружнього поглинання суб`єктів господарювання / В. В. Вірченко // Теоретичні та прикладні питання економіки. – 01/2011. – Вип.24 . – С. 236-244.

виконавчий орган та ревізійну комісію, інші внутрішні документи; інформацію про філії; кодекс корпоративного управління; протоколи загальних зборів акціонерів; висновки ревізійної комісії та незалежного аудитора; річну фінансову звітність; звітність, що подаються державним органам; проспект емісії, свідоцтво про державну реєстрацію випуску акцій та інших цінних паперів.

З іншого, на підприємстві слід обов'язково дотримуватися норм інформаційної та економічної безпеки, без необхідності та відповідних правових підстав не розголошувати інформацію щодо активів підприємства, власників підприємства та його ділових партнерів. Адже на основі отриманої інформації про підприємство рейдер може фальсифікувати документи, увійти у змову з міноритарними акціонерами і отримати у такий спосіб контроль над його активами[1].

3. Порушення підприємством законодавства у процесі свої діяльності. Зазвичай порушення пов'язані з недотриманням норм і стандартів корпоративної поведінки, Господарського кодексу, Закону «Про акціонерні товариства», трудового і екологічного законодавства. Наявність порушень в діяльності підприємства надає можливість рейдеру оскаржувати у судовому порядку угоди підприємства, законність призначення менеджменту, рішення зборів акціонерів, а також блокувати діяльність підприємства скаргами до податкових органів.

4. Зосередження всіх функцій управління у руках однієї особи або однієї владної структури. Зазначене суттєво спрощує для рейдера процедуру організації недружнього поглинання. Для організації рейдерської атаки йому необхідно підкупити або отримати інструменти впливу лише на одну особу або перехопити управління лише однією владною структурою. Таким чином, необхідною є диверсифікація управлінських і контрольних функцій.

5. Відсутність у підприємства належним чином оформленої звітності і документації, наявність подвійної бухгалтерії. Рейдер завжди готовий скористатися будь-якими недоліками і протиріччями установчих документів, внутрішніх положень, типових договорів з метою шантажу власників підприємства, представників його менеджменту, а також блокування діяльності підприємства через порушення проти нього судових справ.

[1] Цінні папери: підручник / За ред. В.Д. Базилевича. - К.: Знання, 2011. – 161 с.

6. Наявність конфліктів, які зумовлені реалізацією економічних відносин на підприємстві за участі великої кількості економічних суб'єктів, що є носіями різних, а іноді і кардинально протилежних за характером економічних інтересів. До них слід віднести: конфлікти між акціонерами підприємства; конфлікти між членами наглядової ради; конфлікти між виконавчим органом управління і наглядовою радою; конфлікти між економічними партнерами підприємства і його правлінням; конфлікти між правлінням підприємства та його кредиторами; конфлікти між акціонерами підприємства та його потенційними інвесторами. Сторони конфліктів можуть піти на змову з рейдером з метою досягнення власних цілей.

Таким чином, необхідність забезпечення стійкого розвитку підприємства, підпорядкування його діяльності єдиній основоположній меті - максимізації ринкової вартості активів, вимагає від керівництва підприємства вирішення внутрішніх і зовнішніх конфліктів шляхом гармонізації та взаємоузгодження інтересів різних груп економічних суб'єктів на основі розробки та реалізації відповідної фінансової та організаційно-економічної стратегії, яка повинна перш за все забезпечити об'єднання усіх економічних суб'єктів навколо єдиної мети, що слугуватиме гарантом взаємного задоволення їх індивідуальних економічних потреб.

7. Недооцінка підприємством ринкової вартості власних активів, власної позиції на ринку, а також конкурентів. Неадекватність системи безпеки та системи менеджменту підприємства вартості його активів робить підприємство привабливим об'єктом для рейдерської атаки. Якщо акціонери і керівництво підприємства не можуть належним чином оцінити власний фінансового господарський стан, вони не в змозі прогнозувати дії рейдерів і забезпечити захист активів підприємства. Теж саме стосується необхідності реалістичної оцінки конкуренції на ринку, адже конкуренти можуть бути у змові з рейдером або самі виступати у якості потенційного рейдера[1].

8. Наявність у структурі активів підприємства майна з недостатньо чітко визначеними правами власності на нього або оформленого на підставні чи фіктивні дочірні компанії. Зазвичай це дозволяє уникнути оподаткування і приховати доходи, але, водночас надає можливість рейдеру переоформити на себе права власності на зазна-

[1] Осипенко ОБ. Защита компании от недружественного поглощения и корпоративного шантажа. - М.: Юркнига, 2005. – С. 237.

чене майно. У той час, як підприємство не буде мати можливості звернутися до суду через «сумнівний» статус майна і загрози виникнення штрафних санкцій з боку контрольних і податкових органів.

9. Відсутність у власників підприємства взаєморозуміння з його керівництвом (менеджментом). Незадоволене винагородою за власну діяльність керівництво підприємства може здійснювати управління ним у такий спосіб, який у майбутньому дозволить захопити контроль над підприємством.

Однією із найбільш розповсюджених протиправних схем перехоплення контролю над майном акціонерного товариства з боку його менеджменту можна вважати обтяження товариства заборгованістю перед афільованою по відношенню до менеджменту фінансовою структурою. Менеджмент акціонерного товариства своїми діями ускладнює або робить неможливим вчасне погашення заборгованості, що дає можливість кредитору ініціювати справу про банкрутство.

10. Безвідповідальне ставлення суб'єктів підприємницької діяльності до можливих рейдерських атак, а також існування тіньової економіки та корупції. Крім того, значна частина підприємств на сьогоднішній день все ще використовує стандартні статути, замість добре продуманих, адаптованих до власної діяльності установчих документів, що містять спеціальні антирейдерські положення. Переважна частина суб'єктів підприємницької діяльності, заощаджуючи кошти, не використовують послуги фахівців у галузі корпоративного права та економічної безпеки. Ці та інші помилки керівництва підприємств і створюють сприятливі умови для діяльності рейдерів.

11.Наявність неконтрольованої кредиторської заборгованості та прострочених зобов'язань. Зазначені обставити надають можливість рейдеру скуповувати «борги» підприємства з метою отримання контролю над його активами через накладання судом стягнення на майно в рахунок заборгованості, через накладання арешту на майно на час розгляду судом справи про примусове стягнення заборгованості, а також через порушення судового провадження у справі про банкрутство підприємства-боржника.

Досліджуючи екзо- та ендогенне середовище підприємства, першочергово необхідно дослідити рівень його потенційної небезпечності, джерела невизначеності, а також з’ясувати, яким чином підприємство може взаємодіяти із цією невизначеністю. Адже сучасний стан економіки та ситуація з розповсюдженням рейдерства при-

ховує у собі безліч загроз для нормального функціонування підприємства, що криються як усередині, так і поза ним.

Дослідниками подається комбінована класифікація чинників, що впливають на рівень небезпечності діяльності господарюючого суб'єкта. Достатньо ґрунтовною в цьому сенсі є класифікація С.К. Рамазанова та інших авторів[1] щодо визначення ендогенних та екзогенних факторів небезпеки підприємств.

Так, до перших з них відносять: неефективний процес управління (планування, організування, мотивування, контролювання та регулювання), нераціональну організаційну структуру, малоефективний апарат управління, недостатність ресурсів належної якості (фінансових, матеріальних, трудових тощо), недостатню кваліфікацію працівників, збої у виробничо-технологічних процесах, слабку орієнтованість на інвестиції, недостатнє інформаційне забезпечення, низький рівень корпоративної культури, збої в процесах постачання і збуту, неякісні маркетингові дослідження, слабку інноваційну орієнтованість, незадовільну планово-аналітичну діяльність, зменшення частки ринку, погіршення фінансово-економічних результатів (збільшення собівартості, зниження показників ліквідності, рентабельності тощо) та ін.

До екзогенних факторів згідно із запропонованою концепцією відносять: підвищення інфляції, недосконаліть нормативно-правової бази, коливання на валютних ринках, політичну нестабільність в державі або в країнах контрагентів, зниження купівельної спроможності споживачів, монополізацію ринку, загострення конкуренції, появу кризи в конкретній галузі чи суміжних галузях, податковий тиск та тиск зі боку органів управління, загрозу рейдерства, спади в економіці, недосконалу банківську систему, спади чи коливання в ринковій кон'юнктурі, невідповідний розвиток науки та техніки, слаборозвинену інфраструктуру, несприятливі міжнародні події, погіршення демографічного стану, природно-екологічні проблеми тощо.

На думку О.Ф. Яременко[2] складність і різноманітність чинників впливу на стан економічної безпеки ілюструє наступна табл. 2.8.

---

[1] Рамазанов С.К., Степаненко О.П., Тимашова Л.А. Методи антикризового управління: Монографія. – Луганськ: Вид-во СНУ імені В.Даля, 2004. – 192 с.

[2] Яременко О.Ф. Аспекти побудови паспорта загроз підприємства // Вісник Хмельницького національного університету. – 2011. - №2. – Т.1. – С. 15.

Таблиця 2.8

Загальна система факторів, які загрожують безпеці підприємства

Непередбачуваність дій державних органів	Нестабільність соціальних умов	Стихійні лиха локального характеру	Недотримання договорів керівництвом фірми
Зовнішні		Внутрішні	
Прямої дії	Непрямої дії	Об'єктивні	Суб'єктивні
Нестабільність економічної, фінансової, зовнішньо-економічної та іншої політики	Непередбачені зміни економічного стану в регіоні	Непередбачені зміни у внутрішньо господарських відносинах	Низький рівень роботи працівників підприємства
Непередбачувані зміни кон'юнктури внутрішнього та зовнішнього ринку	Непередбачені зміни в галузі підприємницької діяльності	Брак бізнес-інформації на фірмі	Вибуття ключових співробітників
Непередбачуванідіїконкурентів	Непередбачуванізміни у міжнароднійситуації	Фінансовіпроблеми на підприємстві	
Корупція та рекет	Стихійні лиха	Відсутність-механізмумотивації	
Революційнізміни в НТП	Непередбаченізміниекономічної обстановки в країні		
Непередбачуванізміни у взаємостосунках із господарськимисуб'єктами			

За концепцією Н.В. Радванської, повне викорінення захватів та поглинань неможливе, а ефективно лише вживати запобіжних заходів, враховувати всі можливі ризики та виділити декілька ознак «рейд-придатності» підприємства:

«розпилений» пакет акцій; недооцінений актив;

організаційні та правові проблеми; протиріччя внутрішніх документів чинному законодавству;

порушення під час придбання активів і акцій; неправильне оформлення володіння активами та акціями;

помилки під час визначення функцій і повноважень органів управління товариством;

неврегульованість корпоративних відносин; порушення законодавства, особливо порядку проведення зібрання акціонерів та ради директорів, компетенції органів самоврядування;

порушення порядку схвалення угод; номінальні особи в органах управління;

відсутність захисту інформації, конфіденційності, внаслідок чого цінна інформація про організацію може бути отримана без значних зусиль;

порушення при роботі з поштою та прийомом кореспонденції; відсутність нормально функціонуючої служби безпеки об'єктів та ін[1].

Значний теоретичний і практичний інтерес становить функціональний підхід до визначення прояву загроз через уявлення складових економічної безпеки підприємства, запропонований О.М. Яременком[2]. Так автор пропонує з'ясувати перелік екзогенних та ендогенних складових, на які здатні негативно вплинути, відповідно, чинники внутрішнього та зовнішнього середовища. Так, до екзогенних належать наступні елементи.

1) ресурсна складова полягає в забезпеченні виробництва основними видами ресурсів, необхідним їх 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 підприємства.

---

[1] Радванська Н.В. Рейдерство як загроза економічній безпеці підприємства та держави // Вісник Хмельницького національного університету. – 2011. - №2. – Т.1. – С. 204-206.

[2] Яременко О.Ф. Аспекти побудови паспорта загроз підприємства // Вісник Хмельницького національного університету. – 2011. - №2. – Т.1. – С. 14-20.

2) екологічна складова визначає відповідність екологічності результатів виробництва нормативним параметрам, затвердженим відповідним законодавством, загрозу втрати здоров'я працівниками підприємства, втрату прибутків через значні штрафні санкції за порушення законодавчої бази.

3) ринкова складова відображає ступінь відповідності існуючих внутрішніх можливостей підприємства власній стратегії розвитку та зовнішнім можливостям. Показниками є частка ринкової ніші, що належить підприємству, конкурентна позиція, можливість протистояти конкурентному тиску, адаптаційні можливості суб'єкта господарювання тощо.

4) інтерфейсна складова визначає надійність взаємодії підприємства з економічними контрагентами. Загрозу являють непередбачені зміни угод, зміна умов контрактів тощо.

5) міжнародна складова. Її функціями є: дослідження законодавства країни-партнера в рамках підприємницької та експортно-імпортної діяльності, питання місцевого оподаткування, культурно-релігійні традиції, ресурсно-кліматичні умови, питання конкуренції тощо. Необхідність цієї складової – пряме і непряме блокування доступу українських товарів на європейські ринки, застосування до них політики протекціонізму та інших обмежень.

До числа ендогенних складових згідно вказаної концепції варто відносити:

1) фінансова складова. Є найбільш показовою щодо стану економічної безпеки підприємства. Призначення даної складової полягає у забезпеченні фінансової стійкості підприємства, недопущенні банкрутства, зростанні прибутковості та рентабельності виробництва, поточної і абсолютної ліквідності, платоспроможності і кредитоспроможності, тенденцій зменшення обсягу кредиторсько-дебіторської заборгованості, ефективності і достатності оборотних засобів(як власних, так і запозичених) тощо.

2) технологічна складова, що характеризується рівнем впровадження прогресивних технологій, своєчасним оновленням основних виробничих фондів, безпекою праці на виробництві, раціональним використанням виробничих потужностей, пошуком внутрішніх резервів поліпшення використання технологій. До основних негативних впливів належать спрямованість на підрив технологічного потенціалу підприємства, порушення технологічної дисципліни, відсутність або об-

меженість інноваційної діяльності, інвестиційна непривабливість підприємства, значна енергоємність виробничо-технологічних процесів.

3) кадрова складова, що враховує забезпеченість та інтелектуально-кваліфікаційний рівень працівників підприємства, організацію системи управління персоналом, навчання і мотивацію співробітників підприємства, збереження і розвиток інтелектуального капіталу підприємства, забезпечення прожиткового мінімуму працівникам підприємства, зростання заробітної платні, системи мотивації і оплати праці за кінцевими результатами роботи, відповідність заробітної платні кваліфікації працівників. Негативними тенденціями є звільнення провідних спеціалістів, зниження частки інженерно-технічних працівників, зниження освітнього рівня, плинність кадрів, значна частка працівників-сумісників.

4) правова, або юридична складова - характеризує правову захищеність як самого підприємства, так і його працівників в рамках договірної та ділової документації, захищеність комерційної інформації, дотримання норм патентного права, цензуру публічної інформації, роз'яснення та дотримання норм законодавства.

5) захисна складова (фізично-силова, кримінальна) передбачає захист інтелектуальної власності працівників (патентних і авторських прав) від промислово-економічного шпигунства, від розкрадань і крадіжок, захист комерційної таємниці, спроби негативного впливу(фізичного та морального характеру) на працівників фірми. Основними причинами виникнення проблемних ситуацій є нездатність підприємств-конкурентів досягти переваг коректними методами, спроби отримання злочинними особами доходів через шантаж, шахрайство та крадіжки тощо. У зв'язку з цим на підприємствах організовуються служби безпеки, головною функцією яких є дотримання правопорядку на підприємствах і охоронна діяльність.

6) інформаційна складова характеризує рівень якісної, точної, своєчасної інформації про умови зовнішнього середовища та контрагентів(конкурентів, клієнтів, постачальників і т.д.), захист інформаційного забезпечення наукової, виробничо-комерційної і маркетингової діяльності підприємства. Ця складова має особливість: вона може належать як до ендогенних, так і до екзогенних[1].

[1] Яременко О.Ф. Аспекти побудови паспорта загроз підприємства // Вісник Хмельницького національного університету. – 2011. - №2. – Т.1. – С. 15.

Визначення системи чинників дозволяє виробити методологію та адресність мінімізації загроз рейдерських захоплень та поглинань, отримавши відповідь на друге з поставлених питань. Так, у контексті *юридично-консультативного забезпечення безпеки підприємства* від рейдерських атак варто здійснювати наступні заходи: фахове юридичне опрацювання договірних відносин підприємства; планування і обґрунтування юридичного забезпечення комерційної діяльності; правова оцінка рівня дослідно-експерних робіт; оцінка кваліфікації працівників підрозділу та правове супроводження роботи з персоналом.

Фінансова складова мінімізації ризиків рейдерських атак передбачає посилення централізованого фінансового контролю; аналіз негативних наслідків розвитку виробничої й маркетингової структур з погляду стану і змін, насамперед платоспроможності, рентабельності і прибутковості; аналіз стану ринку цінних паперів з погляду їх привабливості, ресурсів на інвестиції та розвиток, а також захисту від набуття акцій конкурентами і можливого встановлення контролю над підприємствами; аналіз ділових пропозицій підприємству; створення інформаційного центру для отримання постійної інформації про борги підприємства; оптимізація величини та оборотності дебіторсько-кредиторської заборгованості; визначення вигідної схеми виплат боргу тощо.

У напряму *кадрової складової безпеки підприємства* від рейдерських захоплень певною користю будуть характеризуватися наступні заходи: запровадження методів оцінки, добору, атестації, підготовки, просування кадрів, підвищення матеріальної відповідальності за результати праці; підвищення частки праці кваліфікованих працівників; можливість залучення та ефективне використання висококваліфікованого персоналу; мотивація діяльності, система матеріальної та нематеріальної винагороди; вдосконалення системи заробітної плати та рівня доходів робітників; покращення умов праці робітників; система соціальних виплат працівникам; стимулюючі заходи для всіх співробітників щодо покращення діяльності підприємства, розмір яких визначається на підставі точних і зрозумілих критеріїв; запровадження соціально-орієнтованих програм, фінансованих підприємством для власного персоналу.

Фізично-силовий аспект мінімізації рейдерських атак передбачає створення власної системи безпеки або залучення спеціалізованих організацій; охорона співробітників, гарантування безпеки майна, перевезень; технічний захист приміщень, транспорту, кореспонденції,

переговорів, документації; збирання інформації про потенційних рейдерів та ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій; забезпечення протипожежної, охоронної спеціалізації, відео спостереження тощо.

В контексті забезпечення *інформаційної безпеки та мінімізації витоку інформації*, необхідної для реалізації рейдерського захоплення варто здійснювати аналіз власної вихідної інформації на предмет виявлення інформації яка не підлягає розголошенню; здійснювати посилення захисту інформації від несанкціонованого доступу; забезпечувати збирання інформації про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій з метою припинення таких спроб створення бази «небажаних» контрагентів; збирання різних видів необхідної інформації, що здійснюється через офіційні контакти з різноманітними джерелами відкритої інформації, неофіційні контакти з носіями закритої інформації, а також її розробка та систематизація за допомогою спеціальних технічних засобів; перевірка податкових та інших платіжних документів щодо їх достовірності; пошук інформації про партнерів, споживачів, конкурентів із надійних джерел; підготовка та проведення акцій, що покращують імідж підприємства та його ділову репутацію; технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу зацікавлених юридичних і фізичних осіб до закритої інформації; перевірка зв'язків з діловими партнерами; формування сприятливого іміджу підприємства; протидія спробам завдання шкоди репутації через поширення неправдивої інформації.

Таким чином, підсумовуючи проведене у підрозділі дослідження, слід зазначити, що в Україні на сьогоднішній день є всі передумови для розгортання рейдерства та проведення успішних рейдерських захоплень. З'ясування системи чинників, факторів та детермінантів, що сприяють успішному захопленню чи поглинанню, дає підстави запропонувати наступні висновки, відповівши у такий спосіб на третє з поставлених на початку дослідження запитань.

1. Визначення системи вищевказаних чинників і факторів є необхідним для своєчасної їх ідентифікації та вироблення адресних заходів з нейтралізації, блокування джерела рейдерських загроз та усунення наявної можливості їх реалізації.

2. Сукупність загроз та небезпек, які впливають на діяльність підприємства потребують встановлення величини ризику та втрат, що

може зазнати суб'єкт господарювання, визначення ймовірності виникнення, оцінки стану робіт по попередженню небезпек та загроз та можливості усунення їх дії, розробки заходів по усуненню, уникнення втрат, що можуть виникнути. Для вирішення вказаних завдань варто, на нашу думку, запровадити практику розроблення на сучасних підприємствах паспортів загроз рейдерських захоплень та недружніх поглинань. Паспорт загроз розробляється з метою підвищення ефективності системи управління за кризових умов, формування адекватних заходів по попередженню та уникненню загроз та небезпек захоплення чи поглинання. Започаткування практики розроблення паспорту загроз підприємства дозволить виявити найбільш небезпечні фактори впливу, співставити ступінь небезпеки із рівнем захищеності, встановити достатність сил та засобів, що можуть протидіяти загрозам та небезпекам протиправних захоплень і забезпечити достатність засобів заходів по їх попередженню та мінімізації негативного впливу на практику господарювання.

3. З урахуванням потреби практичної наближеності концепції системного уявлення чинників, які сприяють реалізації планів рейдерських захоплень і поглинань, вкрай потрібним вбачається формалізація проявів рейдерських загроз та небезпек, побудова відповідної економіко-математичної моделі з визначенням імовірності з метою чіткого прогнозування захоплень чи поглинань, що й підтверджує необхідність розробки засобів діагностики.

РОЗДІЛ 3

СТРАХУВАННЯ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Поняття, сутність та правовий зміст страхування, його місце у системі забезпеченні економічної безпеки

У XXI століття страхування ввійшло як одне з найбільш розвинених та ефективних сфер діяльності. Про це свідчать суми надходжень страхових премій, які у світі щороку зростають швидше ніж валовий внутрішній продукт. Водночас, багато дослідників страхової справи, справедливо вважають, що рівень розвитку страхового ринку є одним із важливих показників економічного розвитку держави. Так, на думку В. Ельбрехта: «Розвиток страхового ринку України є нагальною потребою, надиктованою зростанням рівня ризикованості економічних, політичних, соціальних та екологічних процесів, виступає важливим показником стану економіки держави»[1].

З формуванням у 1892 році страхового товариства «Дністер» українські фахівці робили спроби створити українську страхову термінологію. Адже, на думку Р. Тринько та О. Мельника: «Без зрозумілого категорійного апарату, без ефективної термінології практично важко уявити собі можливість успішного функціонування будь-якої економічної системи, економічного механізму»[2]. Що стосується термінології, то ще Р. Декарт свого часу писав: «Вірно визначайте слова, і ви визволите світ від половини непорозумінь»[3].

Питання про співвідношення понять «страхування» і «страхова діяльність» є вельми актуальним і складним. Досить часто в офіційних документах ними користуються як словами-синонімами. В окремих випадках це проходить безболісно, тому що не зачіпає ніяких принципових аспектів, а в інших – навпаки, вільне поводження з цими термінами породжує не вирішувані протиріччя. З огляду на це виникає нагальна потреба в більш уважному вивченні зазначених термінів з по-

---

[1] Ельбрехт В. Еволюція страхування / В. Ельбрехт // Вісник Запорізького юридичного інституту. – 2004 - № 2 (27). – С. 71.

[2] Страхування в системі економічної безпеки / Керівник авт. кол. проф. Р.І. Тринько (монографія). – Львів: ЛьвДУВС, 2008. – С. 90.

[3] Декарт Р. Избранные сочинения. - М.: Наука, 1970. – С. 508.

зиції не тільки їх походження, але й з'ясування сутності та значущості тих реальних явищ дійсності, котрі ними означуються.

У зв'язку з цим виникає необхідність більш глибокого дослідження термінів «страхування», які закріплені у законодавстві України.

У своїй повсякденній діяльності людина завжди піддається різній небезпеці, яка загрожує йому особисто, його близьким або його майну. Інакше кажучи, людина постійно піддається різному роду ризиків. У певних випадках причина небезпеки коїться у відсутності знань про навколишнє середовище (бурі, зливи, блискавки тощо). В інших випадках це стосується слабкого розуміння умов економічного ринку, виробничого процесу тощо. Таким чином, ризик супроводжує людину на протязі всього його життєвого шляху.

У теорії страхового права існують різні способи обмеження ризику:

− заходи спрямовані на попередження небезпечних подій (наприклад, будівництво будинків з вогнестійких матеріалів);

− заходи спрямовані на усунення небезпеки, яка вже виникла, комбінування ризиків, створення резервних фондів та ін.

Але найбільш ефективним способом обмеження ризиків є інститут фінансового права – страхування. При страхуванні особа, якій загрожує визначений ризик, за невеликий внесок, привертає до несення ризику іншу особу (страхову компанію), що бере на себе відповідальність за наслідки, які можливі після настання страхового випадку[1].

Роль страхування у повсякденному житті має велике значення. Воно дає можливість як фізичній, так юридичній особі відновити пошкоджені матеріальні речі (майнове страхування). Страхування може забезпечити фізичну особу матеріально у зв'язки з втратою ним працездатності, що дасть можливість відновитись після хвороби чи отриманих травм (особисте страхування). Страхування може також забезпечити виплату грошових коштів у випадку виникнення для нього такого обов'язку (страхування відповідальності). Все це дає людині можливість почувати себе впевнено у будь-якій ситуації, а також дивитись у майбутнє без остраху.

У юридичній науці поняття «страхування» ототожнюють з поняттям «страхова діяльність». Це трапляється тому, що в українському зако-

[1]Серебровский В.И. Избранные труды по наследственному и страховому праву / В.И. Серебровский. – М.: Статут (в серии «Классика российской цивилистики»), 1997. – С. 434.

нодавстві відсутнє закріплене поняття «страхова діяльність», хоча вживання цього поняття в нормативних актах є дуже розповсюдженим явищем. Відсутність законодавчо закріпленого визначення терміну «страхова діяльність» безумовно є прогалиною національного законодавства України, що спричиняє багато непорозумінь під час ведення страхової справи.

Аналізуючи термін «страхування» можна дійти висновку, що страхування відображає ідею застереження, захисту та безпеки. У багатьох слов'янських мовах, у тому числі й в українській, виникнення терміна «страхування» пов'язують із коренем цього слова «страх». Це також підтверджується висловленням російського вченого Л. Рейтмана: «Власники майна, які вступали між собою у виробничі відносини, мали страх за його збереження, за можливість знищення чи втрати у зв'язку зі стихійними явищами, пожежами та іншими непередбачуваними загрозами економічному життю»[1].

З іншого ж боку в європейських мовах коренем такого ж терміну «insurance industry − страхування» є слова: впевненість, безпека, передбачливість.

У відповідності до теорії розподілу збитків, Адольфа Вагнера, страхування є така господарча діяльність, яка усуває або зменшує шкідливі наслідки окремих непередбачених випадків для майна окремої фізичної особи таким чином, що воно розподіляє їх на ряд випадків, яким загрожує однакова небезпека, що насправді ще не настала[2].

Очевидним дефектом цього визначення є те, що воно не включає в себе тих випадків, коли страхування взагалі не передбачає мети відшкодування шкоди (наприклад, випадки особистого страхування).

Д. Кростпід страхуванням розуміє поєднання ризиків з метою їх оплатного вирівнювання. Визначення Кроста є дуже загальним, а також включає самострахування.

М. Бремер розуміє страхування як прийняття на себе страховиком обов'язку сплатити за винагороду (премію) страхувальнику або вигодонабувачу деяку суму грошей у випадку настання відомого випадку, який не залежить від зацікавлених осіб.

---

[1] Цивільне право України: В 2-х томах. Т.2. Підручник / За ред. д-ра юрид. наук, проф. Є.О. Харитонова; канд. юрид. Наук Н.Ю. Голубєвої. – Х.: ТОВ «Одіссей», 2008. – С. 402.

[2] Серебровский В.И. Избранные труды по наследственному и страховому праву / В.И. Серебровский. – М.: Статут (в серии «Классика российской цивилистики»), 1997. – С. 436.

У словнику С.І. Ожегова страхування визначається наступним чином: «Це збереження будь-кого від можливих збитків за рахунок періодичних внесків до спеціальної установи, яка в разі настання збитків сплачує грошову винагороду»[1].

У науці страхування деякі автори підходять до визначення «страхування» з точки зору страхового фонду. Так, наприклад В.К. Райхер визначає страхування як форму організації централізованого страхового фонду за рахунок децентралізованих джерел із внесків, які здійснюються в цей фонд його учасниками[2].

Перевагою цього визначення є його універсальність, воно може розповсюджуватися на всі види страхування, незалежно від їх специфічних ознак. Таке визначення має право на існування, але воно не повністю розкриває суть поняття, що спричиняє перепони для його розуміння.

У числі останніх за часом спроб дати єдине визначення страхування необхідно відокремити визначення Ю. Гірке, Сюмієна та Емара. Гірке визначає страховий договір як самостійний договір, в силу якого одна сторона приймає на себе від іншої сторони за оплату зобов'язання по виконанню дій, яке складається у відомому майновому наданні на випадок настання невідомого, господарчо-шкідливого випадку.

Сюмієн визначає страхування як договір, в силу якого страховик групує на засадах взаємності інших осіб (страхувальників), для того, щоб дати їм можливість взаємно відшкодувати збитки, яким вони піддаються у випадку реалізації відомих ризиків, за сплату кожним страхувальником відомої суми (премії), яку страховик обертає у загальну масу з вирахуванням витрат, які передбачені статутом.

Емар, комбінує не тільки економічні та юридичні фактори, але ще й технічні, та дає наступне визначення страхування: страхування є операцією, в силу якої одна сторона – страхувальник – за сплачену ним винагороду – премію – вимовляє в свою користь або в користь третьої особи на випадок здійснення відомого ризику надання від іншої сторони – страховика, - який, приймає на себе сукупність ризиків, врівноважує їх відповідно до законів статистики[3].

---

[1]Ожегов С.И. Словарь русского языка. – М., 1978. – С. 710.

[2]Райхер В.К. Общественно-исторические типы страхования. – М.: ЮКИС, 1992 . –С. 19.

[3]Серебровский В. И. Избранные труды по наследственному и страховому праву / В. И. Серебровский. – М.: Статут (в серии «Классика российской цивилистики»), 1997. – С. 442.

Звертаючись до страхування, ми можемо спостерігати деяку алєаторність (випадковість) у двох напрямках.

Перший напрямок полягає у тому що, коли страхувальник сплачує страхову премію, то він не знає напевно, отримає страхову винагороду чи ні, а якщо отримає, то при тривалості внеску премії чи покриє страхове відшкодування сплачені ним премії.

У свою чергу, страховик не знає, чи прийдеться йому взагалі сплачувати страхову винагороду, а також він не знає часу та об'єму відшкодування – це другий напрямок.

Необхідно відмітити той факт, що не дивлячись на велику кількість визначень поняття «страхування» як в економічній, так і в юридичній літературі, до теперішнього часу не вдалося досягнути створення такого визначення, яке б, з одного боку, не було занадто вузьким та обіймало усі види страхування, а з іншого боку, не було занадто широким.

Фахівцями страхового права були зроблені спроби дати визначення терміну «страхова діяльність» та сформулювати цілісне науково-обґрунтоване поняття страхової діяльності. Так, на думку професора В.В. Шахова: «… страхова справа являє собою багатофактурну, динамічну систему, яка складається із постійно взаємодіючих частин»[1].

Професор В.Р. Ідельсон вбачав у страховій справі: «…такий вид господарської діяльності, який отримує вигоду із страхових угод»[2].

У свою чергу український фахівець у сфері страхового права Н.Б. Пацурія сформулювала поняття «страхової діяльності» наступним чином: «Врегульована нормами права господарська діяльність страхової організації, переважно як суб'єкта підприємництва, що здійснюється на підставі ліцензії із організації і безпосереднього надання страхових послуг, яка пов'язана із формуванням, управлінням страховими фондами та здійсненням майбутніх страхових виплат у разі настання страхових випадків, передбачених договором страхування або чинним законодавством»[3].

Що стосується наукової точки зору стосовно понять «страхування» та «страхова діяльність», то деякі автори, по суті, ставлять знак рівності між ними. Так, А.А. Іванов визначає страхування як вид необхідної

---

[1]Шахов В.В. Страхование. – М: ЮНИТИ, 1997. – С. 15.

[2] Идельсон В.Р. Страховое право. – М.: Анкил, 1993. – С. 3

[3] Пацурія Н.Б. Страхове право України: Навчальний посібник / Н.Б. Пацурія. – К.: ЮрІнком Інтер, 2006. – С. 30.

суспільно корисної діяльності, при якій громадяни та організації наперед страхують себе від несприятливих наслідків у сфері їх матеріальних та особистих благ шляхом внесення грошових внесків до особливого фонду спеціалізованої організації (страхової компанії)[1]. Аналогічної точки зору дотримуються В.С. Анохін[2] та Н.С. Ковалевська[3] ставлячи знак рівності між страховою діяльністю та економічними відносинами, що виникають у сфері страхування.

У законодавстві України стосовно визначення поняття «страхування» склалася двозначна ситуація, коли одному і тому ж терміну дається різне визначення. А відносно визначення «страхова діяльність» − воно взагалі відсутнє.

На відміну від діючого поняття, яке закріплене ст. 1 Закону України «Про страхування»: «Страхування – це вид цивільно-правових відносин щодо захисту майнових інтересів фізичних осіб та юридичних осіб у разі настання певних подій (страхових випадків), визначених договором страхування або чинним законодавством, за рахунок грошових фондів, що формуються шляхом сплати фізичними особами та юридичними особами страхових платежів (страхових внесків, страхових премій) та доходів від розміщення коштів цих фондів»[4].

Також є чинним термін «страхування», яке закріплене у ч. 1 ст. 352 Господарського кодексу України відповідно до якого страхування – це діяльність спеціально уповноважених державних організацій та суб'єктів господарювання (страховиків), пов'язана з наданням страхових послуг юридичним особам або громадянам (страхувальникам) щодо захисту їх майнових інтересів у разі настання визначених законом чи договором страхування подій (страхових випадків), за рахунок грошових фондів, які формуються шляхом сплати страхувальниками страхових платежів[5].

---

[1]Гражданское право: Учебник / Егоров И.Д., Елисеев И.В.,Иванов А.А. и др. / Под ред. Ю.К. Толстого, А.П. Сергеева. Ч. II. М.: «ПРОСПЕКТ», 2000. – С. 496

[2]Анохин В.С. Предпринимательское право: Учебник. М.: ВЛАДОС, 1999. – С. 369;

[3]Коммерческое право: Учебник / Под ред. В.Ф. Попандопуло, В.Ф. Яковлевой. С-П.: Изд.-во СПб. ун-та, 1998. – С. 275.

[4]Закон України «Про страхування» від 04.10.2001 р. № 2745 – III (із змін. та доп.) // Право і практика. – 2009. - № 4. – С. 3 – 38.

[5] Господарський Кодекс України від 16.01.2003 р. № 436 – IV // Офіційний вісник України. – 2003. – № 11. – Ст. 462.

Виходячи із змісту цього визначення можна сміливо стверджувати, що це визначення наголошує на діяльності суб'єктів страхового ринку.

Це недоцільно, бо поняття «страхування» значно ширше поняття «страхова діяльність». Сам термін «страхування» включає в себе всі елементи, які стосуються страхових відносин (об'єкт, предмет, метод, суб'єкт та ін. ознаки). Натомість термін «страхова діяльність», який спрямований на створення, надання та супровід своїх послуг, стосується лише діяльності спеціально уповноважених державних організацій та страховиків. Отже, вони своїми діями приводять до руху безпосередній механізм страхування, це є підтвердженням того, що термін «страхування» є ширшим за термін «страхова діяльність» вони співвідносяться одне до одного як ціле та частина цілого, а від так ці поняття неможна ототожнювати між собою.

Проаналізувавши ці два поняття страхування, які наведені у статях вітчизняного законодавства, та зіставивши їх зміст, можна дійти висновку, що у страховому законодавстві України склалась ситуація коли один термін «страхування» містить в собі два різних змісти. Ця ситуація, яка склалася у страховому праві не відповідає вимогам юридичної техніки.

Як відомо, рівень юридичної техніки є надійним показником рівня розвитку правової культури суспільства. Приведемо міркування із цього приводу одного з найбільших німецьких юристів XIX в. Рудольфа Ієрінга (1818-1892): «Проти домагання на захист, що пред'являється особистим егоїзмом, суспільство має право виставити свої інтереси. Інтереси ж суспільства складають те, що вигідно не одному, а всім, на чому всі можуть зійтися, і цей інтерес є справедливість. Вона вища за свободу, індивід існує не для себе виключно, але і для світу; тому свобода, тобто те, що відповідає особистим інтересам індивіда, і повинна підкорятися справедливості, тобто тому, що потрібний інтересами всіх»[1].

З огляду на це виникає потреба в розмежуванні цих понять. Ми не збираймося давати поняттю «страхова діяльність» авторське визначення, а пропонуємо виправити ситуацію яка склалась наступним чином. Спочатку необхідно на законодавчому рівні закріпити юридичний термін, а

[1] Иеринг Р. Цель в праве. − СПб., 1881. − С. 109-110.

потім вести розмову, якщо є така необхідність, про його вдосконалення. Отже, доцільне наступне вирішення цього питання.

Якщо в визначені «страхування», яке закріплене ч. 1 ст. 352 ГКУ, акцент робиться саме на діяльності спеціально уповноважених державних організацій та суб'єктів господарювання (страховиків), то це поняття за змістом визначення є поняттям «страхової діяльності». А від так необхідно внести зміни до ч. 1 ст. 352 Господарського кодексу України змінивши слово «страхування» на словосполучення «страхова діяльність».

З урахуванням обов'язкової присутності у всіх страхових відносинах страховика, який за своєю економіко-правовою сутністю є суб'єктом господарювання, асоціювання страхової діяльності з цивільно-правовим інститутом також бачиться не коректним.

Від страхування необхідно також відрізняти деякі процеси, які зовні на нього схожі, але по суті є самостійними інститутами – порука та договір гарантії. Від безоплатної поруки теоретично провести відмінність страхування не складно. Страхування є (у його договірній формі) операцією самостійною і відшкодувальною; порука – є операцією акцесорною, такою, що припускає існування головного зобов'язання, і безоплатною. Значно складніше вирішити питання зі встановленням відмінності, коли порука носить відшкодувальний характер. Нерідко схожість між різними формами відшкодувальної поруки та страхування (страхування кредиту) є такою близькою, що проведення чіткої межі між цими явищами викликає великі труднощі.

Теоретично відмінність між відшкодувальною порукою та страхуванням кредиту лежить також в акцесорному характері першого і самостійному − другого.

Поручитель приймає на себе поруку за виконання зобов'язання третьою особою − головним боржником ст. 553 ЦКУ. Страховик відповідно до законодавства ніякої на себе поруки не приймає: він сам є головним боржником. Тому він є відповідальним навіть тоді, коли неплатоспроможну третю особу не може притягати до відповідальності (неможливість виконання, що звільняє від відповідальності і т. п.). Крім того, порука за своєю природою є на сам перед борговим зобов'язанням, а не зобов'язанням про відшкодування шкоди, яким є всяке страхування майна (у тому числі й страхування кредиту).

Хоча ЦКУ не закріплює норми про відшкодувальну поруку, але, звичайно, таке цілком допустимо і зустрічається нерідко в

українській банківській практиці у вигляді так званої банківської поруки (інакше, гарантійного листа ст. 200 ГКУ), по якій банк приймає на себе перед третіми особами гарантію по виконанню їх клієнтами грошових зобов'язань. Відповідно до ст. 200 ГКУ гарантія є специфічним засобом забезпечення виконання господарських зобов'язань шляхом письмового підтвердження (гарантійного листа) банком, іншою кредитною установою, страховою організацією (банківська гарантія) про задоволення вимог управленої сторони у розмірі повної грошової суми, зазначеної у письмовому підтвердженні, якщо третя особа (зобов'язана сторона) не виконає вказане у ньому певне зобов'язання, або настануть інші умови, передбачені у відповідному підтвердженні[1].

Догматично для страхового права, але проблема вирішується досить просто, оскільки згідно точному сенсу закону, окрім страхових компаній, ніякі інші установи, підприємства та організації, як центральні, так і місцеві, проводити операції зі страхування не мають права. Тому операції відшкодувальної поруки, які здійснюються різними підприємствами (банками та іншими установами), не є страховими операціями та не підпадають під дії норм страхового права. Страхування відрізняється також від договору гарантії. Відповідно до ст. 560 ЦКУ договором гарантії є договір, через який одна сторона банк, інша фінансова установа, страхова організація (гарант) гарантує перед кредитором (бенефіціаром) виконання боржником (принципалом) свого обов'язку[2].

У цьому самостійному характері зобов'язання міститься глибока відмінність договору гарантії від поруки як відношення акцесорного[3]. Тоді як при договорі поруки поручитель приймає на себе відповідальність за чужий борг, гарант обіцяється тільки надати іншій стороні відому вигоду або дохід від ведення підприємства (наприклад, гарантія державою виплати відсотків по облігаційній позиці, випущеній акціонерним будівельним підприємством) або відшкодувати збиток, понесений при експлуатації підприємства.

Гарантія є односторонньою угодою, вона зобов'язує тільки гаранта. У цьому договір гарантії відрізняється від договору страхування як пра-

---

[1] Господарський кодекс України // Відомості Верховної Ради України. − 2003. − № 18,19-20,21-22. − ст. 144.

[2] Цивільний кодекс України // Відомості Верховної Ради України. − 2003. − № 40-44. − С.356.

[3] Акцесорне зобов'язання − зобов'язання, що є похідними, залежними від головного зобов'язання. Воно встановлюються, як правило, з метою забезпечення виконання головного зобов'язання (наприклад, неустойка, застава, порука, завдаток, гарантія).

вовідношення двостороннє. Крім того, особа, виступаюча гарантом, має найчастіше відомий самостійний інтерес в успішній діяльності підприємства іншої сторони, тоді як страховик зазвичай такого інтересу не має.

3.2. Страхування ризиків підприємства: поняття та класифікація

Сучасна зовнішня і внутрішня політика України спрямована на забезпечення реалізації курсу щодо євроінтеграції та інтеграції у світову економічну спільноту на засадах рівноправного партнерства. За цих умов національна безпека України розглядається як один із пріоритетних напрямів державної політики і важлива передумова сталого розвитку суспільства.

Формування і реалізація в Україні державної політики національної безпеки сьогодні є чи не найголовнішою проблемою ефективного управління суспільством, що трансформується.

Успішне подолання наявних загроз на шляху розбудови вітчизняної економіки потребує вирішення надзвичайно складних зовнішньоекономічних та внутрішньо економічних завдань. Це можливо зробити тільки за умови створення та функціонування ефективної системи страхування ризиків підприємництва в Україні, яка б гарантувала повноцінний захист недержавного сектору національної економіки в умовах рейдерських загроз.

Особливе місце в системі національної економічної безпеки посідає проблема економічної безпеки окремих підприємств. З одного боку, функціонування підприємств здійснюється в умовах нестаціонарного зовнішнього середовища, для якого характерні зниження обсягів інвестиційних вкладень, високі процентні ставки за довготерміновими банківськими кредитами, нестабільність податкового законодавства, що істотно знижує рівень життєдіяльності підприємств і підвищує імовірність переходу в кризовий стан.

З іншого боку, кризові тенденції на мікрорівні створюють передумови негативних тенденцій розвитку регіональних систем і зниження рівня національної економічної безпеки.

Економічна безпека підприємства – це стан захищеності його діяльності від негативного впливу зовнішнього середовища, а також спроможності швидко усунути загрози, пристосуватися до наявних умов, що негативно впливають на його діяльність. Зміст цього поняття

включає систему заходів, які забезпечують конкурентоспроможність і економічну стабільність підприємства, а також сприяють підвищенню рівня добробуту працівників.

Отже, виходячи з цього, належна робота керівництва підприємства з формування системи страхування ризиків має бути водночас спрямована на виявлення джерел і розробку заходів з мінімізації негативного впливу чинників впливу на життєдіяльність підприємства.

Як відомо протиправне захоплення підприємства може включати в себе такі суспільно небезпечні дії як умисне знищення або пошкодження чужого майна, погроза знищення чужого майна шляхом підпалу, вибуху або іншим загально небезпечним способом, самовільне зайняття земельної ділянки, фіктивне підприємництво, протидія законній господарській діяльності, доведення до банкрутства, маніпулювання на фондовому ринку тощо. У випадку настання такого роду несприятливих ситуацій, в які може потрапити будь-яке підприємство, страхування є не тільки способом захисту від руйнівних чинників, а й способом подолання несприятливих періодів економічних відносин. Тобто, страхування ризиків підприємства спрямоване на захист його кінцевих результатів, забезпечення досягнення цілей. Воно створює фінансові гарантії стабільності й прибутковості виробництва.

Отже, страхування ризиків підприємства являється важливою формою забезпечення їх ресурсами та їх збереження. Відтак, страхування ризиків підприємства є одним з засобів формування грошових ресурсів, одним із найбільш стабільних джерел довгострокових інвестицій, а також забезпечує оптимізацію формування платіжного балансу, що стабілізує фінансову діяльність суб'єктів господарювання.

Одна з найважливіших функцій управління виробництвом – створити умови для подальшої успішної діяльності підприємства. З цієї причини одним з основних принципів і цілей менеджменту є вдале подолання ризикових ситуацій (в умовах рейдерських загроз), що забезпечує в перспективі максимальну фінансову стійкість. Саме на це спрямоване страхування ризиків підприємства, і, зокрема, страхування майна. В економічній літературі, присвяченій проблемам підприємств, існує багато підходів до класифікації ризиків в діяльності підприємства.

У страхуванні термін «підприємницькі ризики» визначає ті ризики, що пов'язані з майном підприємств; з необхідністю компенсувати шкоду, заподіяну найманим працівникам внаслідок нещасного ви-

падку на виробництві, а також споживачам продукції цього підприємства; з виконанням зобов'язань у межах комерційної діяльності, з укладанням договорів, контрактів; з можливістю втрат через ушкодження або знищення засобів виробництва та ін.

Отже, страхування підприємницьких ризиків – це сукупність страхування майна та страхування відповідальності.

Слід зазначити, що в усіх розвинутих країнах для підприємців є нормою страхування найбільш небезпечних ризиків, пов'язаних з виробничою діяльністю з метою запобігання шкоді від настання різних негативних подій. В свою чергу, відшкодування спричинених збитків сприяє відновленню виробничого процесу.

Страхова теорія на основі критерію субстанції, що є носієм ризику, виокремлює ризики майнового походження, що покриваються страховим захистом у межах видів майнового страхування.

Майном підприємства є основні фонди та оборотні кошти, а також інші цінності, вартість яких відображається в самостійному балансі підприємства. Тобто під терміном «майно» слід розуміти будівлі, споруди, обладнання, транспортні засоби, інвентар, сировину, матеріали, товари та інші матеріальні цінності.

Відповідно до Закону України «Про страхування»[1] та Ліцензійних умов провадження страхової діяльності, затверджених розпорядженням Державної комісії з регулювання ринку фінансових послуг від 28.08.2003 р № 40 та зареєстрованих у Мін'юсті України 15.09.2003 р. за № 805/8126[2], страхування різних видів майна є переважно добровільними видами страхування.

Серед них варто виокремити страхування майна юридичних осіб (на випадок пожежі, стихійного лиха та крадіжки); страхування майна застави (особливо в банківських операціях); страхування предмета іпотеки; страхування електронних пристроїв; страхування будівельно-монтажних ризиків; страхування товарів на складах; страхування експонатів виставок тощо.

---

[1] Закон України «Про внесення змін до Закону України «Про страхування» від 04.10.2001 р. № 2745-III // www.radagov.ua.

[2]Про затвердження Ліцензійних умов провадження страхової діяльності від 28.08.2003 р.: Розпорядження Державної комісії з регулювання ринків фінансових послуг № 40 // www.rada.gov.ua.

У літературних джерелах[1] розглядаються різні варіанти фінансування захисту майнової бази підприємств:

- організація фонду самострахування;
- укладення договорів поруки;
- укладення договорів страхування з професійними страховиками.

Фонд самострахування є складовою страхового фонду суспільства. Він формується шляхом щорічних відрахувань до досягнення розміру, що вказаний у статутних документах суб'єкта господарювання, а порядок використання коштів передбачається самими учасниками, які формують цей фонд.

В умовах ринку підприємства функціонують у несталому економічному середовищі, що постійно змінюється: зростають ціни на матеріальні ресурси, продукцію, що виготовляється, переглядаються умови отримання банківських позик, коливається співвідношення попиту і пропозиції тощо.

Водночас підприємства прагнуть забезпечити стійке становище, можливість працювати без фінансових та виробничих зривів, досягти оперативного подолання тимчасових ускладнень у процесі виробництва, особливо в умовах рейдерських загроз, зокрема, за допомогою самострахування. Тому фонд самострахування трансформується у фонд ризику, який створюється суб'єктами підприємництва для забезпечення їхньої діяльності при несприятливій економічній кон'юнктурі, затримці замовниками платежів за поставлену продукцію, нестачі коштів для погашення одержаної позики.

Але самострахування, за всієї своєї привабливості з погляду економії коштів, має низку недоліків:

у випадку катастрофічних збитків для їх покриття може не вистачити власних коштів, що викликає загрозу вимушеної ліквідації підприємства;

самострахування вимагає відволікання до резервів значних ресурсів, які перебувають у господарському обігу, оскільки вони не зосереджуються на окремому рахунку в банку;

на момент настання ризику в підприємства може не бути достатніх фінансових можливостей на покриття збитків;

---

[1]Страхування: Підручник / Керівник авт. кол. і наук. ред. С. С. Осадець. — К: КНЕУ, 2006. — 528 с.; Плиса В. Й. Страхування: підручник / В. И. Плиса. — К: Кравале, 2010 — 472 с.

самострахування вимагає кваліфікованого управління резервними фондами.

Фінансування ризику може бути також забезпечене за допомогою укладання договорів поруки, згідно з якими на певних умовах ризик передається одним суб'єктом іншому. Проте ця форма має обмежене застосування. Оскільки вимагає надзвичайно високої довіри між партнерами.

Найпоширенішою й найдоцільнішою формою організації страхового захисту майна підприємств є укладання договорів страхування з професійними страховими компаніями. Страховики, на відміну від поручителів, мають змогу вирівняти та перерозподілити ризики між багатьма суб'єктами. Перевагою вирівнювання ризиків за допомогою страхового механізму є те, що воно здійснюється не лише в часі, але й просторі, тобто серед суб'єктів певного середовища.

Умови страхування майна юридичних осіб, що пропонуються страховими компаніями, передбачають можливість страхового захисту не тільки майна, що належить підприємству, але й майна, що взяте в найм, лізинг, на зберігання переробку, комісію чи ремонт від фізичних та юридичних осіб.

Визначимо чіткіше можливі майнові інтереси, що не суперечать чинному законодавству і пов'язані з володінням, користуванням та розпорядженням такими видами майна:

- будівлями, спорудами, устаткуванням, інвентарем, товарно-матеріальними цінностями, готовою продукцією, сировиною, матеріалами та іншим майном, яке належить підприємству і відображено в його балансі;

- майно, отримане за договором лізингу, оренди (якщо воно не застраховане в орендодавця) чи прийняте від інших організацій і (або) населення.

Рухоме майно приймається на страхування і перебуває під страховим захистом тільки на території, указаній у договорі страхування.

При зміні місця перебування застрахованого майна підприємство повинно завчасно повідомити страховика й у випадку збільшення ступеня ризику сплатити додаткову премію, визначену страховою компанією.

На особливих умовах, визначених у договорі, страховик може взяти під страховий захист майно, незалежно від місця його перебування.

Резервуари (трубопроводи, апарати і т. п.), та інше технологічне обладнання потрапляють під страховий захист за умови, якщо вони пере-

бувають у тому технологічному зв'язку між собою і використовуються для тих речовин та матеріалів, які було відображено в заяві на страхування, технологічному регламенті, монтажно-технологічних схемах та в інших документах, що є доповненнями до договору страхування.

Страхова компанія дозволяє підприємству використати *вибіркове страхування.* Тобто застрахувати окремі майнові об'єкти на власний вибір.

Не приймаються на страхування предмети, факт знищення яких складно встановити: грошові знаки; цінні папери; вироби з дорогоцінних металів, напівдорогоцінного та дорогоцінного каміння; рідкісні та антикварні предмети; слайди та фотокартки; предмети релігійного культу; філателістичні колекції; документи, рукописи; майно, яке міститься в застрахованому приміщенні, але не належить страхувальникові.

У договорі вказуються страхові ризики, обсяг страхової відповідальності, винятки зі страхових випадків та обмеження страхування.

Так, страховими ризиками є:

1) знищення або пошкодження майна внаслідок пожежі, удару блискавки;

2) знищення або пошкодження майна внаслідок землетрусу, виверження вулкану та дії підземного вогню, гірського обвалу, цунамі, бурі, урагану, граду, сходження снігових лавин, злив, повені, сильного снігопаду, просідання ґрунту.

У договорі можуть бути передбачені й інші події:

- вибух газу, котлів, машин, апаратів; аварії опалювальної, протипожежної, водопровідної, каналізаційної систем;
- проникнення води із сусіднього приміщення;
- крадіжки.

Найчастішою з небажаних подій на підприємствах є пожежі. Тому при укладенні договорів більшим попитом користується ризик знищення або пошкодження майна внаслідок пожежі, удару блискавки.

Таке страхування називається пожежним. Хоча захист від комплексу ризиків (повний пакет страхового захисту) підвищує ступінь безпеки господарської діяльності підприємства. За погодженням сторін перелік страхових ризиків може бути розширений чи звужений.

Проте не відшкодовуються збитки, що виникли внаслідок таких причин:

1) обробка вогнем, теплом чи іншим термічним впливом на майно з метою переробки або в інших цілях (сушіння, зварювання, копчення, гаряча обробка тощо);

2) пошкодження тиском, що виник унаслідок вибуху, а також обробка вибухом чи тиском у виробничих чи інших цілях (зварювання вибухом, закріплення матеріалів вибухом, штампування тиском тощо);

3) використання вибухових речовин (динаміт, тротил тощо) та інших хімічних сполук або сумішей речовин, яким властиві швидкі екзотермічні реакції, що супроводжуються виділенням значної кількості тепла чи газів, спеціально призначених для проведення вибухів у тій чи іншій формах, або для екзотермічних реакцій у режимі теплового вибуху тощо;

4) груба недбалість чи намір страхувальника (у тому числі з метою збільшення розміру страхового відшкодування);

5) порушення встановлених законодавством або іншими нормативними актами правил та норм безпеки чи інших аналогічних норм;

6) неминучі в процесі роботи чи природно пов'язані з нею випадки самозаймання, корозії, гниття, природного зносу;

7) усякого роду військові дії, громадянська війна, народні збурення, страйки та їх наслідки, реквізиція, арешт, конфіскація, знищення чи пошкодження майна за розпорядженням цивільної чи військової влади;

8) дія бомб, мін, снарядів та інших знарядь війни;

9) радіоактивне забруднення та (чи) вплив ядерної енергії в будь-якій формі;

10) дія гризунів чи інших шкідників;

11) обвал будівель чи їх частин, якщо такий обвал не викликаний страховим випадком;

12) викрадення майна під час або безпосередньо після страхового випадку.

Метою встановлення таких обмежень є підвищення відповідальності страхувальника за збереження майна.

Підприємець може зазнавати втрат через ушкодження або знищення засобів виробництва, невиконання контрагентами умов договорів.

Окрім цього, можливі значні фінансові втрати через зниження заздалегідь обумовленого рівня рентабельності, через необхідність компенсувати шкоду, заподіяну найманим робітникам внаслідок не-

щасного випадку па виробництві, а також споживачам продукції цього підприємств (табл..3.1).

Таблиця 3.1

Класифікація підприємницьких ризиків

Ознаки класифікації	**Види підприємницьких ризиків**
Сфера виникнення	*Зовнішні,* не пов'язані з діяльністю підприємства (зміна законодавства, політики, соціального стану)
	Внутрішні, джерелом яких є господарська діяльність (розробка, виробництво і реалізація продукції, інвестиції, помилки керівництва і персоналу, зловживання, недотримання умов договору
Тривалість дії	*Постійні,* що загрожують підприємству в даній географічній зоні і в даній галузі економіки (ризики неплатежів у районах з депресивною економікою)
	Короткочасні, що діють у період часу, менший за виробничий цикл (ризики при транспортуванні продукції чи сировини)
Ймовірність	*Допустимі,* що загрожують втратою частини чи всього прибут-
	Критичні, що загрожують втратою прибутку і частини доходу
	Катастрофічні, що загрожують втратою бізнесу і банкрутством підприємця
Причина виникнення	*Спекулятивні (динамічні),* що виникають у результаті гри па курсових і цінових різницях
	Статистичні (прості), що виникають у результаті несприятливих факторів (стихійних лих, техногенних і антропогенних катастроф, аварій, нещасних випадків) і призводять до втрат

Розглянемо детальніше деякі з цих ризиків.

Політичний ризик - це можливість виникнення збитків чи скорочення розмірів прибутку, які є наслідком державної політики. Врахування такого ризику особливо важливе у країнах з нестійким законодавством, відсутністю традицій і культури підприємництва. Політичні ризики можна умовно поділити на: націоналізації й експропріації без відповідної компенсації, трансферта (зв'язаний із можливістю обмеження конвертації місцевої валюти), розриву контракту через дії

влади країни, де знаходиться компанія-коитрагент, військових дій. Політичний ризик може бути національним, регіональним і глобальним.

Технічний ризик визначається ступенем організації виробництва, наявністю превентивних заходів (регулярної профілактики обладнання, заходів безпеки), можливістю проведення ремонту обладнання власними силами фірми.

До таких ризиків відносять ризики втрат внаслідок негативних результатів науково-дослідних і конструкторських робіт, неможливістю досягнення запланованих технічних параметрів розробок і низьких технологічних можливостей виробництва. Технічний ризик відноситься до групи внутрішніх ризиків, оскільки виникнення його залежить від діяльності самого підприємства.

Виробничий ризик пов'язаний з виробництвом продукції, товарів і послуг та із здійсненням будь-яких видів виробничої діяльності, в процесі якої підприємці стикаються з проблемами неадекватного використання сировини, зростання собівартості, збільшення втрат робочого часу, використання нових методів виробництва.

Комерційний ризик це ризик, який виникає в процесі реалізації товарів і послуг, вироблених чи куплених підприємцем. Сюди відносять ризики, пов'язані з реалізацією товару (послуг) па ринку, його транспортуванням, з прийомом товару (послуг) покупцем, з платоспроможністю покупця та ризик форс-мажорних обставин.

Термін «підприємницькі ризики» визначає ті ризики, що пов'язані з майном підприємства, з життям і здоров'ям людей, які працюють на ньому, з виконанням зобов'язань у межах комерційної діяльності, з укладанням договорів, контрактів. Отже, страхування підприємницьких ризиків – це сукупність страхування майна, страхування відповідальності та особистого страхування.

За допомогою страхування створюються певні фінансові гарантії стабільності і прибутковості виробництва на випадок настання несприятливих. ситуацій у будь-якій підприємницькій структурі, що входить до складу ринкового механізму.

Нині значного поширення набуває страхування майна підприємств, пов'язане із забезпеченням страхового захисту матеріально-технічної бази виробництва. Це обумовлено необхідністю протидії навмисного знищення або ушкодження чужого майна при здійсненні силового рейдерского нападу. При страхуванні майна страхувальни-

ком може бути його власник або особа, яка отримала майно в користування, оренду, лізинг; на зберігання, під заставу тощо. До цього страхування входить багато видів, котрі найчастіше поділяються за об'єктами страхування і страховими випадками, а саме: страхування основних і оборотних фондів, страхування засобів транспорту, вантажів, електронних пристроїв, страхування машин і механізмів, страхування будівельно-монтажних ризиків, страхування машин від поломок.

Найпоширенішим і навіть традиційним видом страхування ризиків на підприємстві є страхування майна промислових підприємств від вогню та інших небезпек. Страхування від вогню полягає у відшкодуванні збитків від раптових і непередбачуваних випадків пожежі або вибуху, а також деяких інших супутніх явищ. За цим видом укладаються основний та додатковий договори страхування. За основним договором страхуванню підлягає все майно, що належить підприємству. Ставки страхових внесків за договорами страхування майна коливаються від 0,05 % до 0,5 % вартості майна (при страхуванні приміщень, меблів). При страхуванні обладнання промислових підприємств страховий збір коливається від 0,15 % до 1% їх вартості, а якщо страхуються дорогі марки автомобілів, то ставки страхових внесків можуть досягти 17 %.

Для повного відшкодування збитків, завданих основним і оборотним фондам, необхідна їх оцінка.

Основою для визначення страхової суми є дійсна вартість застрахованого майна на момент підписання договору, що визначається за балансовою вартістю та вартістю придбання з урахуванням зносу. Страхова сума не повинна перевищувати страхової вартості. Якщо вона менша, то страхувальник має право на відшкодування тільки тієї частини збитку, що відноситься до загальної суми збитку так, як страхова сума до страхової вартості. Йдеться про так зване «предстрахування». Страхувальник сплачуватиме меншу за розміром страхову премію.

Страхова вартість визначається:

для товарів, що виготовляє страхувальник (незавершеного будівництва та готової продукції), - це затрати на виготовлення аналогу;

для товарів, якими страхувальник торгує, сировини, яку страхувальник використовує для виробництва товарів, та природних ресурсів це ціпа покупки заміни;

для машин і устаткування витрати па придбання або відновлення застрахованого об'єкта аналогічного втраченому (за мінусом зносу);

для будівель і споруд--за вартістю будівництва будівлі чи споруди повністю аналогічної тій, що знищена, із урахуванням місцевості, техніко-експлуатаційного стану будівлі та її зносу.

При настанні страхового випадку страхове відшкодування виплачується після того, як повністю виявлено причини та розмір збитків. Розмір збитку в разі загибелі (руйнування) будівель, споруд та іншого майна, що належить до основних засобів, визначається на підставі повної балансової або договірної вартості, за якої вони застраховані, а в разі пошкодження цих об'єктів - на основі вартості відновлення (ремонту) і в межах страхової суми.

Витрати на відновлення враховують: витрати на придбання матеріалів та запасних частин для ремонту; витрати на оплату ремонту; витрати на доставку матеріалів до місця ремонту та інші видатки, необхідні для доведення пошкодженого майна до стану, що був перед настанням страхового випадку.

До суми збитку входять також втрати від пошкодження майна внаслідок заходів, що вживалися для його рятування, зберігання та впорядкування застрахованого майна після настання страхового випадку, виграти на складання кошторисів на відновлення пошкоджених об'єктів, проведення експертиз тощо.

Кількість і вартість майна, наявного па момент настання страхового випадку, визначається за даними бухгалтерського обліку і звітності та на підставі первинних документів про надходження та видатки, інвентаризаційних залишків невикористаних матеріалів. Після розрахунку розміру збитку, визначають розмір страхового відшкодування.

Страхове відшкодування виплачується:

– у випадку повної загибелі майна у розмірі дійсної (відновної) вартості з вирахуванням зносу та вартості залишків майна, придатного для подальшого використання, але в межах страхової суми;

– у разі часткового пошкодження майна - у розмірі різниці між заявленою страховою сумою та вартістю залишків майна, придатних для подальшого використання, а при страхуванні за відновною вартістю - в розмірі витрат па його відновлення, але не більше страхової суми.

Щоб вижити за цих складних умов підприємствам потрібно приймати нетрадиційні та сміливі рішення, що підвищує ступінь ризику. При зазначених обставинах підприємствам потрібно не уникати ризи-

ку, а вміти правильно оцінити його ступінь і безпосередньо управляти ним з метою недопущення настання збитків.

Пропонуємо сформулювати дієві шляхи поліпшення економічної безпеки підприємств, що дасть змогу підвищити рівень національної безпеки країни:

1) актуальним наразі є корегування моделі забезпечення національної безпеки, а також розбудова системи страхування ризиків підприємництва, організації належного функціонування і взаємодії державних і недержавних суб'єктів сектору страхового ринку України;

2) світовий досвід переконує в необхідності якісного нормативного забезпечення діяльності індустрії страхування та її співробітництва з державними та приватними підприємствами;

3) в рамках індустрії страхування підприємницьких ризиків доцільно створити об'єднання страховиків цього виду страхування, яке могло б сприяти захисту їхніх інтересів, реалізації стратегічних завдань становлення і розвитку страхових ризиків підприємництва та бути його громадським представником в суспільстві;

4) прискорене і не завжди рівноправне входження економіки України в систему міжнародних економічних зв'язків загострює питання зовнішніх впливів на підприємницьку діяльність. Набуває реального втілення тенденція, що проявляється в усіх країнах світу, що виражається в ефективному використанні страхових послуг, вдосконаленні методів їх творення, аналізу і матеріалізації в конкретний страховий продукт;

5) завданням першорядного значення для індустрії страхування має стати формування добре продуманої, чітко організованої інформаційної бази – інформаційної основи системи страхової діяльності. Ця інформаційна основа буде об'єднуючим, підтримуючим фактором для кожного із учасників при умові, коли вона постійно буде поновлюватись потрібною для підприємств інформацією, інформацією про ризики, про методику страхування, тенденції і небезпеки ринків тощо.

Для впровадження вищезазначених пропозицій потрібно виконати великий обсяг підготовчих заходів, зокрема вдосконалення розподілу повноважень та процедур прийняття рішень на державному рівні, контроль за виконанням рішень та використанням коштів, вдосконалення методів ведення фінансової звітності підприємств тощо. Тому у сфері страхування підприємницьких ризиків потрібно знайти оптимальне рішення щодо подальшого стимулювання страхування економічних суб'єктів найефективнішим способом.

В Україні страхування ризиків господарюючих суб'єктів ще недостатньо розвинене. А ось світовий досвід показує, що розглянутий вид страхування економічно вигідний і є щоденною практикою роботи підприємств.

3.3. Мінімізація ризику втрати права власності, шляхом рейдерського захоплення, завдяки використанню титульного страхування

Протидія рейдерству є найактуальнішою проблемою для економік країн пострадянського простору. Даний вид правопорушення не обійшов жодну країну світу, деякі країни (США, Німеччина, Великобританія) успішно «перехворіли» рейдерством і виробили власну, властиву цій державі систему заходів протидії. Інші держави (країни східної Європи) не можуть підібрати оптимальну систему сил і засобів для боротьби з цим негативним явищем і до сьогоднішнього дня.

Як відзначають автори монографії «Рейдерство: джерела, процедури, способи запобігання»[1] рейдерство негативно впливає на підприємницький клімат, сприяє дестабілізації роботи підприємств, руйнує трудові колективи, провокує конфлікти в суспільстві, формує несприятливий інвестиційний клімат і міжнародний імідж країни.

Рейдерство на сьогоднішній день є безкарним з боку держави правопорушенням, яке дозволяє привласнити підприємство та об'єкти нерухомості, що належать йому на праві власності. Протягом останніх декількох років жодного порушника права власності, жодну особу або компанію, які брали участь в рейдерському захопленні підприємств, установ, організацій не притягнуто до відповідальності. Хоча дане правопорушення супроводжується здійсненням кримінальних злочинів: підробка документів, шахрайство, дача хабаря, протидія законної господарської діяльності та інші.

У економічній та юридичній науці тривалий час йде дискусія з приводу способів протидії рейдерству. Дослідженням цієї проблеми займалися як вітчизняні, так і зарубіжні вчені. Достатньо пригадати

[1]Рейдерство : витоки, процедури, способи запобігання : монограф. / О.А. Бурбело, Г.В. Козаченко, Ю.С. Погорелов, С.О. Бурбело ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. − Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. − С. 83.

роботи Л.А. Андрєєва, З.С. Варналія, Ю.О. Борісова, О.І. Белікова, О.В. Бочарової, О.А. Бурбело, В.А. Горіна, В.С. Житомирського, А.В. Козаченко[1], В.І. Лазуренка, В.К. Мамутова, М.А. Сергеева та інших учених в цій області. Проте необхідно відзначити, що бракує комплексних досліджень по захисту майнових прав і способів мінімізації ризиків від здійснення такого виду правопорушення.

В Україні ринок нерухомості існує вже 20 років. За цей час був прийнятий ряд нормативно-правових актів, проголошені і закріплені основні правові інститути, такі як право власності, державна реєстрація нерухомості, правова регуляція рієлторських послуг. Втім, як це не прикро визнавати, відносини у сфері нерухомого майна надалі залишаються "найтемнішими» і невизначеними в правовому плані. Рієлторськая діяльність не потребує ліцензії, а, отже, і не передбачає чітких вимог до її здійснення. А де обертаються великі гроші, там завжди будуть охочі нажитися на довірливих клієнтах. Все це зумовлює достатньо великий інтерес до цієї діяльності у різних шахраїв, які, користуючись недосконалим законодавством і легковажністю громадян, одержують чималий «економічний ефект». Дійсно, закріпивши на законодавчому рівні інститут права власності, законодавець не зовсім продумав механізм захисту цього права. Особливо це стосується захисту права власності добросовісних набувальників нерухомості.

У класичному вигляді рейдерство з'явилося з введенням в обіг акцій, тому його пов'язують з переходом країн від адміністративно-планової економіки до ринкової. Завдяки акціям, які вільно обертаються на ринку, з'явилася можливість придбання підприємства без згоди його фактичного власника[2].

Проте, саме існування таких фактів ставить під сумнів законність права власності, і дуже часто є причиною визнання його недійсним. Як наслідок – добросовісний набувальник є вимушеним повернути придбану нерухомість, а повернення сплачених за майно засобів є

---

[1]Рейдерство : витоки, процедури, способи запобігання : монограф. / О.А. Бурбело, Г.В. Козаченко, Ю.С. Погорелов, С.О. Бурбело ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. − Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. − 184 с.

[2]Рейдерство : витоки, процедури, способи запобігання : монограф. / О.А. Бурбело, Г.В. Козаченко, Ю.С. Погорелов, С.О. Бурбело ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. − Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. − С. 28.

вже його особистою проблемою, оскільки стягнути їх (навіть на підставі рішення суду) є украй проблематичним.

Схожа ситуація існує у всіх країнах СНД. Конфлікт двох власників – законного і фактичного, розв'язується, як правило, на користь першого. Проте існує інститут захисту фінансових гарантій, який виявляється в страхуванні фінансових ризиків. Реальною гарантією захисту порушених інтересів добросовісного набувальника може стати страхування фінансового ризику втрати або обмеження права власності на об'єкт нерухомості або, як його ще називають, титульне страхування. Цей вид страхових послуг тільки розвивається на страховому ринку України, і компаній, які надають таку послугу не так вже і багато.

Наші російські партнери, в цій сфері мають деякий досвід. У них цей процес почався ще 1993 року, в кінці 90-х рр. такий вид послуг надавали багато страховиків, а в 2004-2005 рр. титульне страхування поступово стає буденним явищем на страховому ринку Росії.

Крім того, необхідно враховувати особливості самої тарифної політики відносно даного виду страхування. Адже, пожежі та стихійні лиха є явищами звичайними і всім зрозумілими, вірогідність їх настання і оцінка ризику є відомими більшості страховиків. Тарифна політика формується на фундаментальній статистичній базі в середовищі, де працюють закони математики, а ось, що таке втрата права власності за рішенням суду (з використанням протиправних дій рейдерів), як часто це буває, які чинники і яким чином впливають на вірогідність страхових випадків – на жаль, частіше за все є невідомим не тільки споживачу, але і самим страховикам. Тому лише деякі з останніх активно розвивають програми по страхуванню ризику втрати права власності.

Дієвим і економічно доцільним способом захисту майнових прав може бути титульне страхування, яке є страхуванням фінансового ризику втрати або обмеження права власності на об'єкт нерухомості. Тепер, цей різновид страхових послуг є новим на українському страховому ринку і надається лише невеликою кількістю страхових компаній, а проблематика титульного страхування права власності залишається практично недослідженою вітчизняною економічною і юридичною наукою.

У більшості розвинених країнах компенсації (відшкодування збитку) учаснику ринку нерухомості в чітко обумовлених випадках припадає на державу, а виплати здійснюються або за рахунок бюдже-

ту, або за рахунок засобів спеціалізованого фонду (але, якщо засобів фонду не вистачає, наступає субсидіарна відповідальність бюджету).

Також у країнах, де система реєстрації прав на нерухоме майно заснована на веденні Земельної книги, відповідальність за помилки реєстраторів несуть бюджети відповідних територіальних утворень, на території яких вони знаходяться, а у разі браку цих коштів наступає субсидіарна відповідальність, яка переходить на бюджети вищого рівня. Така система компенсації збитку колишнім власникам нерухомого майна характерна для Німеччини та Австрії.

Відмінною від вказаної вище системи компенсації збитків, є система, яка прийнята в Швеції. Шведське законодавство не передбачає створення для цих цілей спеціалізованих гарантійних фондів. Компенсація збитку учаснику ринку нерухомості здійснюється за рахунок загальних доходів бюджету, незалежно від підстави для здійснення таких виплат. За рішенням суду виплата може бути здійснена як добросовісному набувальнику (при цьому майно у нього вилучається), так і колишньому власнику нерухомості (якщо майно залишається у добросовісного набувальника).

Наприклад, у США (де перша титульна страхова компанія Law Property Assurance and Trust Society[1] була утворена ще в 1853 році) прийнята система реєстрації угод (актова реєстрація), при якій орган державної реєстрації не розглядає зміст угоди, не тлумачить юридичне значення прав, які можуть бути придбані, а лише реєструє документи, надаючи їм, таким чином, статус публічності і доступності для іншої зацікавленої особи. Така система не надає власникам гарантій їх права, лише робить незареєстровані документи менш значними, чим зареєстровані. Тому система державної реєстрації логічно доповнюється інститутом спеціалізованих титульних страхових компаній, які ретельно вивчають законність здійснення угоди з нерухомістю і відсутність неврахованих прав інших осіб. У разі висунення ким-небудь обґрунтованих претензій на нерухомість після відповідної судової процедури страхова компанія виплачує страхове відшкодування.

Потреба в титульному страхуванні є очевидною, адже, на ринку нерухомості в нашій країні стовідсоткову чистоту попередніх угод забезпечити достатньо важко. Також масштаб рейдерства дає підстави говорити про актуальність страхування ризиків втрати права власності.

[1]Title insurance in the United States // [Електронний ресурс] http://en.wikipedia.org/wiki/Title_insurance_in_the_United_States.

Слід зазначити, що до титульного страхування звертаються лише найосвіченіші учасники ринку, які через сформовану практику і внутрішні стандарти є вимушеними оцінювати і мінімізувати свої ризики.

Титульне страхування − найефективніший спосіб захистити свої майнові інтереси. Такий вид страхування передбачає гарантію повернення грошових коштів, якщо операцію покупки нерухомості визнають недійсною.

Зміст титульного страхування полягає в тому, що воно захищає від наслідків подій, які відбулися у минулому. До таких порушень відносяться: продаж по підроблених документах, перевищення повноважень представника учасника операції, недієздатність або нездатність розуміти значення своїх дій одним з учасників операції, розділ спадкового майна з порушенням інтересів окремих спадкоємців, здійснення операції з сумісним майном подружжя без згоди одного з них тощо.

Об'єктами титульного страхування є майнові інтереси страхувальника, які пов'язані: з нанесенням збитку його майновим правам в результаті позбавлення права власності на майно, на підставі рішення суду, що вступило в законну силу; з його судовими витратами по веденню в судових органах справ щодо заперечування свого права власності на це майно.

Предметом договору титульного страхування є: нерухоме майно, що є предметом іпотеки; житлові приміщення (житлові будинки або їх частини, квартири, кімнати, котеджі, садові будинки, дачі, ізольовані приміщення і т.п.); нежилі приміщення (споруди, будівлі, приміщення, їх частини, ізольовані приміщення, гаражі, будівлі виробничого, господарського, соціально-побутового та іншого призначення, розташовані на окремих земельних ділянках); незавершені законсервовані капітальні будови; підприємства як майнові комплекси; земельні ділянки.

Страховим випадком признається факт спричинення збитку страхувальнику в результаті втрати права власності на майно, відповідно до рішення суду, що вступило в законну силу.

Події по реприватизації великих металургійних підприємств і повернення їх в державну власність в Україні підтвердили, що право власності не є таким абсолютним, як його декларують в правовій науці. І ще раз примусили задуматися добросовісних набувальників про необхідність титульного страхування, яке є законною і ефективною гарантією захисту власного права на нерухомість.

На нашу думку, для більш швидкого упровадження інституту титульного страхування в Україні, необхідно прийняти відповідну правову базу, деталізувати і закріпити правовий механізм реалізації цієї послуги, визначити критерії і методи оцінки страхових ризиків титульного страхування. Також, доцільним є, інформування населення про судову практику у справах про визнання таких угод недійсними. Велика кількість рейдерских атак на крупні підприємства дає підстави стверджувати, що з часом рівень довір'я власників до титульного страхування виросте.

Також необхідно відзначить, що швидкий розвиток цього інституту стане надійною фінансовою гарантією захисту права власності, а також сприятиме стабільності і надійності операцій на ринку нерухомості.

Особливу увагу необхідно приділити терміну дії договору титульного страхування. Він укладається на термін від 3 до 10 років (саме стільки складає термін позовної давності для операцій купівлі-продажу нерухомості). Це означає, що договори страхування, які укладені через 10 років після здійснення угоди, не передбачають ніякого страхового захисту, оскільки судове рішення про визнання угоди незаконною вже не може бути прийнято.

Необхідно перерахувати основні чинники, які стримують активний розвиток титульного страхування в Україні:

− достатньо висока вірогідність визнання договорів, щодо відчуження земельних ділянок, недійсними;

− обережність страхових компаній відносно даного виду страхування в результаті його порівняної новизни, а, отже, і високої ризикованості;

− недосконаліть системи оформлення і реєстрації правозастосовних документів на земельні ділянки;

− складність отримання інформації щодо прав на земельні ділянки, а також дослідження і оцінки ризиків їх оскарження;

− наявність в українському законодавстві окремих категорій осіб, які мають загальні з власником права на нерухомість;

− юридична і організаційна складність титульного страхування порівняно із звичайним майновим страхуванням;

− недосконаліть земельного законодавства, що значно підвищує титульні ризики власників земельних ділянок, внаслідок чого страхові компанії вимушені встановлювати високу вартість страхування, тим самим, знижуючи на його попит;

− відсутність у більшості населення і бізнесу страхової культури, більшість громадян не усвідомлює вигідності страхування майнових ризиків;

− непоінформованість ріелторів, їх клієнтів і самих страхувальників з основами титульного страхування, з його перевагами і механізмами реалізації.

Можна з упевненістю стверджувати, що потенційна потреба в упровадженні титульного страхування в Україні є достатньо високої, адже як на ринку нерухомого майна, так і земельних ділянок в нашій державі стовідсоткову чистоту попередніх угод забезпечити достатньо важко.

Отже, надійним економіко-правовим інструментом, який успішно функціонує в провідних країнах світу і захищає права суб'єктів ринкових відносин, стає титульне страхування. Для більш швидкого упровадження інституту титульного страхування в Україні, необхідно активно розвивати і оперативно приймати відповідну нормативно-правову базу, деталізувати і закріпити економіко-правовий механізм реалізації цієї послуги, обґрунтувати критерії і науково-методичні основи оцінки страхових ризиків при титульному страхуванні.

РОЗДІЛ 4

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

4.1. Напрям забезпечення економічної безпеки залізничного транспорту

В умовах нестабільної економічної ситуації процес успішного функціонування і економічного розвитку підприємств України багато в чому залежить від вдосконалення їх діяльності в галузі забезпечення економічної безпеки. Економічна безпека характеризує можливості підприємства своєчасно і адекватно реагувати на зміни, які відбуваються в зовнішньому та внутрішньому середовищах. Крім того, економічна безпека підприємства є результатом умілого, обґрунтованого управління сукупністю внутрішніх чинників, які визначають результати діяльності підприємства. Безпека проявляється в процесі протидії підприємства негативним зовнішнім і внутрішнім обставинам, його реакції на зовнішні та внутрішні збурення, що виводять його зі стану рівноваги.

В якості чинників, які негативно впливають на економічну безпеку залізничного транспорту України, можна розглядати наступні: недостатність та неефективність держаної підтримки діяльності підприємств залізничного транспорту; неефективність законів; відсутність сприятливих умов для проведення науково-технічних досліджень; зростання розміру кредиторської заборгованості, зменшення обсягів перевезень, у тому числі транзитних; неефективність кадрової політики; корумпованість державних та галузевих структур; зростання конкуренції на внутрішньому ринку перевезень; невідповідність якості послуг європейським стандартам якості та технічно-експлуатаційної сумісності; низький рівень логістизації діяльності тощо.

Аналіз останніх досліджень та виділення невирішених частин загальної проблеми. В науковій літературі дослідженню економічної безпеки підприємств, побудові системи управління нею та інструментам забезпечення присвячено велика кількість праць. Ця проблема склала об'єкт дослідження таких вчених: Козаченко Г.В., Ейтутіса Г.,

Іскарової Н., Лянного Г., Ляшенко О. М. Компакова П., Коробчинського О., Тимофєєвої Т., Шевченко І., Шемаєва Л., Шинкаренко В.Г. та ін[123456789]. Значний обсяг теоретичних надбань вищезазначених вчених, все ж таки, достатньо повно не розкрив специфіку забезпечення економічної безпеки транспортних підприємств України.

Значення економічної безпеки у діяльності дуже велике і відіграє найголовнішу роль у забезпеченні позитивної динаміки його розвитку. Концепція економічної безпеки підприємства охоплює всі області виробничо-господарської діяльності. Для підвищення економічної безпеки підприємство залізничного транспорту, повинно:

1) забезпечити відповідність місії і стратегії своєї діяльності системі своїх пріоритетних інтересів;

2) визначити і оперативно коректувати пріоритети в діяльності підприємства і створення умов для їх реалізації;

3) забезпечити відповідності обсягу перевезень цього підприємства його ресурсному потенціалу і ємності ринку;

4) забезпечити внутрішню збалансованість у його діяльності;

5) знизити ризики в діяльності підприємства;

6) забезпечити зацікавленість персоналу в ефективності діяльності підприємства;

---

[1]Лянной Г. Система экономической безопасности предприятия // BOS — журнал о личной и коммерческой безопасности. — 2006. - №7. – С. 16-19.

[2]Колпаков П.А. Концептуальные основы экономической безопасности фирмы : автореф. дис. канд. екон. наук / П.А. Колпаков. — М., 2007.— 25 с.

[3] Коробчинський О.Л. Методика формування системи економічної безпеки підприємства // Актуальні проблеми економіки. — 2009. – № 4 . — С. 41-45.

[4]Шевченко І. Особливості формування економічної безпеки підприємства // Наука молода. - 2010. - №10. – С. 178-181.

[5]Воронкова А.Э., Козаченко А.В., Рамазанов С.К., Хлапенов Л.Е. Современные технологии управления промышленным предприятием. – Киев: Лібра . 2007. – 254 с.

[6]Козаченко А.В., Пономарев В.П., Ляшенко А.Н. Экономическая безопасность предприятия: сущность и механизм обеспечения : [монография]. — К. : Либра, 2003. — 280 с.

[7]Козаченко А.В., Пономарев В.П. Методические основы оценки уровня экономической безопасности предприятия // Региональные перспективы. — №2-3(9-10).-С. 104-106.

[8] Тимофєєва Т.О. Розробка механізму щодо забезпечення економічної безпеки залізничного транспорту: автореф. дис. канд. екон. наук: 08.00.03 — економіка та управління національним господарством / Т.О. Тимофєєва; Укр. держ. акад. залізн. трансп. — Х., 2009. — 20 с.

[9] Шинкаренко В.Г. Економічна безпека автотранспортних підприємств та їхня роль у роботі господарського комплексу України / В.Г. Шинкаренко // Збірник наукових праць НТУ. — 2009. Режим доступу до статті: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/81.pdf.10.

7) створити гнучку систему резервування ресурсів тощо.

Розглядаючи напрямки забезпечення економічної безпеки підприємств на прикладі залізничного транспорту, в їх складі слід виокремити:1) розвиток транспортної інфраструктури та міжнародних транспортних коридорів;2) впровадження швидкісних пасажирських перевезень;3) розвиток прогресивних технологій транспортування.

Модернізація транспортної інфраструктури з позицій забезпечення економічної безпеки має відбуватися на основі пріоритетності ліквідації явних «вузьких місць», модернізації та розвитку наявних потужностей у порівнянні із новим будівництвом. Значна частина наявної інфраструктури і технічних засобів, що забезпечують її функціонування, експлуатуються поза межами встановлених нормативних строків служби і є морально та фізично застарілими. При невисоких техніко-економічних параметрах та низькій надійності в експлуатації вони постійно потребують збільшення витрат на технічне обслуговування та ремонт, що здійснюється переважно за рахунок власних коштів залізниць.

Від технічного стану залізничної інфраструктури, її достатності та оснащеності залежать: розвиток економічних відносин; координація роботи залізничного транспорту та його взаємодія з іншими видами транспорту; швидкість і ефективність переміщення транспортних потоків; вартість та якість перевезень; екологічний стан; соціальні питання.

Розвиток транспортної інфраструктури має узгоджуватися із розвитком комунікацій енергетики, зв'язку, оскільки багатоцільове використання певних об'єктів може дозволити ефективно використовувати кошти, забезпечуючи тим самим економічне зростання, а, отже, і економічну безпеку. Стратегічне планування транспортної інфраструктури має враховувати такі її характеристики як довготривалість, широкомасштабність, рівень транспортних мереж, врахування інтересів та потреб інших видів транспорту.

Розвиток транспортної інфраструктури з точки зору економічної безпеки має здійснюватися з метою збереження та розвитку єдиного політичного, економічного та оборонного простору держави; вирішення комплексу геостратегічних задач, що дозволить посилити позиції держави у якості транспортного мосту між Європою, Азією та Америкою; досягти концентрації та економії ресурсів за рахунок побудови об'єктів багатоцільового призначення; стимулювання компле-

ксного освоєння перспективних ресурсних баз, а також здатності вирівнювання соціально-економічного розвитку регіонів[1].

Основними напрямками розвитку залізничної інфраструктури є наступні:

1) перебудова існуючих і побудова нових залізничних сполучень відповідно до стратегії розвитку економіки України;

2) поступове скорочення зайвих та малоінтенсивних ділянок мережі залізниць з метою приведення її у відповідність обсягам транспортної роботи і структурі виробництва;

3) підвищення технічного рівня колійного господарства шляхом нарощування обсягів всіх видів ремонтних робіт, впровадження нових технологій їх виконання, закупівлі сучасної ремонтно-будівельної техніки;

4) організація швидкісного і високошвидкісного руху поїздів на ділянках мережі за напрямками міжнародних транспортних коридорів та на магістралях, що з'єднують найбільші міста України;

5) модернізація існуючої мережі, в першу чергу, на ділянках швидкісного руху і міжнародних транспортних коридорів;

6) поступове наближення до міжнародних стандартів і вимог;

7) забезпечення максимальної безпеки руху;

8) впровадження ресурсозберігаючих технологій;

9) переоснащення депо відповідно до вимог технічного обслуговування та ремонту сучасного тягового і причіпного рухомого складу тощо[2].

Для України основними пріоритетами сьогодні є модернізація та комплексний розвиток транспортної мережі, у тому числі мережі транспортних коридорів. Їх наявність на території України накладає відбиток на функціонування всієї мережі транспортних комунікацій держави. Це зобов'язує її працювати синхронізовано, з більшою відповідальністю дотримуватися графіків роботи та доставки вантажів, забезпечувати впровадження європейських стандартів якості перевезень. Міжнародні транспортні коридори слугують передумовою сталого економічного зростання та підвищення конкурентоспроможності

---

[1]Козаченко А.В., Пономарев В.П. Методические основы оценки уровня экономической безопасности предприятия // Региональные перспективы. – №2-3(9-10).-С. 104-106.

[2]Шапочка М. К., Рибіна О.І. Проблеми та напрямки реструктуризації залізничної інфраструктури // Вісник Хмельницького національного університету. – 2010. – № 2, т.2. – С.44-48.

національної залізничної мережі. Їхній розвиток, поза сумнівом, поліпшить інвестиційну привабливість залізничного транспорту та підвищить ефективність інвестиційних процесів, стимулюватиме розвиток наукоємного виробництва та перехід на інноваційну модель розвитку, дасть змогу створити нові робочі місця, прискорить інші зміни у економіці залізничного транспорту.

Наступним напрямком забезпечення економічної безпеки залізничного транспорту України є розвиток швидкісних пасажирських перевезень. Пасажирські перевезення швидкісними магістралями на фоні світового загального скорочення довжини залізничних мереж постійно зростають, їх частка до 2020 р. складе 15% загального обсягу перевезень, що можливо за рахунок відтоку перевезень з автомобільного та повітряного транспорту. При виборі пасажирами виду транспорту найбільш пріоритетними є такі показники, як тривалість поїздки, частота оберту, якість обслуговування та вартість проїзду. Тому швидкісні залізничні перевезення є оптимальним видом, що дозволяє встанови баланс між параметрами якість, вартість, час перевезення. На сьогоднішній час високошвидкісні залізничні магістралі експлуатуються у Великобританії, Бельгії, Німеччині, Іспанії, Італії, Кореї, Франції, Японії. Незначні за довжиною високошвидкісні дільниці існують в Норвегії, Швеції, США, Тайвані. Будівництво високошвидкісної залізничної мережі в Україні:

— забезпечить комплексне вирішення транспортних проблем на важливіших напрямках пасажиро- та вантажопотоків, в т.ч. які входять в міжнародні транспортні коридори;

— сприятиме залученню країни до передових транспортних технологій, підвищить рівень технологічного прогресу галузі;

— сприятиме вирішенню екологічних проблем та збільшенню безпеки перевезень;

— сприятиме розвитку конкурентного середовища в транспортній сфері тощо.

Прискорення доставки пасажирів та вантажів неможливо без впровадження прогресивних технологій транспортування. Так для вантажних перевезень таким визначено, в першу чергу комбіновані перевезення. З точки зору забезпечення економічної безпеки залізничного транспорту вони дозволяють скористатися перевагами поєднання якостей двох домінуючих видів транспорту — маневреності, оперативності і швидкості автомобільного транспорту і великої продуктивно-

сті, всепогодності і безпеки руху залізничного транспорту. Це забезпечує збільшення вантажопотоку, швидкості, якості послуг. Розглядаючи переваги, які обумовлюють сьогодні актуальність розвитку контейнерних перевезень вантажів, можна виділити наступні важливі завдання:

— впровадження новітніх технологій перевізного процесу, що поєднають в собі відносно високу швидкість і помірну вартість доставки вантажів;

— здійснення організаційно-технічної роботи зі створення нових контейнерно-контейнерних терміналів та розвитку нових транзитних маршрутів даного напрямку перевезень в перспективних географічних напрямках;

— посилення екологічних вимог транспортним підприємствам вирішить питання економії енергоресурсів, попередження перевантаженості автодоріг і скорочення кількості дорожньо-транспортних пригод;

— можливість застосування до експортних та імпортних контейнерних перевезень спрощених митних процедур і лояльних тарифних ставок.

— гарантування безпеки та збереження вантажів під час руху незалежно від погодних умов.

Для організації і широкого впровадження системи контейнерних перевезень в Україні необхідно покращити взаємодію автомобільного і залізничного транспорту.

Вирішенню цієї задачі повинні сприяти такі організаційно-технічні заходи:

— створення транспортно-експедиторських фірм (з відділеннями в початкових і кінцевих пунктах контейнерних маршрутів), що відають питаннями формування поїздів, їх відправлення, приймання, навантаження, розвантаження і доставки контрейлерів. Такі фірми повинні володіти терміналами для обробки поїздів на кінцевих станціях, парком контрейлерів, автотягачами і спеціалізованими залізничними платформами.

При цьому необхідно враховувати, що типи і оснащення терміналів залежать від конструкції спеціалізованих платформ, які використовуються для перевезення контрейлерів, і що в ряді випадків (або ж систематично) контейнерні термінали сполучаються з контейнерними пунктами.

— визначення кінцевих і проміжних пунктів, між якими необхідно здійснювати регулярні контейнерні перевезення з рухом поїздів за спеціальними маршрутними графіками.

Таким чином, забезпечення економічної безпеки залізничного транспорту вимагає активізації зусиль керівництва галузі в напрямках забезпечення розвитку міжнародних коридорів, впроваджені прогресивних технологій транспортування, організації швидкісного руху залізницями України. Такі заходи мають позитивно вплинути на якість послуг залізничного транспорту, його відповідність сучасним потребам вантажовласників та європейським стандартам транспортування, забезпечити конкурентоспроможність залізничного транспорту України на вітчизняному та міжнародному ринках перевезень.

4.2. Чинники, що впливають на економічну стійкість підприємства

Якість рішень, що приймаються, з забезпечення стійкості і здатності підприємств виживати, в значній мірі визначається мірою обізнаності керівництва про фактично існуючі і назріваючі загрози зсередини і ззовні підприємства[1]. Непоінформованість веде до прийняття рішень, що містять у собі ту бо іншу частку ризику неотримання тієї запланованої віддачі, яка мала була статися від введення в дію запланованих ресурсів. Якщо виходити з головних цілей підприємства, під ризиком потрібно розуміти виникнення несподіваної кризової ситуації, внаслідок чого не буде отримано, наприклад, очікуваного прибутку, що у підсумку приведе економіку підприємства до втрат. Якщо ці втрати виявляться дуже високими і будуть мати стійкий характер, то підприємство втратить стійкість і, зрештою, припинить своє існування внаслідок банкрутства.

Чинник ризику, як слідство складності, і непередбачуваність характеру середовища функціонування підприємства грають в ринкових умовах господарювання вельми важливу роль.

У розвинених країнах це пов'язано із зростаючою невизначеністю поведінки ринку внаслідок ряду причин: зростаюча небезпека старіння цілих виробничих галузей в зв'язку з обвальними за своїми мас-

[1] Александров І.О. Моделі економічної динаміки і система національних розрахунків. – Донецк: ІЕП НАН України, 1998. – 100 с.

штабами і глибиною технологічними змінами; всезростаюча неможливість прогнозування купівельного попиту в зв'язку з нестабільністю схильностей, що посилюється, і переваг покупців; витрати часу, що все збільшуються на дослідження і розробки при життєвому циклі знову зробленого продукту, що скорочується.

В умовах української економіки дія цього чинника пов'язана поки що головним чином з відомою нестабільністю і досить складним станом економіки загалом.

Очевидно, що незалежно від причин, які викликають необхідність підвищення інформаційної "пильності" підприємств, кожне з них, будучи благополучним або з кризовими симптомами, повинно враховувати неминучість виникнення ризикових ситуацій, які можуть привести до збоїв в його роботі або до ще більш серйозної дестабілізації.

Стійкість реального сектора економіки з неминучістю означає його орієнтацію на розширене відтворювання, тобто на виконання двох необхідних умов збалансованого функціонування і розвитку: умови стійкого простого відтворювання виробничих фондів в масштабах національного технологічного контуру; умови збалансованого зростання основних фондів, зберігаючи умови простого відтворювання і забезпечення зростання виробництва продукції реального сектора.

Ці умови, нажаль, сьогодні порушені. Відсутність економічного зростання, значна нерівномірність прибутків, як по галузевій вертикалі, так і по територіальній і демографічній горизонталям з непрямими індикаторами порушення умов збалансованого функціонування економіки.

Характерно, що порушення кожного з вищезазначених умов зумовлене дією позитивних зворотних зв'язків, що створюють в системі економічних взаємодій систему так званих хибних кіл, які роблять виконання цих умов недосяжними. Таким чином, закріплюється несприятлива ситуація в економіці.

До числа причин, що обумовлюють нестійкий стан сучасних підприємств і утруднюють процес управління ними, потрібно віднести[1]:

1. Нерегульоване ціноутворення в умовах неефективності конкурентних шляхів задоволення життєво важливих суспільних потреб приводить до збільшення темпів інфляції. Істотним елементом механі-

[1]Геєць В. Економічні реформи в Україні: моделі, реалії та уроки // Банківська справа. – 1996. – № 4. – С. 26-33.

зму ціноутворення при цьому є позамежна рентабельність окремих ланок технологічного контуру.

2. Високотехнологічна й інша імпортна продукція машинобудівного профілю, домінуючи на внутрішньому ринку, порушує збут і виробництво вітчизняних аналогів, що мають в своїй вартості порівняно велику частку невиробничих витрат (посередницькі витрати, чистий прибуток і т.д.).

3. Прагнення банків залучити в фінансовий сектор вільні кошти встановлює банківський процент, вищий за темп інфляції. Цей процент в умовах великої інфляції виявляється стійко вищим за прибутковість інвестицій в реальний сектор, що блокує ці інвестиції за рахунок кредитів. Підтримка протягом тривалого часу високого банківського процента (вище за 25%) приводить до непродуктивних витрат оборотних коштів підприємств.

4. Взаємодія державного і приватного секторів носить принципово несиметричний характер, оскільки обидва функціонують за різними правилами.

5. Впровадження ринкових відносин в сферу державних механізмів супроводжується перетіканням коштів, які не контролюються, в приватні руки, падінням ефективності державних витрат.

Об'єктивними джерелами загроз втрати стійкості підприємства є його навколишнє середовище і структура внутрішніх чинників виробництва. Загрози втрати стійкості можуть бути представлені наступною класифікацією:

По джерелах виникнення:

зовнішні загрози, що створюються зовнішнім, навколишнім середовищем (мікросередовища) підприємства;

внутрішні загрози, що створюються внутрішнім середовищем підприємства.

По інституціональних джерелах виникнення:

глобальні загрози, що створюються глобальним навколишнім середовищем (глобальними параметрами або тенденціями розвитку світу);

національні загрози, зумовлені національним навколишнім середовищем;

регіональні загрози, що створюються регіональними параметрами і тенденціями розвитку;

місцеві загрози, зумовлені місцевими умовами;

локальні загрози, що створюються макросередовищем суб'єктів національної економіки.

По причинно-наслідкових зв'язках:

первинні загрози, зумовлені першоджерелом загрози;

вторинні загрози, що створюються взаємодією декількох первинних загроз.

По відношенню до інтересів людей:

об'єктивні загрози, що формуються незалежно від цілеспрямованої діяльності людей;

суб'єктивні загрози, що створюються свідомо окремими групами людей, виходячи з їх інтересів.

По видах загроз:

політичні загрози, що створюються політичними процесами і рішеннями політичних органів і партій;

соціальні загрози, зумовлені соціальними процесами або діями окремих соціальних груп (конфліктами, протистоянням і т.п.);

релігійні загрози, що створюються діями релігійних організацій, канони яких не співпадають з інтересами інших релігій;

економічні загрози, що викликаються економічними процесами;

правові загрози, зумовлені законодавчими процесами або відповідними актами законодавчих органів;

екологічні загрози, що створюються екологічними процесами або екологічними інтересами людей;

технологічні або техногенні загрози, зумовлені відмовами систем техногенного характеру;

інформаційні загрози, що створюються відсутністю достовірної інформації або її спотворенням по об'єктивних або суб'єктивних причинах.

По характеру впливу;

прямі загрози, що надають безпосередній вплив на параметри об'єкта або на його чинники виробництва;

непрямі загрози, характер впливу яких виявляється непрямим шляхом, тобто, через їх вплив на прямі загрози.

За масштабом впливу;

загальнопланетарні загрози, вплив яких носить глобальний характер, наприклад, загрози екологічного характеру, зумовлені зміною клімату на планеті;

національні загрози, вплив яких виявляється в масштабі всієї країни;

регіональні загрози, характер впливу яких має масштаб регіону;

інституціональні загрози, вплив яких виявляється в масштабі інституціональних утворень країни;

приватні загрози, вплив яких виявляється лише в масштабі окремих суб'єктів національної економіки.

По імовірності вияву:

реальні загрози, вияв яких має достовірний характер;

вірогідні загрози, вияв яких носить вірогідний характер, що оцінюється високою мірою імовірності;

З представленого списку видно, що в основі класифікації загроз втрати стійкості підприємства лежать дві основні ознаки, а саме: причини їх виникнення і вплив загроз на його параметри, що вельми важливо для їх аналізу. оцінки наслідків при вияві загроз і управління ними або попередження загроз для забезпечення безпеки підприємства.

Як було сказано раніше, одним з основних чинників, пов'язаних з необхідністю розробки комплексу заходів, направлених на забезпечення стійкого функціонування і розвитку підприємства, є невизначеність середовища функціонування підприємства, а також пов'язаний з цим вплив на діяльність підприємства – чинника економічного ризику. Уникнути економічного ризику неможливо, тому необхідно в процесі планування і організації діяльності підприємства визначити найбільш значущі чинники, що впливають на процес прийняття рішень, джерела і величину виникнення ризику і збитку від появи ризикових ситуацій, і далі вже на цій основі розробити комплекс заходів щодо захисту від ризику і забезпечення діяльності підприємства.

Всі можливі чинники ризику можливо поділити на дві групи. До першої групи відносяться ті, що передбачуються, тобто відомі з економічної теорії або господарської практики. Разом з тим можуть з'явитися чинники, виявити які на апріорній стадії аналізу чинників ризику підприємства нереально. Ці чинники відносяться до другої групи. Одне із завдань полягає в тому, щоб, створивши регулярну процедуру виявлення чинників ризику, звузити коло чинників другої групи і тим самим послабити вплив так званої неповноти генерації чинників ризику.

Найбільший інтерес в контексті проблем, що розглядаються в роботі, представляє класифікація економічного ризику в залежності

від місця виникнення - зовнішні по відношенню до підприємства ризики і внутрішні ризики (рис. 4.1)[1].

До зовнішніх чинників ризику відносяться чинники, зумовлені причинами, не пов'язаними безпосередньо з діяльністю даного підприємства, що залежать від економічного і політичного стану країни. Це імовірність жорстких урядових заходів, які можуть викликати зміни фінансово-економічної діяльності підприємства, податкової політики, розвитку інфляційних процесів, що не контролюються. Дані слабкі сигнали на момент формування бюджету можуть бути ще приховані, але підприємство все одно зобов'язано оцінити їх вплив за допомогою експертних оцінок або методів кількісного прогнозування і моделювання.

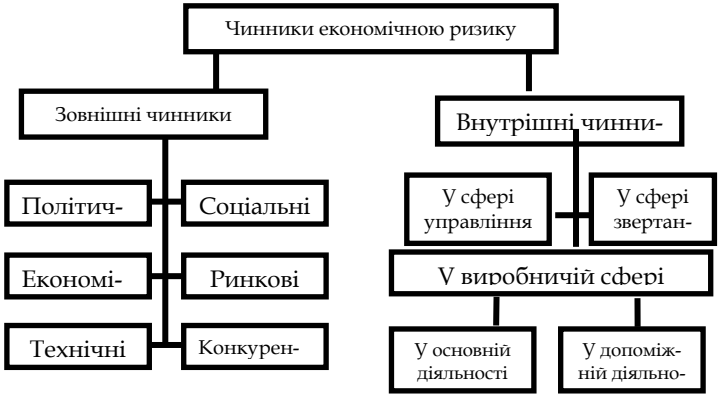


Рис. 4.1. Класифікація чинників економічною ризику, що впливають на економічну стійкість підприємства

Зміни у зовнішньому середовищі - відправна точка в аналізі зовнішніх чинників. Вивченню, аналізу і оцінці даного середовища приділяється велика увага, оскільки вона впливає істотним чином на результати діяльності підприємства загалом.

Основний етап аналізу зовнішніх чинників - їх виявлення. Існують різні джерела інформації про назріваючі сильні сигнали зовнішнього середовища, які являють собою зміни у зовнішній середі. До їх числа відносяться:

[1] Гиг Дж. Ван. Прикладная общая теория систем. – М.: Мир, 1981. – С. 345.

1. Зменшення ролі уряду як замовника невиконання контрактів, припинення НДДКР і освоєння.

2. Зміна структури споживачів.

3. Падіння середніх прибутків населення або прибутків підприємства.

4. Зміна цін, інфляція.

5. Неплатоспроможність споживачів.

6. Зміна структури прибутків і витрат підприємства і населення.

7. Скорочення життєвого циклу товарів.

Наступний етап аналізу зовнішніх випадкових чинників полягає в оцінці впливу потенційних змін зовнішнього середовища на майбутні результати діяльності підприємства. Наслідки можуть бути позитивними, тобто досягаються цілі, які намічаються, і поліпшуються результати його діяльності, або негативними, тобто виникають втрати, гіршають результати, або те й інше.

Далі по кожному можливому варіанту розвитку подій, пов'язаному з виявом дії того або іншого зовнішнього чинника, потрібно дати оцінку швидкості прийняття рішень і часу отримання результату.

Швидкість прийняття рішень (швидкість реагування) може бути класифікована таким чином: висока, якщо керівництво підприємством може негайно реагувати на події; середня, якщо реакцію у відповідь можна відкласти до наступного планового періоду; низька, якщо за оцінками, які є, реакцію у відповідь можна відкласти на невизначено довгий термін або доти, поки не буде отримана більш точна оцінка вірогідних наслідків.

У кожному конкретному випадку зовнішні чинники мають бути розділені на неістотні, які можна виключити з подальшого розгляду, та істотні з високою, середньою і низькою швидкістю реакції. Таким чином, сильні сигнали розподіляються за мірою важливості очікуваних наслідків. У результаті виходить перелік ключових зовнішніх сигналів, що коректується виключенням з нього сигналів, на які знаходяться відповіді, і внесенням замість них нових. Така методика виявлення ключових зовнішніх чинників допомагає скоротити їх перелік, а також визначити пріоритети в рамках ресурсів, які є.

В умовах зовнішнього і внутрішнього середовища, що змінюється, реагування на зовнішні чинники необхідно об'єднати зі стратегічним плануванням.

Результатами такого планування можуть бути:

комплекс оперативних програм і кошторисів поточної діяльності підприємства, направлений на виконання найближчих завдань;

ряд стратегічних задач, представлених у вигляді програм змін.

Внутрішніми чинниками ризику вважаються чинники, поява яких породжується діяльністю самого підприємства, тобто ризики, пов'язані безпосередньо з об'єктом: невиконання зобов'язань постачальниками, невчасна оплата продукції споживачами, оформлення кредитів дочірніми товариствами під поручительство підприємства та інші.

Як і раніше, при дослідженні чинників зовнішнього середовища підприємства увага має бути приділена аналізу цих чинників. До числа таких чинників, насамперед, потрібно віднести: 1. Зміна структури виробництва. 2. Дорожчання сировини та комплектуючих матеріалів. 3. Збільшення собівартості продукції і ціни її реалізації. 4. Повільне зростання середньої заробітної плати. 5. Збитковість товарів. 6. Відповідність активів і власних активів нормативним значенням.

При аналізі внутрішніх чинників необхідно враховувати, що наслідки можуть бути як позитивними, так і негативними.

Наступний етап аналізу зовнішніх чинників - вибір способу реагування на них.

Є істотна відмінність між проблемами, пов'язаними із зовнішніми чинниками, і проблемами, пов'язаними з внутрішніми. Перші вимагають розробки програми черговості дій, тоді як другі повинні вирішуватися на основі використання економічних і технічних засобів підприємства, резервів і фондів, які є в його розпорядженні. Замість того, щоб чекати повної інформації, керівництву підприємства потрібно визначити, які послідовні кроки в плануванні можуть бути зроблені при різному розвитку подій. По мірі надходження конкретної інформації будуть конкретизуватися і заходи у відповідь, кінцевою метою яких має стати або усунення небезпеки, або використання можливостей, що з'явилися. Як і у випадку із зовнішніми чинниками, наслідки дії внутрішніх чинників на результати діяльності підприємства можуть бути або позитивними, або негативними.

Виявлення, аналіз і оцінка чинників ризику є досить важливим етапом в процесі реагування керівництва підприємства на зміни зовнішніх і внутрішніх умов його функціонування. Це лише перша фаза складного процесу управління ризиком, під яким потрібно розуміти процес підготовки і реалізації заходів для зниження небезпеки помилкового рішення і зменшення можливих негативних наслідків небажа-

ного розвитку подій в ході реалізації прийнятих рішень. У реальних господарських ситуаціях можуть використовуватися різні способи зниження рівня ризику; що впливає на ті або інші сторони діяльності підприємства. Все різноманіття методів управління ризиком, що застосовуються в господарській практиці підприємств, стосовно проблеми, що вирішується в роботі, можна розділити на три типи (рис. 4.2)[1].

Рис. 4.2. Класифікація методів управління ризиком

Оскільки ризик - категорія імовірнісна, то для його оцінки використовуються статистичні, експертні методи оцінки і побудова моделей випадкових процесів[2][3].

Підприємства найчастіше використовують статистичний і експертний методи. При виборі методу оцінки ризиків враховуються переваги і недоліки кожного методу. Так, перший метод оцінки вимагає великого обсягу статистичної інформації за тривалий період часу.

[1] Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем: Пер. с англ. М.: Мир, 1973. – 344с.

[2] Уемов А.И. Системный подход и общая теория систем. М.: Наука, 1978. – 196с.

[3] Садовский В.Н. Основания общей теории систем. М.: Наука, 1974. – 254с.

Точність останнього методу залежить від прийнятих в моделі допущень і від числа чинників, які враховуються моделлю.

Для оцінки міри ризику, що впливає на підприємства, під яким також можна розуміти рівень нестабільності підприємства, можуть бути використані різні методи. Статистичний метод вимагає наявності значного об'єму даних, які далеко не завжди є в розпорядженні керівництва підприємства.

При відсутності інформації вдаються до інших методів, наприклад до експертних. Алгоритм вибору методів управління економічною стійкістю на основі результатів аналізу чинників зовнішнього середовища і його фінансово-економічного стану підприємства, що пропонується в роботі, представлений на рис. 4.3.

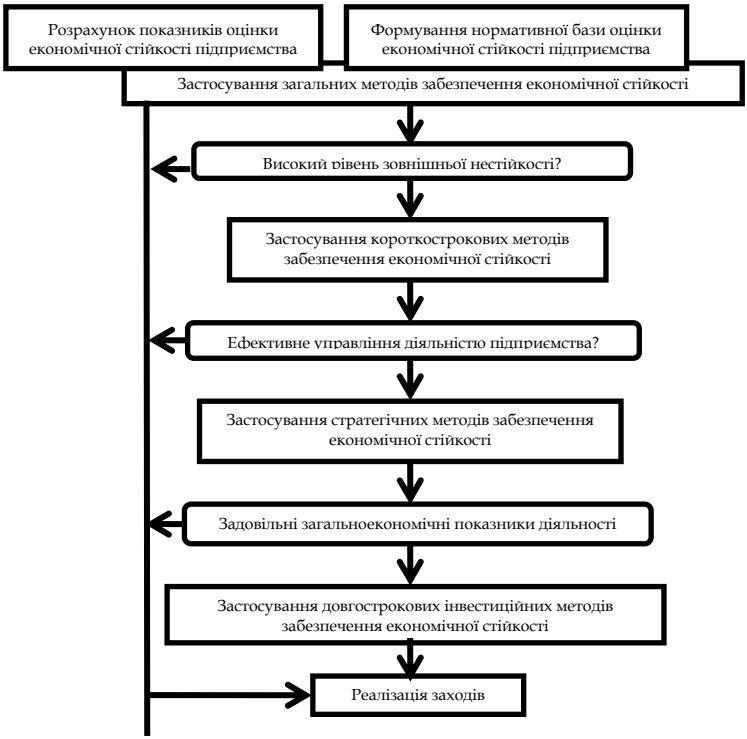


Рис. 4.3. Алгоритм вибору методів забезпечення економічної стійкості.

Алгоритм включає наступні етапи:

Перший етап. Усунення зовнішніх чинників, що впливають на економічну стійкість підприємства. Мета застосування методів першого етапу - доведення коефіцієнта поточної ліквідності і забезпеченості власними оборотними коштами до нормативного рівня.

Оперативні методи відновлення платоспроможності:

вдосконалення платіжного календаря; регулювання рівня незавершеного виробництва;

переклад низькообертових активів у високооборотні;

переоформлення короткострокової заборгованості в довгострокову;

проведення інших оперативних заходів.

Другий етап. Проведення локальних заходів щодо поліпшення фінансового становища. На другому етапі застосовуються наступні методи:

встановлення шляхів припинення штрафних санкцій на прострочену кредиторську заборгованість;

забезпечення достатнім об'ємом фінансових ресурсів для покриття знову виникаючих поточних зобов'язань;

поступове погашення старих боргів.

При реалізації методів другого етапу оцінюється можливість залучення додаткових внутрішніх джерел фінансування. До таких джерел відносяться: реалізація непотрібних і невживаних високооборотних активів, скорочення витрат до мінімально допустимого рівня, проведення енерго- і ресурсозберігаючих заходів.

Третій етап. Створення стабільної фінансової бази.

Застосування методів забезпечення економічної стійкості третього етапу вимагає залучення додаткових інвестицій. Метою довгострокових методів фінансового оздоровлення є забезпечення стійкого фінансового положення підприємства в довгостроковій перспективі - створення оптимальної структури балансу і фінансових результатів, стійкості фінансової системи підприємства до несприятливих зовнішніх впливів.

Встановлення значущості впливу зовнішніх чинників на показники діяльності підприємства, які характеризують рівень його економічної стійкості на базі відповідної системи показників, може бути визначене експертним шляхом - оцінкою міри значущості кожного чинника у відповідній групі показників.

4.3. Показники і методи оцінки економічної стійкості підприємства

Важливим завданням аналізу діяльності підприємств як відкритих систем є обґрунтування критерію вибору, тобто розв'язання питання про те, яким чином порівнювати між собою різні варіанти управлінських рішень, що приймаються[1].

Критерій, як ознака якості рішень, що приймаються, є адекватним відображенням інтересів суб'єктів і об'єктів управління. У моделі підприємства планової економіки як «закритої системи» варіанти рішень, що приймаються, відображали тільки народногосподарські інтереси, а як універсальний критерій використовувалася приведена вартість сукупних витрат.

У сучасних підприємств, як суб'єктів системи ринкових відносин, істотно ускладнюються зв'язки з об'єктами і суб'єктами зовнішнього середовища. Необхідність обліку різних чинників, що носять складний випадковий і недетермінований характер, ускладнює процедуру оцінки і вибору варіантів рішень настільки, що їх треба синтезувати по багатьох цілях альтернатив вибору. Цей синтез проводиться або на основі виявлення взаємозалежності показників, що аналізуються, або на основі експертних оцінок.

У цей час переважають два основних підходи до відповіді на питання, що розуміти під визначенням стійкості підприємства. Згідно з першим підходом, зростання стійкості виробництва ототожнюється зі зниженням коливань його результатів. Згідно з другим, суть стійкості зв'язується з цільовою спрямованістю відтворювання, а тому із задоволенням певного набору конкретних потреб при мінімальних витратах, виходячи з готівкових ресурсів і реальних можливостей їх ефективного використання.

Для найбільш повного задоволення різних потреб необхідне дотримання певних пропорцій в розвитку виробництва, причому ця пропорціональність повинна бути неперервною і змінюватися відповідно до зміни структури потреб. У такому випадку стійкість повинна розглядатися як здатність економічної системи безперервно підтримувати оптимальну пропорціональність в розвитку на різних рівнях.

---

[1] Ильичев А.В. Эффективность проектируемой техники: Основы анализа. – М.: Машиностроение, 1991. – 336 с.

Однією з основних проблем оцінки економічної стійкості сучасних підприємств є недостатня методична підтримка, відсутність у економістів підприємств якісного інструментарію вибору різних варіантів управлінських рішень.

В розробці методичного апарату оцінки економічної стійкості підприємства є декілька проблем[1]: 1) визначення набору індикаторів оцінки стійкості; 2) відсутність граничних критичних значень показників стійкості; 3) недостатня інформаційна статистична база для проведення аналізу стійкості; 4) недосконаліть методів розрахунку сукупного ризику втрати стійкості; 5) інтерпретації отриманих результатів оцінки стійкості.

Як один з можливих варіантів розв'язання зазначеної проблеми, пропонується підхід, що дозволяє за допомогою процедур моделювання давати комплексну оцінку стійкості розвитку виробничої системи. Формально функціонування системи описується набором показників, в якому відбиваються об'ємні значення ресурсів (трудових, матеріальних, фінансових), що переробляються, і результатів, що отримуються (матеріальних, фінансових, соціальних). Природно, що для аналізу стійкості функціонування системи ці показники мають бути представлені у вигляді тимчасових рядів, оскільки саме поняття стійкості поза зв'язком з часом втрачає всіляке значення.

Суть підходу полягає в порівнянні реальних показників господарської діяльності виробничої системи з ідеально можливими (плановими, очікуваними), які формуються на основі аналізу діяльності підприємства і прогнозних оцінок основних параметрів його функціонування. Порівняння відбувається через згортку всіх розрахункових показників в єдиний інтегральний показник, названий результативністю роботи. Перевагою підходу, що пропонується, відносно існуючих, є можливість отримання оцінки стійкості розвитку виробничої системи за будь-яким апріорно заданим критерієм і співвідношенням оцінок, що отримуються по різних критеріях.

Окремим питанням є формування інтегрального критерію оцінки стійкості виробничої системи. Як правило, критерій визначається метою дослідження і багато в чому залежить від тих питань, відповіді на які треба отримати. Формально заданий інтегральний критерій оцінки відображає порядок розташування локальних показників госпо-

[1] Барановский В.К. Концепция перехода Украины на модель устойчивого развития // Проблемы теории и практики управления. – 1998. - №5. – С. 23-24.

дарської діяльності в наборі, що характеризує той або інший її аспект. Розташування показників один відносно до одного визначається укладеним в них економічним значенням. Так очевидно, що зростання обсягів виробництва за певний період часу має випереджати зростання інвестицій в цю виробничу систему, а, наприклад, прибуток, що отримується, повинен рости більш швидкими темпами, ніж собівартість і величина інвестицій. Зіставляючи, таким чином, відібрані для аналізу показники по всій сукупності, одержуємо ранг кожного показника відносно всіх інших.

Внаслідок ранжування формується ідеальний порядок (норматив) проходження показників, який формально відображає прийнятий критерій оцінки. Необхідно зазначити, що при зміні критерію весь порядок розрахунку підсумкової оцінки ефективності по моделі, що пропонується, зберігається незмінним, змінюється тільки взаємне положення показників в нормативі один відносно одного, а це дозволяє говорити про деяку універсальність підходу до оцінки стійкості виробничої системи.

Можливі наступні варіанти реалізації підходу, що пропонується. Перший - це оцінка стійкості розвитку виробничої системи на основі аналізу структури економічних і соціальних показників за певний період часу. Показники представляються у вигляді тимчасових рядів. Природно, що чим довший тимчасовий ряд, тим точніше оцінка, що отримується.

Для кожного моменту часу визначається результативність роботи в залежності від стану структури системи показників, що розглядається. Це дозволяє згорнути різнорідні показники, які характеризують об'єкт дослідження, в один безрозмірний показник, що відображає якісну характеристику сукупності.

Визначивши результативність роботи по заданому критерію для кожного моменту часу, можна отримати інтегральний показник результативності - міру реалізації виробничих можливостей. Залишається тільки співвіднести розраховане значення з нормативним - це і буде кількісна оцінка стійкості виробничої системи, яка розглядається. Природно, що ця оцінка буде відносною, але з урахуванням того, що дана методика застосована до виробничих систем різного масштабу, які функціонують в різних організаційних та інших умовах, оцінки, що отримуються, порівнянні між собою.

Інший варіант моделі дозволяє дати прогноз ефективності майбутньої господарської діяльності і стійкості системи. На основі існуючих методик визначаються значення показників, включених в набір для прогнозу, і виконується розрахунок, аналогічний попередньому варіанту для майбутніх періодів.

За підсумковою оцінкою визначається ефективність передбачуваної стратегії розвитку і дається оцінка стійкості. Оскільки розглядається ефективність господарської діяльності в майбутніх періодах, то з'являється можливість моделювання процесу, пошуку кращих варіантів стратегії за критерієм стійкості.

Цілком природно, що підхід, який пропонується, не вільний від недоліків. Наприклад, важко врахувати численні аспекти ринкової кон'юнктури, її мінливість і слабку передбачуваність.

Однак велика частина недоліків зумовлена не суттю підходу і інструментарію для його реалізації, а тим початковим матеріалом, який використовується для реалізації процедури оцінки рівня стійкості. Зокрема, це стосується показників, які застосовуються для розрахунків. Більшість з них має вартісну природу, а, отже, і можливість неоднозначного і широкого тлумачення їх суті.

У цей час кожне підприємство вимушене визначити для себе найбільш відповідний набір критеріїв оцінки ефективності своєї діяльності і на його основі визначати міру її стійкості і розробляти заходи щодо управління стійкістю.

Багато в чому вибір таких критеріїв залежить від фази життєвого циклу підприємства - на різних етапах життєвого циклу підприємства змінюється значущість, а також характер поведінки показників різних груп. Запропонований підхід дозволить акцентувати увагу керівників і фінансових аналітиків на тих показниках, аналіз яких найбільш важливий на конкретному етапі функціонування і розвитку підприємства. Значущість фінансових показників на різних етапах життєвого циклу підприємства представлена в табл. 4.1[1].

Значущість фінансових показників на різних етапах життєвого циклу підприємства. Доцільно більш детально розглянути особливості аналізу фінансового становища підприємства на кожному етапі його життєвого циклу.

---

[1] Іванов В.Л. Управління економічною стійкістю промислових підприємств (на прикладі підприємств машинобудівного комплексу): Монографія. – Луганськ: Вид-во СНУ ім. В. Даля, 2005. – 265с.

Таблиця 4.1.

Значущість фінансових показників
на різних етапах життєвого циклу підприємства

Фінансові показники	Етапи життєвого циклу				
	Зародження	Прискорення	Сповільнення	Зрілість	Спад
Показники ліквідності					
Показники фінансової незалежності					
Показники прибутковості продажу					
Показники прибутковості капіталу					

Використовуються насамперед

Використовуються у другу чергу

Використовуються в третю чергу

Етап зародження. Формування стратегічного потенціалу починається на етапі зародження підприємства шляхом пошуку найбільш конкурентоспроможних напрямів існування на ринку. Велику увагу на даному етапі потрібно приділяти впливу зовнішніх чинників, які мають бути сприятливі для ведення бізнесу, а також прибутковості вибраної місії. У розрізі фінансового аналізу особлива увага має бути приділена показникам ліквідності і фінансовій незалежності.

Показники ліквідності характеризують поточну платоспроможність підприємства шляхом порівняння в певні періоди величини оборотного капіталу з сумою взятих платіжних зобов'язань, в тому числі з тими, які найближчим часом мають бути оплачені. Дуже високі показники

свідчать про неефективне використання вкладених коштів, низькі показники - про можливу небезпеку виявитися неплатоспроможним.

Предметом розгляду показників фінансової незалежності є сукупність пасивів, тобто власних джерел і зобов'язань. Мова йде про сферу, в яку проникають інтереси власності, критерії максимізації прибутку, а також вплив податків. Оптимізація структури пасивів належить до найбільш важливих аспектів фінансової незалежності.

Таким чином, на етапі зародження підприємства при аналізі його фінансового становища найбільша увага повинна бути приділена показникам перших двох груп: ліквідності і фінансової незалежності. При цьому коефіцієнти, що розглядаються, повинні мати стійку тенденцію зростання і до кінця етапу досягти нормативних значень.

Етап прискорення зростання. Етап прискорення зростання характеризується істотним зусиллям стратегічного потенціалу підприємства при зростанні попиту на його продукцію. Окремі елементи потенціалу підприємства складаються в систему, між ними виникають стійкі зв'язки, що дозволяють отримувати ефект цілісності і істотно посилюють конкурентоспроможність. Крім того, посилюється взаємодія підприємства з родинними і підтримуючими галузями та підвищується міра агресивності конкурентної стратегії підприємства.

На етапі прискорення зростання важливим є стабільність показників ліквідності і незалежності. Якщо вони не стабілізувалися на попередньому етапі, це означає, що підприємство не досягло необхідної міри конкурентоспроможності і стоїть на грані банкрутства. Потрібне втручання на рівні перегляду місії фірми, або, як мінімум, її маркетингової стратегії. Однак основний акцент в фінансовому аналізі на етапі прискорення повинен бути зроблений на показниках оборотності.

Розглядаючи показники оборотності, слід постійно спостерігати за їх динамікою, оскільки використати тут універсальні нормативи неможливо (через вплив тривалості виробничого циклу та інших чинників). Показники оборотності на етапі прискорення мають постійно рости.

До кінця етапу прискорення зростання повинне вже спостерігатися зростання показників рентабельності.

Етап сповільнення зростання. Цей етап зростання може початися з проникненням на ринок як великого числа виробників-конкурентів, так і конкуруючих технологій. Одним з критеріїв успішної діяльності є стабілізація показників рентабельності продажу. Осо-

бливу увагу потрібно приділяти коефіцієнтам рентабельності - всіх операцій по балансовому і чистому прибутку як інтегрованим показникам.

Прибутковість всіх операцій по балансовому прибутку показує, наскільки ефективно і прибутково підприємство веде свою діяльність. Показник потрібно порівнювати з торішньою величиною, з показниками конкурентів, із середніми показниками по галузі. Компанії, що реалізують недорогі товари у великому об'ємі за готівковий розрахунок, будуть мати відносно невисоке значення цього показника (10%). Необов'язково, щоб цей показник зростав. Підприємство, у якого прибутковість продажу нижча, ніж у конкурентів, може збільшити свою частку ринку за їх рахунок.

Етап зрілості. На цьому етапі, маючи стабільні показники рентабельності продажу, необхідно домагатися стабільних і високих показників рентабельності капіталу. Слід також відстежувати інвестиційну діяльність підприємства, що і дозволяє аналізувати показники рентабельності капіталу При цьому доцільно розглядати прибутковість сукупних активів, окремих частин, а також джерел формування.

На цьому етапі всі коефіцієнти повинні мати стабільні значення.

Якщо динаміка показників оборотності і рентабельності свідчить про стабільність або стійке зростання, то можна зробити висновок про нормальний розвиток підприємства. Якщо показники мають тенденцію до зниження або коливань, то слід вжити заходів по зміні стратегії підприємства, оскільки підприємство може виявитися на грані настання стадії спаду.

Етап спаду. Спад конкурентоспроможності наступає в основному через агресивну політику підприємств-суперників, а також за рахунок старіння ресурсі підприємства. На цьому етапі зовнішні чинники знову набувають великого значення: параметри попиту, зв'язку з родинними галузями, суперництво з конкуруючими підприємствами, вплив державних реформ і інш. На цьому етапі вони виявляються грубіше, різкіше, а імовірність настання банкрутства стає більш реальною. На етапі спаду відбувається дестабілізація всіх фінансових показників, тому потрібно відстежувати всі групи показників.

Але не всі з них можуть сигналізувати про дестабілізацію діяльності підприємства в рівній мірі. Найбільш істотними показниками є показники ліквідності і рентабельності. На основі аналізу показників рентабельності можна зробити висновок про можливість або немож-

ливість продовження діяльності підприємства у вибраному напрямі. Показники ліквідності можуть провіщати фінансову кризу або повне банкрутство підприємства.

У запропонованій системі фінансового аналізу показники проранжовані по значущості групи фінансових показників стосовно до етапів життєвого циклу підприємства, виявлені тенденції до їх зміни при нормальному розвитку підприємства на будь-якій стадії його функціонування. Її використання забезпечить більш точну фінансову оцінку підприємства.

Система фінансового аналізу заснована на доступній інформації, не є трудомісткою, що дозволяє застосовувати її для більш глибокої оцінки стану підприємства, яка потім може бути використана для розробки більш обґрунтованих заходів, направлених на забезпечення його стійкого функціонування. У табл. 4.2 представлене дерево показників стійкості.

Таблиця 4.2

Індикатори оцінки зовнішніх і внутрішніх показників діяльності промислових підприємств в забезпеченні економічної стійкості

Група показників	Показник
Зовнішні показники стійкості	
1. Прибуток	1.1 Прибуток
	1.2. Рентабельність
	1.3.Об'єм продажу
2. Конкурентоздатність підприємства	2.1. Інноваційний потенціал підприємства
	2.2. Ринкова активність
	2.3. Стратегічні капіталовкладення
3. Конкурентоздатність продукції	3.1. Якість продукції
	3.2. Ціна продукції
	3.3. Післяпродажне обслуговування
Внутрішні показники стійкості	
1. Фінансово-економічні	1. Коефіцієнт автономії
	2. Коефіцієнт співвідношення позикових і залучених коштів
	3. Коефіцієнт забезпеченості власними коштами

Продовження таблиці 4.2

Група показників	Показник
	4. Коефіцієнт маневреності
	5. Коефіцієнт фінансування
2. Виробничо-економічні	1. Здатність підприємства до освоєння
	2. Час підготовки і освоєння нового виробу
	3. Час виробництва і реалізації нового виробу
	4. Коефіцієнт оновлення
	3. Гнучкість і здібність до адаптації
3.Організаційно-економічні	1. Відповідність стратегічним пріоритетам розвитку підприємства
	2.Пристосованість для застосування сучаснихінформаційних технологій
	4. Забезпечення оперативності в реалізації управлінських рішень
	5. Пристосованість для застосування сучасних схем фінансового менеджменту
	6. Функціональна і структурна логічність
	7. Раціональна міра централізації (децентралізація)

На нижньому рівні трирівневої ієрархічної структури знаходиться мінімальний набір показників, що характеризує життєво важливі для будь-якого підприємства характеристики його функціонування.

Показники розбиті на чотири групи: зовнішні показники (1) – прибуток, конкурентоспроможність підприємства, конкурентоспроможність продукції; внутрішні показники, в свою чергу, розбиті на три групи – фінансово-економічні (2) виробничо-економічні (3) і організаційно-економічні (4). На середньому рівні - агреговані показники Y_i, що визначають стратегічні цілі підприємства.

Агрегування здійснюється за формулою $U_i = w_{ij} \cdot x_j$ де w_{ij} вагові коефіцієнти, отримані експертним шляхом за даними аналізу щомісячних даних; u_j - відповідні показники нижнього рівня.

На верхньому рівні знаходиться агрегований показник стійкості - I. Найбільшу складність в оцінці показників стійкості верхнього і

середнього рівня являє собою визначення вагових коефіцієнтів w_{ij} і w_i від яких залежить не тільки розрахункова величина стійкості, але і вибір подальших заходів щодо стабілізації діяльності підприємства.

На виборі коефіцієнтів значущості для кожного локального і групового показника потрібно зупинитися більш детально.

Процедура оцінки економічної стійкості включає наступні етапи:

1. Визначення експертним шляхом вагових коефіцієнтів значущості локальних показників стійкості.

2. Завдання допустимого ($u^{оп}$), критичного ($u^{кр}$) і катастрофічного ($u^{кт}$) рівнів стійкості на основі фази життєвого циклу підприємства, його тактичних і стратегічних цілей і задач.

3. Розрахунок окремих показників стійкості для випадку, коли сприятливе зростання показника (наприклад, прибуток):

$$u_i = 1 - \frac{a_i^{пл} - a_i}{a_i^{пл}},$$

для випадку, коли сприятливе зниження показника (наприклад, витрати):

$$u_i = 1 - \frac{a_i - a_i^{пл}}{a_i^{пл}}.$$

4. Розрахунок окремих показників стійкості з урахуванням вагового коефіцієнта:

$$U_{ij} = w_{ij} \cdot u_{ij}.$$

5. Розрахунок окремих показників стійкості

$$V_j = \sum_{i=1}^{m} w_{ij} u_{ij}.$$

6. Розрахунок інтегрального показника стійкості

$$I = \sum_{j=1}^{n} w_i V_j$$

7. Прийняття рішення про вибір керуючих впливів по стабілізації діяльності підприємства.

Оцінка рівня економічної стійкості була проведена для одного з підприємств «Укрзалізниці» (табл. 4.3).

Таблиця 4.3.

Показники рівня економічної стійкості одного з підприємств «Укрзалізниці»

Показник	Фактичне значення	Очікуване значення	Розрахунок окремого показника стійкості	Вага	Розрахунок групового показника стійкості
Товарна продукція (в порівняних цінах), тис. грн.	35540	50000	0,711	0,12	0,085
Виручка від реалізації (без ПДВ), тис. грн.	30955	45000	0,688	0,14	0,096
Освоєння капіталовкладень, тис. грн.	1310	1310	1,000	0,05	0,050
Використання виробничої потужності, %	10	25	0,392	0,12	0,047
Собівартість товарної продукції, тис. грн.	33024	33024	1,000	0,07	0,070
Рентабельніс. товарної продукції, тис. грн.	13	13	0,969	0,08	0,078
Витрати на виробництво, тис. грн.	31560	31560	1,000	0,06	0,060
Балансовий прибуток (+), збитки (-), тис. грн.	-3602	2600	-1,385	0,18	-0,249
Результат від реалізації (+), збитки (-), тис. грн.	619	700	0,884	0,18	0,159
	0,396				

Після проведеної експертизи були отримані наступні оцінки значущості (вагові коефіцієнти) локальних і групових показників стійкості (4.3). Допустимий рівень стійкості $u^{\partial n} = 0,9$, критичний $u^{кр} = 0,7$ і катастрофічний $u^{кт} = 0,5$.У табл. 4.4-4.6 представлені розрахунки зовнішніх показників стійкості, показників фінансово-, виробничо- і організаційно-економічної стійкості відповідно.

Таблиця 4.4.

Розрахунок показників фінансово-економічної стійкості

Показник	Фактичне значення	Очікуване значення	Розрахунок окремого показника стійкості	Вага	Розрахунок групового показника стійкості
Коефіцієнт концентрації власного капіталу	0,69	>0,5	1,380	0,10	0,138
Коефіцієнт фінансової залежності	1,45	<2,0	1,275	0,10	0,128
Коефіцієнт маневреності власного капіталу	0,08	>0,5	0,160	0,10	0,016
Коефіцієнт концентрації залученого капіталу	0,30	<0,4	1,250	0,10	0,125
Коефіцієнт структури довгострокових вкладень	0,10	<0,3	1,667	0,10	0,167
Коефіцієнт довгострокового залучення позикових коштів	0,09	<0,2	1,550	0,10	0,155
Коефіцієнт співвідношення залученого і власного капіталу	0,44	<0,4	0,900	0,10	0,090

Продовження таблиці 4.4

Показник	Фактичне значення	Очікуване значення	Розрахунок окремого показника стійкості	Вага	Розрахунок групового показника стійкості
Коефіцієнт абсолютної ліквідності	0,01	<0,2	0,050	0,10	0,005
Коефіцієнт швидкої ліквідності	0,56	<0,8	0,700	0,10	0,070
Коефіцієнт покриття	1,25	<2,0	0,625	0,10	0,063
					0,956
Рівень зношеності обладнання	0,5	0,8	0,625	0,20	0,125
Організаційно-технічний рівень виробництва	0,6	0,8	0,750	0,10	0,075
Наявність надмірних потужностей	0,8	0,9	0,889	0,25	0,222
Рівень автоматизації техпроцеса	0,8	0,8	1,000	0,05	0,050
Забезпеченість матеріально-сировинними і паливно-енергетичними ресурсами	0,5	0,9	0,556	0,05	0,028
Наявність матеріальних резервів	0,7	00,9	0,778	00,10	0,078
Кваліфікація персоналу	0,7	00,8	0,875	00,25	0,219
					0,797

Аналіз початкових даних, а також групових і інтегрального показників стійкості показав, що найбільш нестійкою є фінансово-економічна сфера діяльності: в цьому випадку груповий показник

фінансово-економічної стійкості 0,956 перевищив критичний поріг стійкості. Результати фінансово-економічної діяльності, в свою чергу, позначилися на загальних показниках діяльності підприємства, знизивши рівень залежності від зовнішніх чинників до рівня нижче критичного показника зовнішньої стійкості становив 0,396. Інтегральний показник стійкості становив 0,73, що свідчить про недостатній рівень економічної стійкості підприємства - перевищене значення критичного рівня в 0,7.

Таблиця 4.5

Розрахунок показників організаційно-економічної стійкості

Показник	Фактичне значення	Очікуване значення	Розрахунок окремого показника стійкості	Вага	Розрахунок групового показника стійкості
Вище керівництво	8	10	0,800	0,20	0,160
Фінанси	6	8	0,750	0,15	0,113
Розробки (НІОКР)	6	6	1,000	0,15	0,150
Маркетинг	8	8	1,000	0,20	0,200
Матеріально-технічне постачання	7	8	0,875	0,10	0,088
Кадри	5	8	0,625	0,20	0,125
					0,835

Таблиця 4.6

Розрахунок інтегрального показника стійкості

Показник	Вага	Значення	Розрахунок
Зовнішні	0,3	0,396	0,119
Фінансово-економічна стійкість	0,3	0,956	0,287
Виробничо-економічна стійкість	0,25	0,797	0,199
Організаційно-економічна стійкість	0,15	0,835	0,125
Інтегральний показник стійкості			0,730

4.4. Прогнозування та оцінка рівня економічної безпеки підприємства

Рівень економічної безпеки підприємства залежить від великої кількості показників різних сфер діяльності. Оцінка рівня економічної безпеки підприємства пропонується здійснювати за наведеним у другому розділі методом.

Для прогнозування рівня економічної безпеки однієї з залізниць України (далі залізниця) використаємо статистичні дані з економічної діяльності підприємства.

У табл. 4.7 приведено значення показників стійкості підприємства.

Таблиця 4.7

Значення показників стійкості підприємства залізниці

Показник	2002		2003		2004		2005	
	1 півр.	2 півр.	1 півр.	2 півр.	1 півр.	2 півр.	1 півр.	2 півр.
Зовнішня стійкість	0,268	0,266	0,266	0,274	0,278	0,276	0,283	0,279
Фінансова економічна стійкість	0,528	0,537	0,541	0,555	0,560	0,568	0,581	0,600
Виробничо-економічна стійкість	0.453	0,462	0,464	0,479	0.486	0.494	0,507	0,508
Організаційно-економічна стійкість	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Зовнішня стійкість	0,290	0,297	0,295	0,300	0,295	0,300	0,293	0,287
Фінансова економічна стійкість	0,610	0,633	0,653	0,678	0,697	0,709	0,717	0,734

Продовження таблиці 4.7

Показник	2006		2007		2008		2009	
	1 півр.	2 півр.	1 півр.	2 півр.	1 півр.	2 півр.	1 півр.	2 півр.
Виробничо-економічна стійкість	0,513	0,517	0,516	0,529	0,529	0,537	0,543	0,544
Організаційно-економічна стійкість	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Зовнішня стійкість	0,292	0,294	0,301	0,309	0,319	0,313	0,320	0,315
Фінансова економічна стійкість	0,754	0,761	0,783	0,774	0,778	0,791	0,802	0,798
Виробничо-економічна стійкість	0,553	0,558	0,563	0,571	0,583	0,579	0,585	0,581
Організаційно-економічна стійкість	0,000	000	0,000	0,000	0,000	0,000	0,000	0,000

Окремо один від одного показники дозволяють оцінити стійкість кожного «підрозділу» але для оцінки стійкості підприємства в цілому необхідно сформувати інтегральний показник стійкості, який дозволить провести оцінку рівня економічної стійкості підприємства.

Для обчислення інтегрального показника стійкості використовуються окремі показники стійкості (табл.. 4.7) помножені на вагові показників (табл.. 4.8).

Вагові коефіцієнти отримані методом експертних оцінок[1].

Таблиця 4.8.

Ваги показників стійкості

Показник	Вага
Зовнішня стійкість	0,3
Фінансово-економічна стійкість	0,3
Виробничо-економічна стійкість	0,25
Організаційно-економічна стійкість	0,15

Таким чином отримуємо інтегральний показник стійкості залізниці за 2002-2005 роки (табл. 4.9).

Таблиця 4.9.

Розрахунок інтегрального показника стійкості

Показник	2002		2003		2004		2005	
	1 півр.	2 півр.	1 півр.	2 півр.	1 півр.	2 півр.	1півр.	2 півр.
Інтегральний показник стійкості	0,569	0,580	0,582	0,601	0,611	0,621	0,637	0,637
Інтегральний показник стійкості	00,644	00,649	00,648	00,664	00,664	00,675	00,682	00,683
Інтегральний показник стійкості	00,694	00,701	00,707	00,717	00,732	00,727	00,734	00,730

Вхідними даними для прогнозування є значення окремих показників за 24 періоди (2002-2005 роки). Значення показників у восьмому періоді буде використано для перевірки адекватності прогнозу.

Для прогнозування пропонується використати продукт STATISTICA 6.1.Прогнозування показника зовнішньої стійкості.

[1] Іванов В.Л. Управління економічною стійкістю промислових підприємств (на прикладі підприємств машинобудівного комплексу): Монографія. – Луганськ: Вид-во СНУ ім. В. Даля, 2005. – 265 с.

Початкові дані прогнозу показані на рис. 4.1, 4.2.

	1 Спостереження	2 Зовнішня стійкість
1	1	0,322078699
2	2	0,326038683
3	3	0,329338669
4	4	0,337258637
5	5	0,342538616
6	6	0,350458584
7	7	0,363658531
8	8	0,357718555
9	9	0,350458584
10	10	0,355738563
11	11	0,352438576
12	12	0,363658531
13	13	0,35639856
14	14	0,364318528
15	15	0,381478459
16	16	0,389398427
17	17	0,383458451
18	18	0,388078432
19	19	0,397318395
20	20	0,397978392
21	21	0,401938376
22	22	0,392038416
23	23	0,400618381

Рис. 4.1. Вхідні дані прогнозу показника зовнішньої стійкості

Гістограма (рис. 4.3) ілюструє той факт, що розподілення ряду не є нормальним і в подальшому має сенс спробувати встановити залежність для цього ряду.

Аналіз даних

Знаходження залежності в представлених даних є завданням розбиття вихідного ряду на 2 складові: детерміновану функцію і чисто

випадкову складову. Випадкова складова повинна являти собою гаусовський ряд з незалежними приростами.

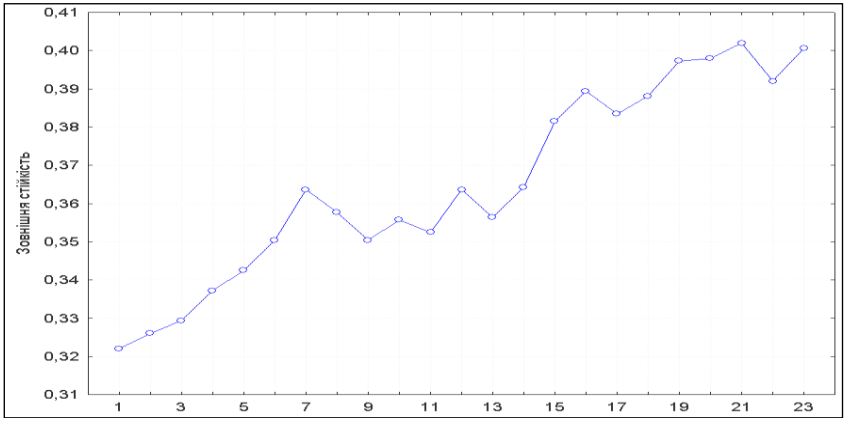


Рис. 4.2. Графік залежності показника зовнішньої стійкості від року

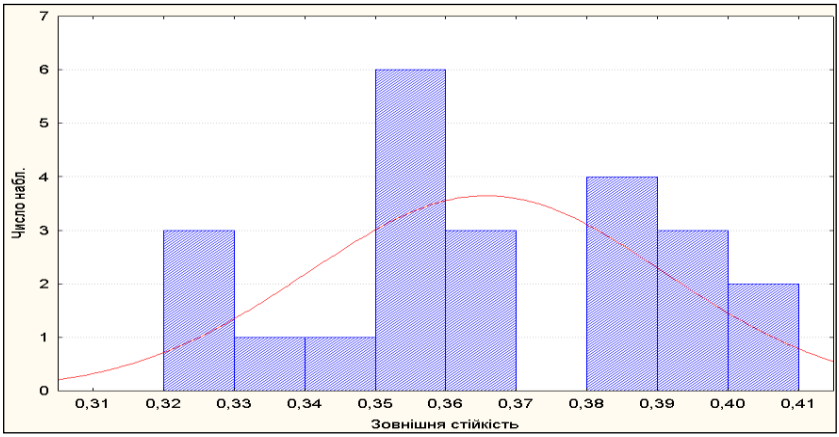


Рис. 4.3. Гістограма ряду даних

Для встановлення характеру невипадкової складової, побудуємо автокореляційну функцію вихідних даних (стандартні помилки – оцінки білого шуму) (рис. 4.4).

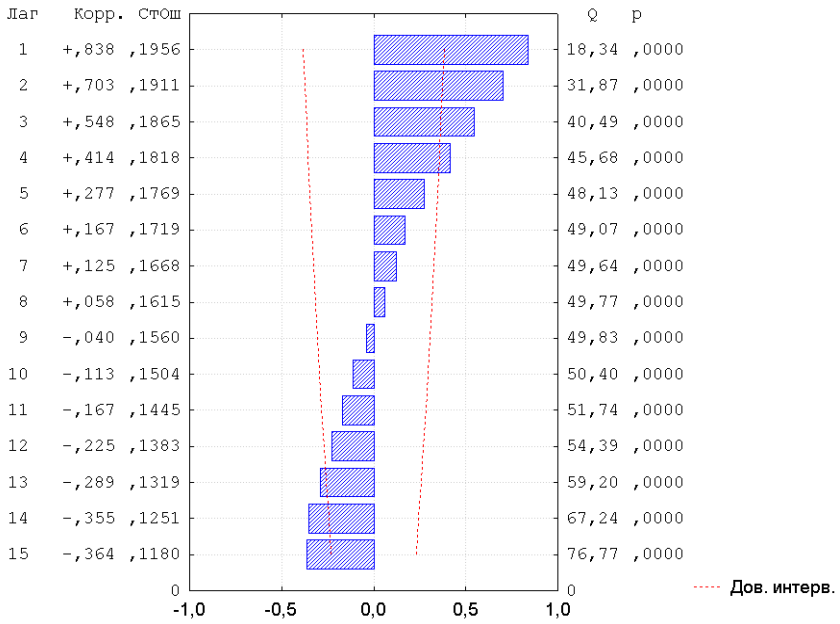


Рис. 4.4. Автокореляційна функція зовнішньої стійкості

По виду автокореляційної функції можна припустити, що ряд описується моделлю авторегресії 2-го порядку. На графіку автокореляції досягають піків на лагах 1.

Прогнозування здійснювалось програмою STATISTICA 6.1[1]. Найбільш точною була модель ARIMA(2;0;1)[23456].

---

[1]Боровиков В.П., Ивченко Г.И. Прогнозирование в системе STATISTICA в среде Windows. Основы теории и интенсивная практика на компьютере: Учеб. пособие. – М.: Финансы и статистика, 2000. – 384 с

[2]Єріна А. М. Статистичне моделювання та прогнозування, Навчальний посібник. – К.: КНЕУ, 2001. – 170с.

[3]Ханк Дж., Райтс А. Бизнес-прогнозирование, 7-е издание: Пер. с английского. – М.:"Вильямс", 2003. – 656с.

[4]Басовский Л. Е. Прогнозирование и планирование в условиях рынка, Учебное пособие. - М.: ИНФРА-М, 2001. – 260с.

[5]Бокс Дж., Дженкинс Г. Анализ временных рядов. Прогноз и управление. – М.: Мир, 1994.

[6]Кендэлл М. Временные ряды. – М.: Финансы и статистика, 1981.

Рис. 4.5. Гістограма прогнозної моделі ARIMA(2;0;1)

Як видно з рис. 4.5 гістограма розподілення результатів прогнозу близька до розподілення Гауса, що показує значимість моделі. Ймовірностне розподілення значень прогнозної моделі близько до лінії тренду (рис. 4.6).

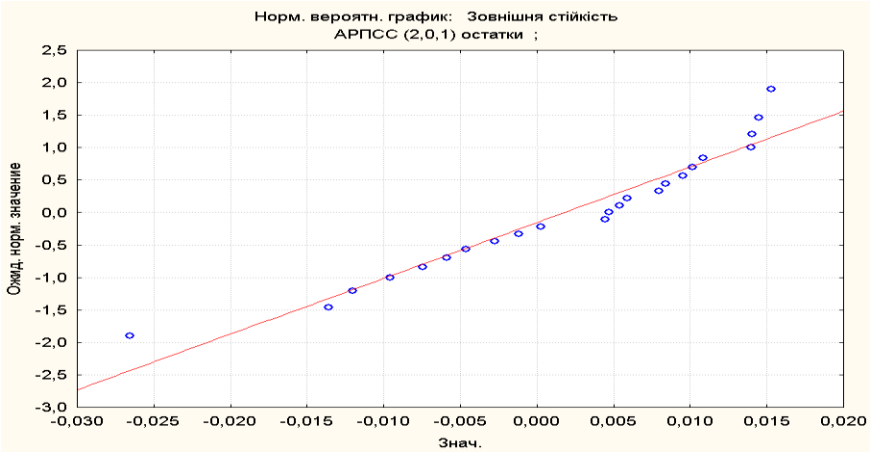


Рис. 4.6. Графік ймовірності розподілення прогнозної моделі

Як можна побачити з рис. 4.7 перевірка прогнозної моделі на адекватність підстановкою контрольного значення (24 період, помічений крапкою на рис. 4.7) підтверджує значність прогнозної моделі.

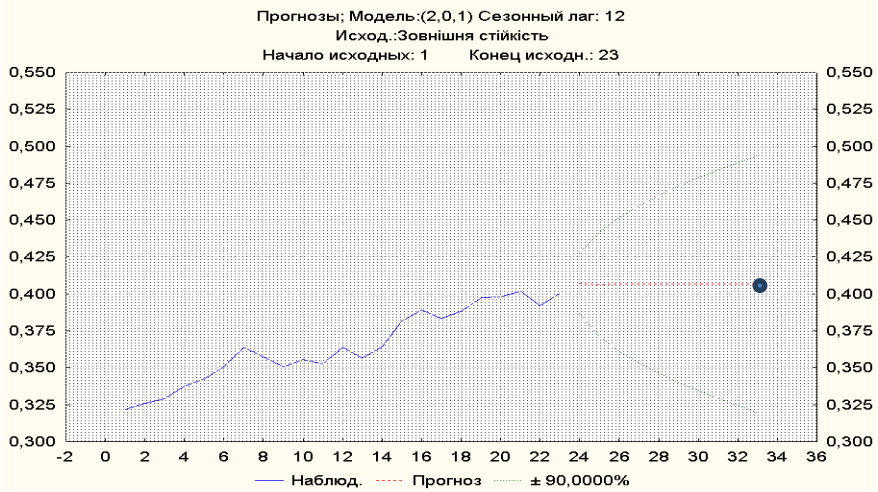


Рис. 4.7. Графік прогнозної моделі с прогнозним інтервалом на 10 періодів

Результати підбору прогнозної моделі у програмі STATISTICA 6.1 приведено на рис 4.8.

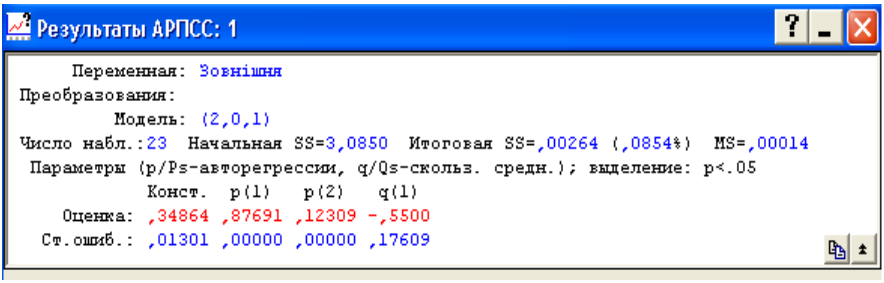


Рис. 4.8. Результат роботи моделі ARIMA(2,0,1)

При цьому автокореляційна та частна автокореляційна функції прогнозного ряду лежать у зоні довіри (рис. 4.9, 4.10), а тому модель адекватна.

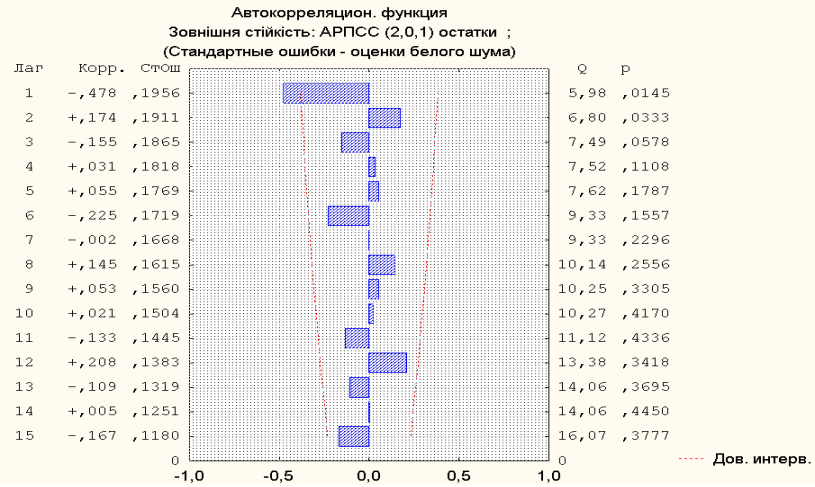


Рис. 4.9. Автокореляційна функція прогнозованих значень моделі

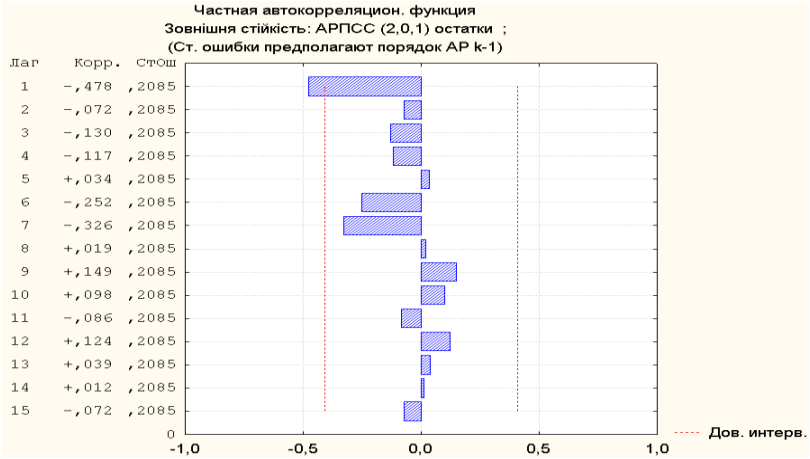


Рис. 4.10. Частна автокореляційна функція прогнозних значень моделі

Аналогічним чином була обрана прогнозна модель для показника фінансово-економічної стійкості підприємства (рис. 4.9-4.18). Модель ARIMA(1,0,1). Контрольне значення збігається з прогнозним (24 спостереження рис.4.18), що ще раз підтверджує адекватність отриманої прогнозної моделі.

	1 Спостереження	2 Фінансово-економічна стійкість
1	1	0,734273117
2	2	0,766128783
3	3	0,767721567
4	4	0,799577233
5	5	0,815505067
6	6	0,8409896
7	7	0,860103
8	8	0,866474133
9	9	0,86488135
10	10	0,8505463
11	11	0,842582383
12	12	0,861695783
13	13	0,872845267
14	14	0,882401967
15	15	0,8983298
16	16	0,899922583
17	17	0,920628767
18	18	0,930185467
19	19	0,915850417
20	20	0,934963817
21	21	0,96044835
22	22	0,958855567
23	23	0,954077217

Рис. 4.11. Вхідні дані прогнозу показника фінансово-економічної стійкості підприємства

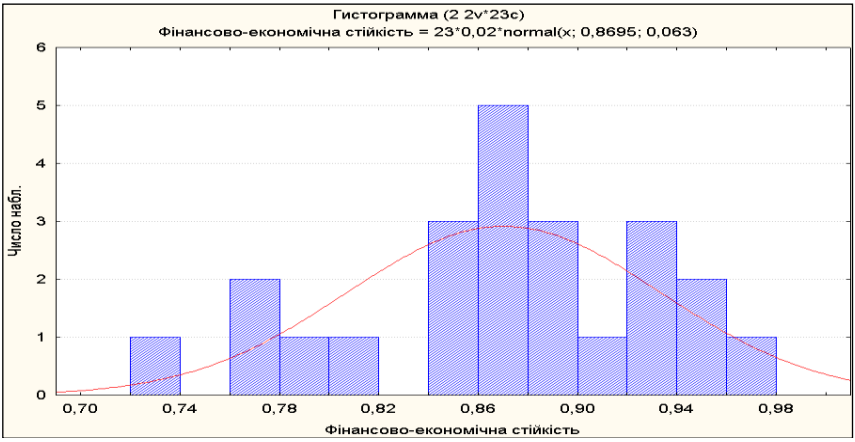


Рис. 4.12. Гістограма ряду даних

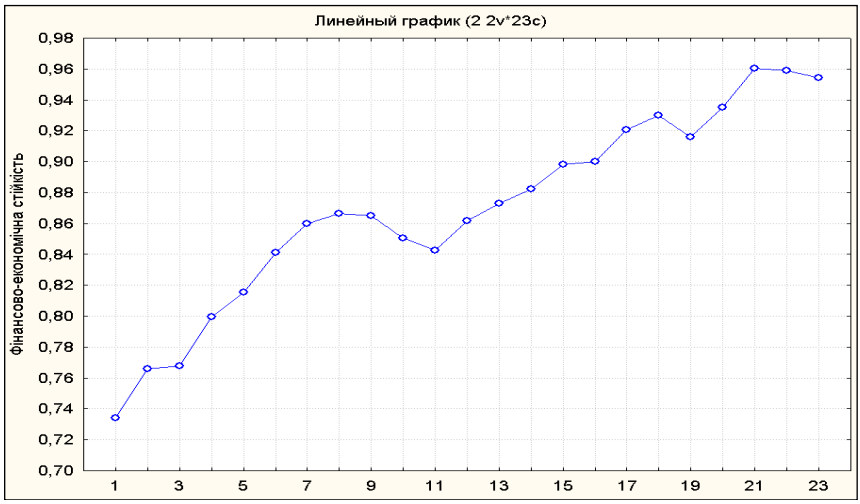


Рис. 4.13. Графік залежності показника фінансово-економічної стійкості від періоду

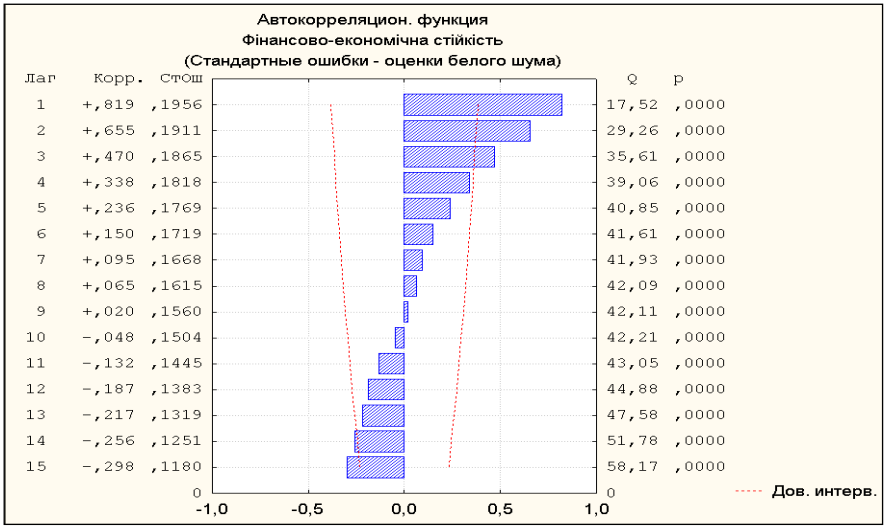


Рис. 4.14. Автокореляційна функція показника фінансово-економічної стійкості

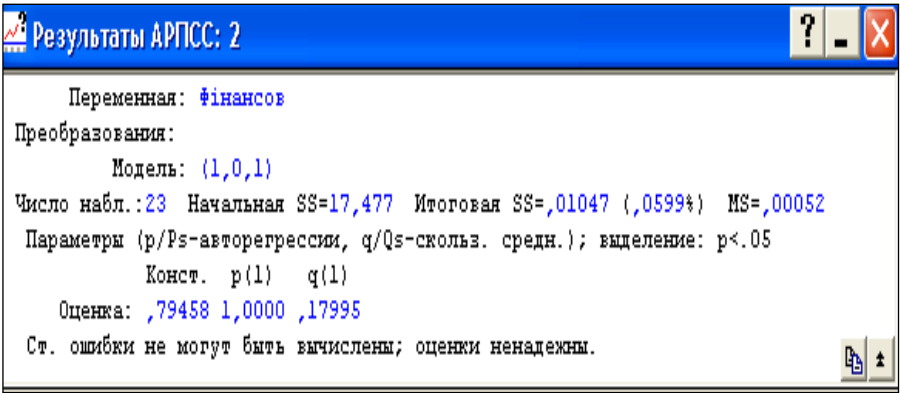


Рис. 4.15. Результат роботи моделі ARIMA(1,0,1)

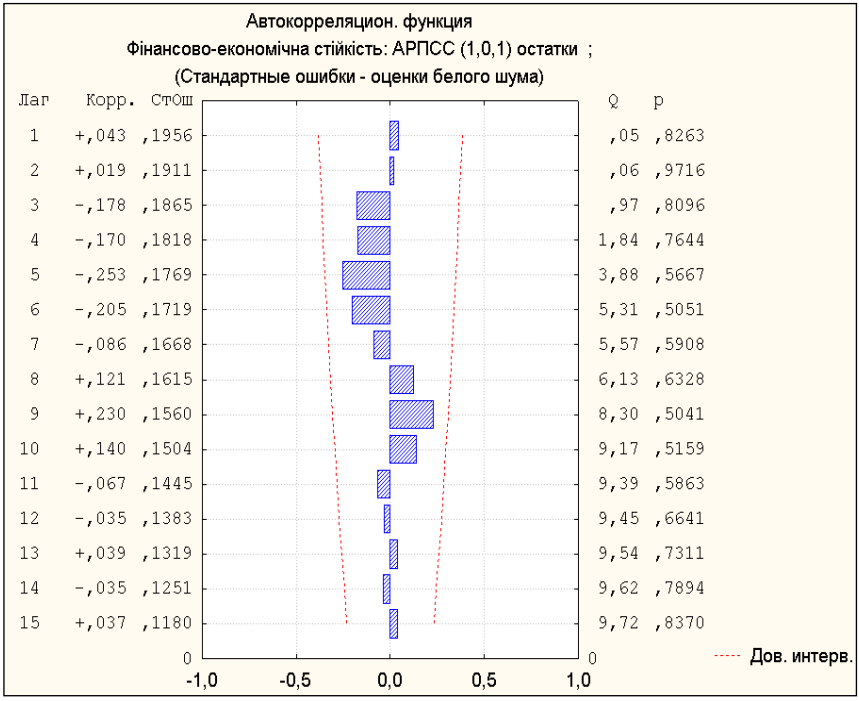


Рис. 4.16. Автокореляційна функція прогнозованих значень моделі

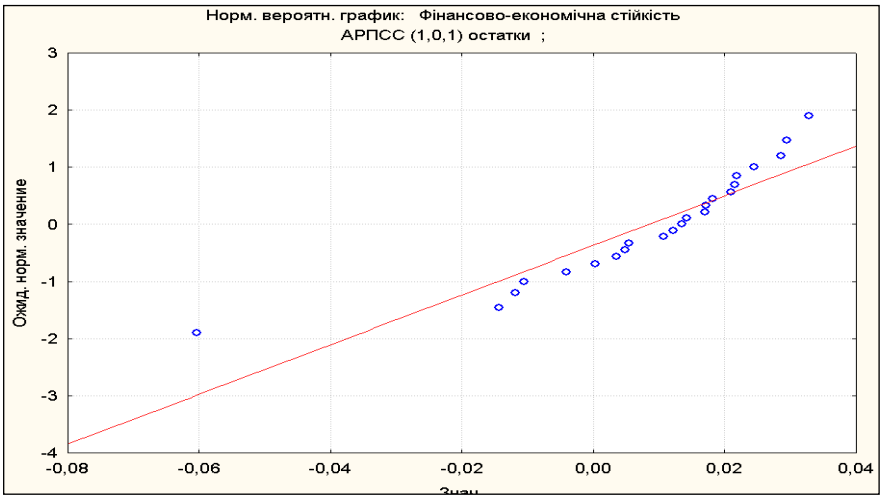


Рис. 4.17. Графік ймовірності розподілення прогнозної моделі

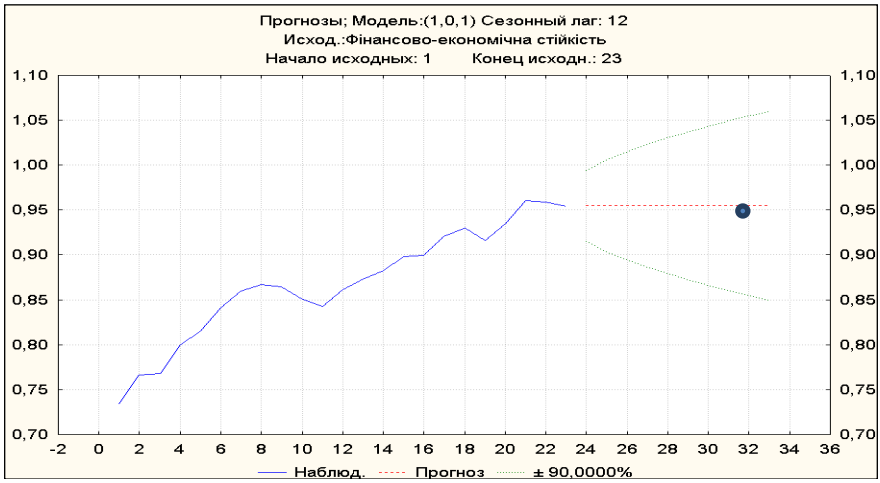


Рис. 4.18. Графік прогнозної моделі с прогнозним інтервалом на 10 періодів

Далі обрана прогнозна модель для показника виробничо-економічної стійкості підприємства (рис. 4.19-4.26). Модель ARIMA(1,0,1). Контрольне значення збігається з прогнозним (24 спосте-

реження рис.4.26), що ще раз підтверджує адекватність отриманої прогнозної моделі.

	1 Спостереження	2 Виробничо-економічна стійкість
1	1	0,675727192
2	2	0,671744517
3	3	0,671744517
4	4	0,69298545
5	5	0,7009508
6	6	0,6969681 25
7	7	0,714226383
8	8	0,703605917
9	9	0,7328122
10	10	0,750070458
11	11	0,746087783
12	12	0,758035808
13	13	0,744760225
14	14	0,758035808
15	15	0,74077755
16	16	0,72484685
17	17	0,738122433
18	18	0,743432667
19	19	0,760690925
20	20	0,7806043
21	21	0,80450035
22	22	0,789897208
23	23	0,808483025

Рис. 4.19. Вхідні дані прогнозу показника виробничо-економічної стійкості підприємства

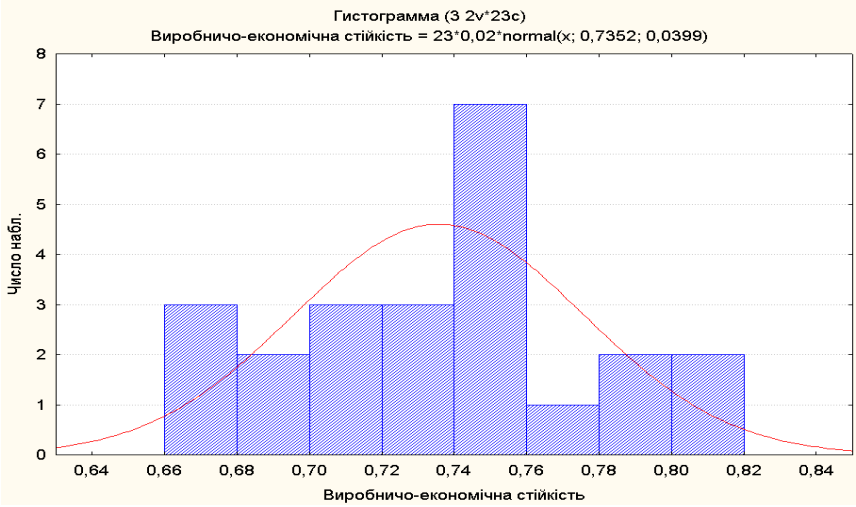


Рис. 4.20. Гістограма ряду даних

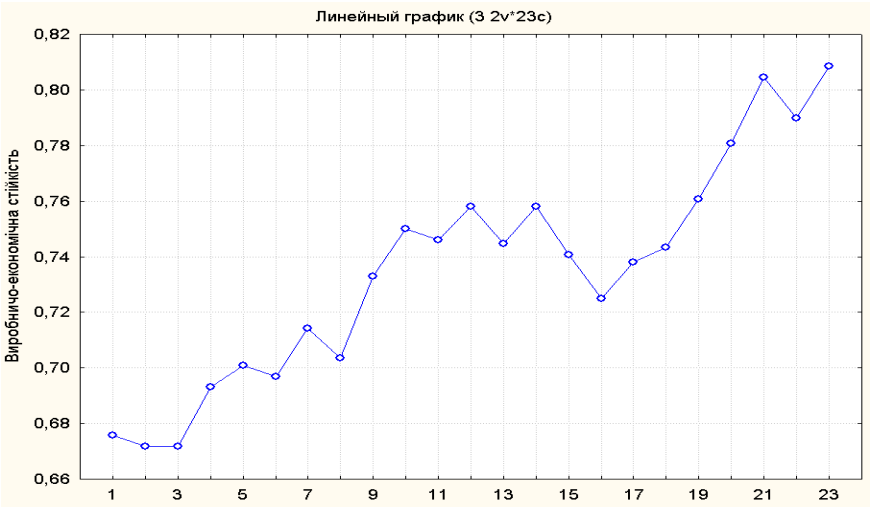


Рис. 4.21. Графік залежності показника виробничо-економічної стійкості від часу

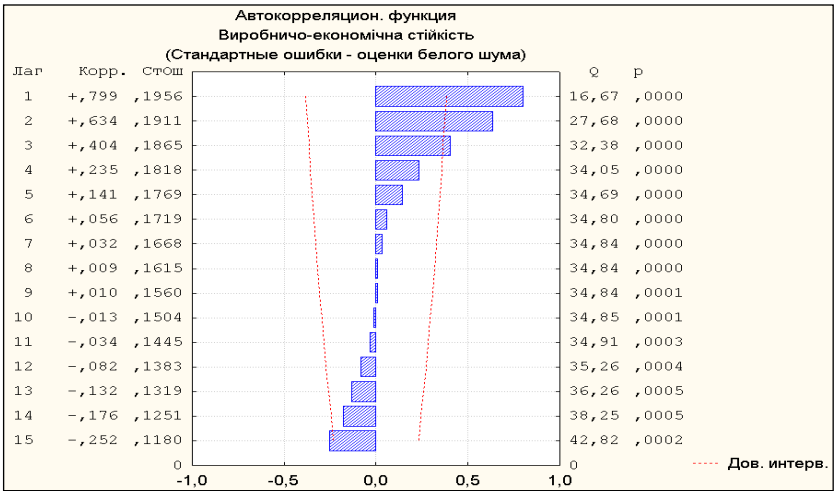


Рис. 4.22. Автокореляційна функція виробничо-економічної стійкості

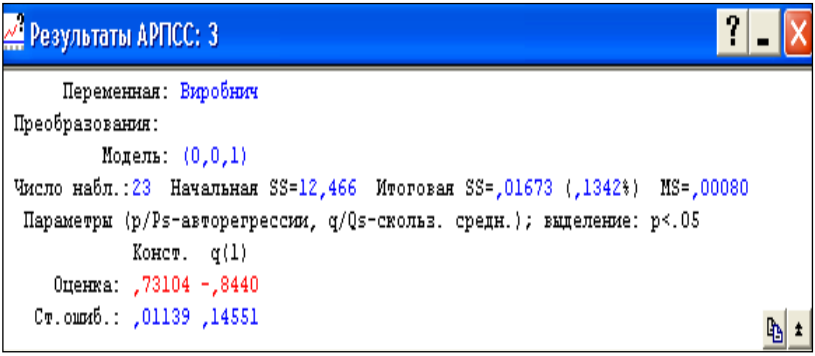


Рис. 4.23. Результат роботи моделі ARIMA(0,0,1)

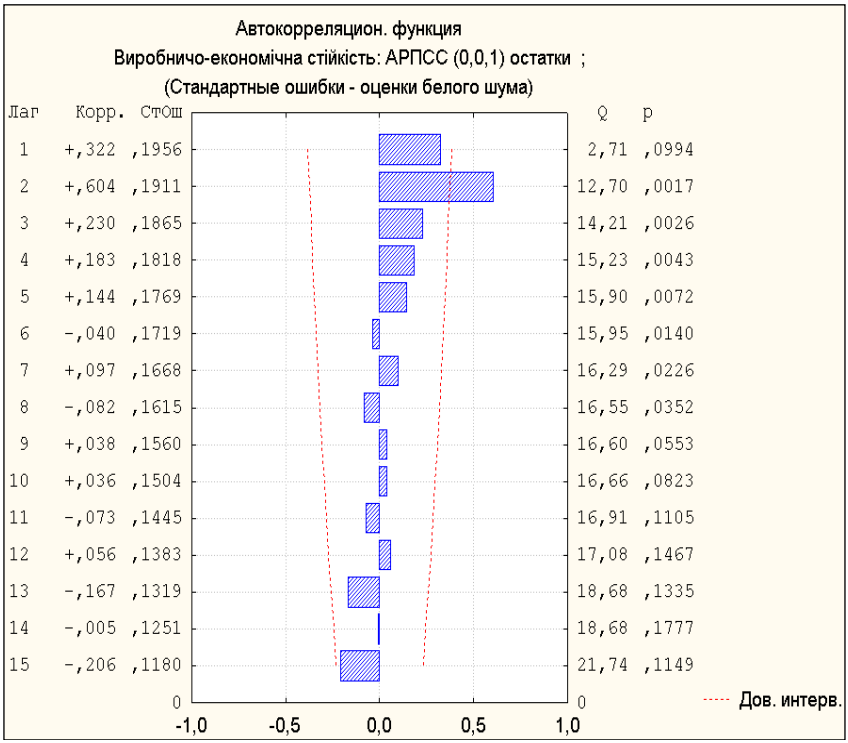


Рис. 4.24. Автокореляційна функція прогнозованих значень моделі

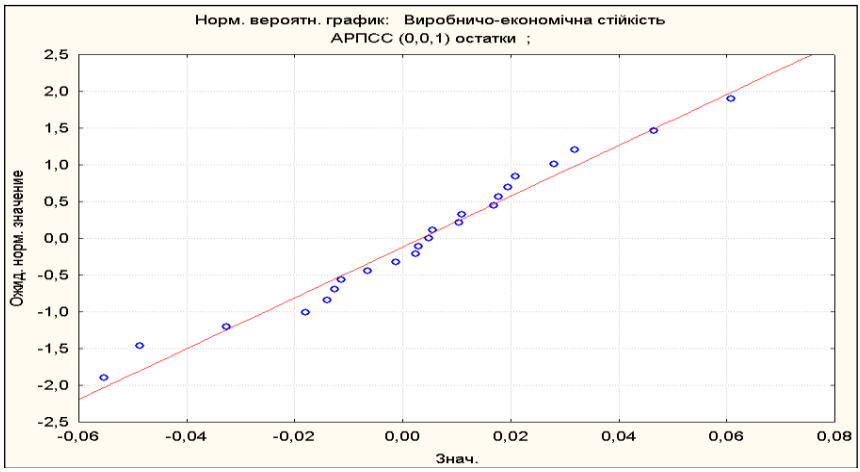


Рис. 4.25. Графік ймовірності розподілення прогнозної моделі

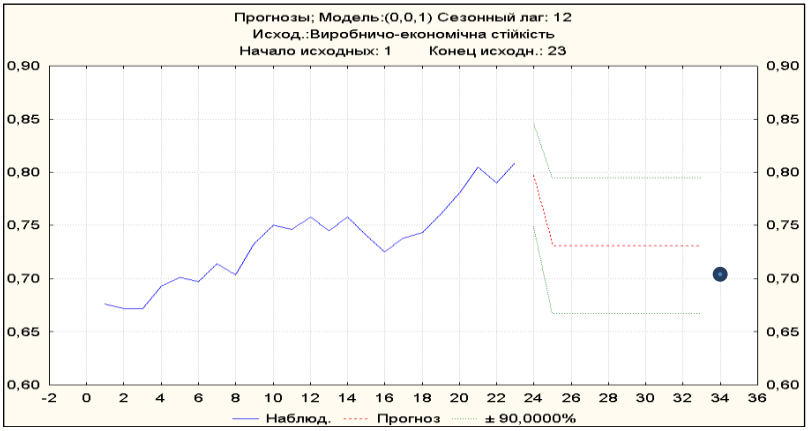


Рис. 4.26. Графік прогнозної моделі с прогнозним інтервалом на 10 періодів

Наступною була обрана прогнозна модель для показника організаційно-економічної стійкості підприємства (рис. 4.27 - 4.33). Модель ARIMA(4,0,0). Контрольне значення збігається з прогнозним (24 спостереження рис.4.33), що ще раз підтверджує адекватність отриманої прогнозної моделі, хоча й менш адекватна ніж попередні.

	1 стереже	2 Організаційно-економічна стійкість
1	1	0,552491667
2	2	0,562233333
3	3	0,566408333
4	4	0,580325
5	5	0,585891667
6	6	0,594241667
7	7	0,608158333
8	8	0,627641667
9	9	0,638775
10	10	0,662433333
11	11	0,683308333
12	12	0,70975
13	13	0,729233333
14	14	0,741758333
15	15	0,750108333
16	16	0,7682
17	17	0,789075
18	18	0,796033333
19	19	0,819691667
20	20	0,80995
21	21	0,814125
22	22	0,828041667
23	23	0,839175

Рис. 4.27. Вхідні дані прогнозу показника організаційно-економічної стійкості підприємства

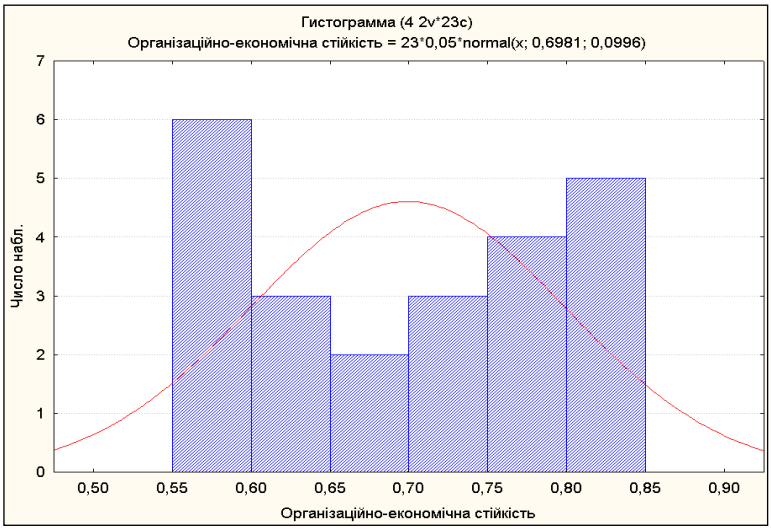


Рис. 4.28. Гістограма ряду даних

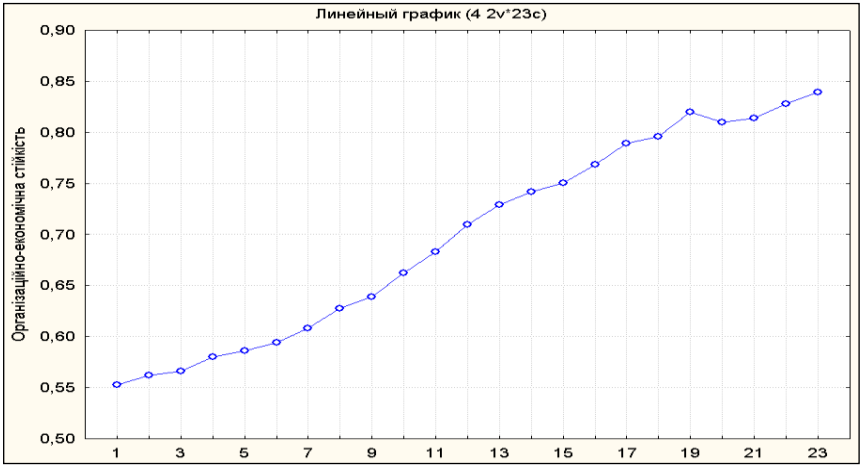


Рис. 4.29. Графік залежності показника організаційно-економічної стійкості від року

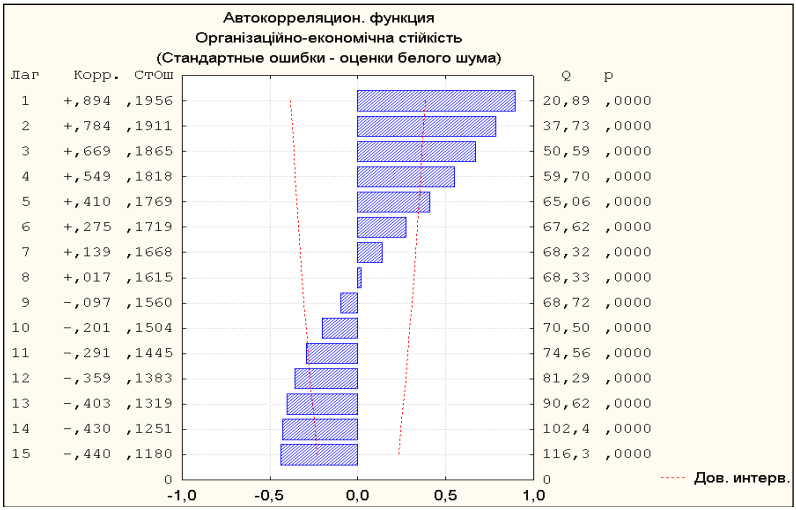


Рис. 4.30. Автокореляційна функція організаційно-економічної стійкості підприємства

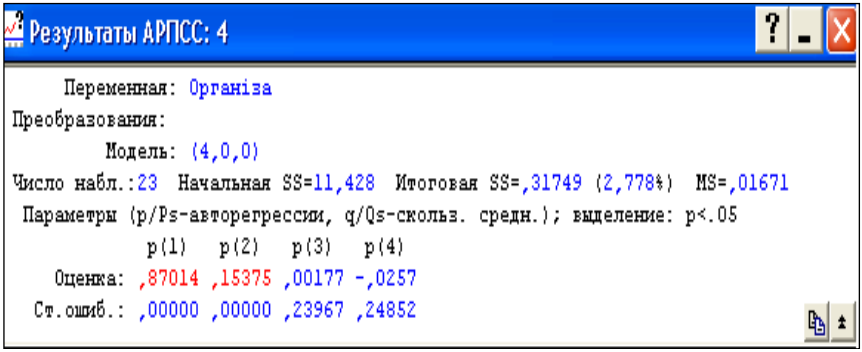


Рис. 4.31. Результат роботи моделі ARIMA(4,0,0)

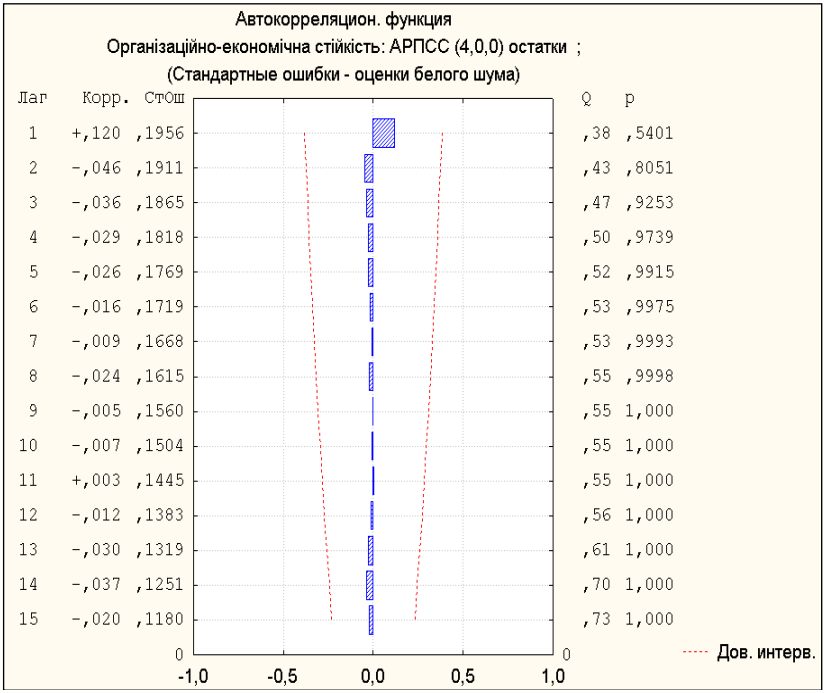


Рис. 4.32. Автокореляційна функція прогнозованих значень моделі

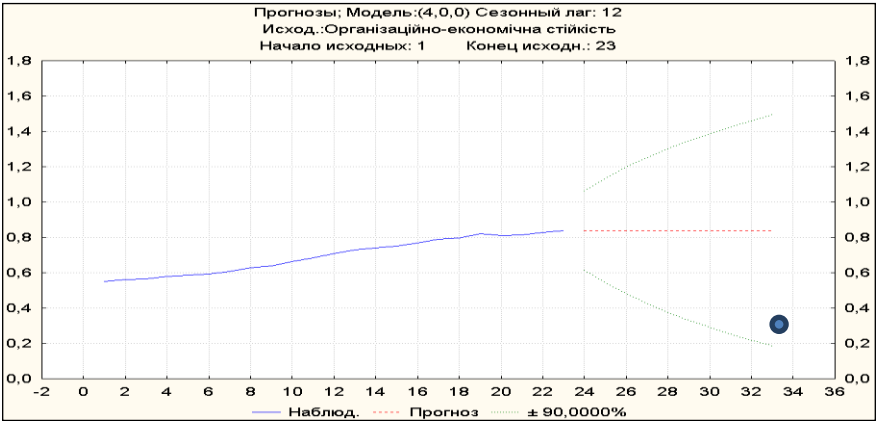


Рис. 4.33. Графік прогнозної моделі
с прогнозним інтервалом на 10 періодів

На підставі проведених вище робіт з прогнозування показників окремих розділів економічної стійкості підприємства можна зробити висновок про те, що на підставі отриманих прогнозних моделей можна з досить високою точністю здійснювати прогноз інтегрального показника стійкості залізниці. Це можливо через те, що інтегральний показник розраховується безпосередньо за допомогою чотирьох окремих показників.

Прогнозні значення окремого показника зовнішньої стійкості приведені в табл. 4.10.

Таблиця 4.10

Прогнозні значення показника зовнішньої стійкості

Період		Прогноз	Нижчий, 90%	Верхній, 90%	Ст. похибка
2013	2 півр.	0,40724	0,387	0,428	0,012
2014	1 півр.	0,40643	0,371	0,442	0,021
	2 півр.	0,40653	0,361	0,452	0,026
2015	1 півр.	0,40651	0,353	0,460	0,031
	2 півр.	0,40651	0,346	0,467	0,035
2016	1 півр.	0,40651	0,340	0,473	0,038

Продовження таблиці 4.10

	2 півр.	0,40651	0,334	0,479	0,042
2017	1 півр.	0,40651	0,329	0,484	0,045
	2 півр.	0,40651	0,324	0,489	0,048
2018	1 півр.	0,40651	0,319	0,494	0,050

Значення показника у другому півріччі 2013 року відоме і дорівнює 0,39599, що у свою чергу підтверджує адекватність прогнозної моделі.

Прогнозні значення окремого показника фінансово-економічної стійкості приведені в табл. 4.11 Значення показника у другому півріччі 2013 року відоме і дорівнює 0,955, що у свою чергу підтверджує адекватність прогнозної моделі.

Таблиця 4.11

Прогнозні значення показника фінансово-економічної стійкості

Період		Прогноз	Нижчий, 90%	Верхній, 90%	Ст. похибка
2013	2 півр.	0,955	0,915	0,994	0,023
2014	1 півр.	0,955	0,904	1,006	0,030
	2 півр.	0,955	0,894	1,015	0,035
2015	1 півр.	0,955	0,886	1,023	0,040
	2 півр.	0,955	0,879	1,031	0,044
2016	1 півр.	0,955	0,872	1,037	0,048
	2 півр.	0,955	0,866	1,043	0,051
2017	1 півр.	0,955	0,861	1,049	0,055
	2 півр.	0,955	0,855	1,055	0,058
2018	1 півр.	0,955	0,850	1,060	0,061

Прогнозні значення окремого показника виробничо-економічної стійкості приведені в табл. 4.12. Значення показника у другому півріччі 2013 року відоме і дорівнює 0,796, що у свою чергу підтверджує адекватність прогнозної моделі.

Таблиця 4.12

Прогнозні значення показника виробничо-економічної стійкості

Період		Прогноз	Нижчий, 90%	Верхній, 90%	Ст. похибка
2013	2 півр.	0,797	0,749	0,846	0,028
2014	1 півр.	0,731	0,667	0,795	0,037
	2 півр.	0,731	0,667	0,795	0,037
2015	1 півр.	0,731	0,667	0,795	0,037
	2 півр.	0,731	0,667	0,795	0,037
2016	1 півр.	0,731	0,667	0,795	0,037
	2 півр.	0,731	0,667	0,795	0,037
2017	1 півр.	0,731	0,667	0,795	0,037
	2 півр.	0,731	0,667	0,795	0,037
2018	1 півр.	0,731	0,667	0,795	0,037

Прогнозні значення окремого показника організаційно-економічної стійкості приведені в табл. 4.13.

Таблиця 4.13

Прогнозні значення показника організаційно-економічної стійкості

Період		Прогноз	Нижчий, 90%	Верхній, 90%	Ст. похибка
2013	2 півр.	0,83816	0,615	1,062	0,129
2014	1 півр.	0,83890	0,543	1,135	0,171
	2 півр.	0,83906	0,480	1,199	0,208
2015	1 півр.	0,83902	0,424	1,254	0,240
	2 півр.	0,83904	0,375	1,303	0,268
2016	1 півр.	0,83903	0,331	1,347	0,294
	2 півр.	0,83902	0,291	1,387	0,317
2017	1 півр.	0,83901	0,253	1,425	0,339

Продовження таблиці 4. 14

Період		Прогноз	Нижчий, 90%	Верхній, 90%	Ст. похибка
	2 півр.	0,83900	0,218	1,460	0,359
2018	1 півр.	0,83899	0,184	1,494	0,379

Значення показника у другому півріччі 2013 року відоме і дорівнює 0,835, що у свою чергу підтверджує адекватність прогнозної моделі. На підставі графічного аналізу рис. 4.7, 4.18, 4.26, 4.3 можна зробити висновок про те, що інтегральний показник стійкості підприємства має виражену тенденцію зниження через те, що рівень виробничо-економічної стійкості у прогнозному періоді значно зменшується, а інші показники залишаються приблизно на тому ж самому рівні що й у теперішній час. При цьому вага показника виробничо-економічної стійкості досить високий (0,25).

З використання прогнозних моделей та вагових коефіцієнтів (табл. 4.2) обчислюємо прогнозний ряд інтегрального показника економічної стійкості підприємства на 2 півріччя 2013 – 1 півріччя 2018 роки (табл. 4.14). Та на основі таблиці побудуємо графік прогнозу (рис. 4.34). Так як у другому кварталі 2013 року значення інтегрального показника було 0,73 (норма 0,7)[1] робимо висновок, що тенденція незначного зменшення рівня інтегрального показника стійкості залізниці є сприятливим знаком.

Таблиця 4.14

Інтегральний показник стійкості підприємства

Період		Прогноз	Нижчий, 90%	Верхній, 90%
2013	2 півр.	0,73365	0,670	0,797
2014	1 півр.	0,71697	0,631	0,803
	2 півр.	0,71702	0,616	0,819
2015	1 півр.	0,71701	0,602	0,832

[1]Іванов В.Л. Управління економічною стійкістю промислових підприємств (на прикладі підприємств машинобудівного комплексу): Монографія. – Луганськ: Вид-во СНУ ім. В. Даля, 2005. – 265с.

Продовження таблиці 4. 15

Період		Прогноз	Нижчий, 90%	Верхній, 90%
	2 півр.	0,71702	0,591	0,843
2016	1 півр.	0,71702	0,580	0,854
	2 півр.	0,71701	0,571	0,863
2017	1 півр.	0,71701	0,562	0,872
	2 півр.	0,71701	0,553	0,881
2018	1 півр.	0,71701	0,545	0,889

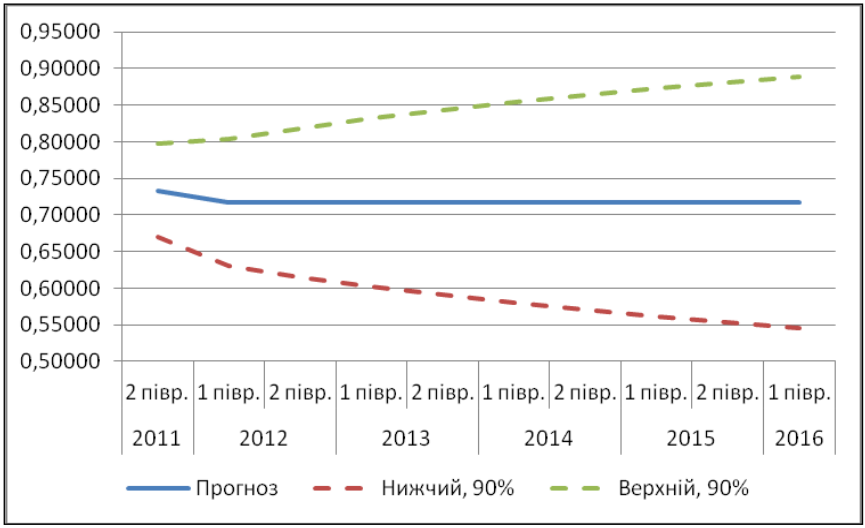


Рис. 4.34 Графік прогнозних значень інтегрального показника стійкості

Наближення показника інтегральної стійкості до стандарту дозволить знизити кошти які вилучені з обороту і направити їх на розвиток підприємства в цілому.

РОЗДІЛ 5

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ЯК СКЛАДОВА ЙОГО ЕКОНОМІЧНОЇ БЕЗПЕКИ

5.1. Сутність і зміст інформаційної безпеки промислового підприємства

Одним з основних завдань корпоративної інформаційної системи (КІС) як і будь-якої іншої технічної системи, є сервісний супровід бізнес-процесів. Будь-яка використана в бізнесі технічна система, будучи важливим елементом інфраструктури, повинна надавати бізнесу певний тип сервісу. КІС надає бізнесу інформаційний сервіс, але й сама потребує підтримки та захисту[1234], особливо в умовах рейдерських загроз. Сервіс полягає в наданні бізнесу необхідної інформації потрібної якості, в потрібний час і в потрібному місці, тобто зрештою інформації для управління самим бізнесом.

По суті, інформація в такому розумінні стає одним з ключових елементів інформаційної інфраструктури[5678910].

---

[1]Кузнецов А. А. Защита деловой информации. - "Экзамен", 2008. - 255 с.

[2]Леоненков А В. Нечеткое моделирование в среде MATLAB и fuzzy ТБСИ. - СПб: БХВ-Петербург. 2009. - 736 с.

[3]Липаев В.В. Стандарты на страже безопасности информационных систем//РС WECC/RR - 2000. - №30. - С. 34-40.

[4]Малкж А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. - М: Горячая линия. Телеком, 2004.- 280 с.

[5]Медынский В.Г., Ильдеменов С.В. Реинжиниринг инновационного предпринимательства: Учеб. пособие/Под ред. проф. В.Л. Ирикова. - М.: ЮНИТИ, 1999. - 414 с.

[6]Петраков А., Мельников В., Клейменов С. Информационная безопасность и защита информации (3-е издание): - "Academia", 2008. - 336 с.

[7]Петраков А., Мельников В., Клейменов С. Информационная безопасность (2-е издание). — "Academia", 2007.- 336 с.

[8]Партыка Т.Л., Попов И.И. Информационная безопасность (2-е издание). - "Форум", 2007. - 368 с.

[9]Морозов Н. П., Чернокнижный С. Б. Защита деловой информации для всех. – М.: "ИД "Весь!"", 2003. -160 с.

[10]Персональный сайт ведущего украинского специалиста в области защиты информации Домарева В. В.[Электронный ресурс] http://www.security.ukrnet.net/

Ще однією бізнес-задачею корпоративної системи інформаційної безпеки(ІБ) є забезпечення гарантій достовірності інформації, або, кажучи іншими словами, гарантій довірливості інформаційного сервісу КІС[12].

Забезпечення інформаційної безпеки носить комплексний характер і передбачає необхідність поєднання законодавчих, організаційних та програмно-технічних заходів.

Під інформаційною безпекою будемо розуміти захищеність інформаційних активів як частини інфраструктури бізнес-процессів, від випадкових або навмисних впливів власного або штучного характеру, що можуть призвести нанесенням шкоди власникам або користувачам інформаційних активів в бізнес-системі як частини підтримуючої інфраструктури.

Захист інформаційних активів полягає в підтримці цілосності, доступності та, якщо буде потрібно, конфіденційності інформаційних активів в бізнес-системах (рис. 5.1).

Забезпечення інформаційної безпеки потребують різні категорії господарюючих суб'єктів. Залежно від рівня відповідності господарюючих суб'єктів реалізуються відповідні їм рівні забезпечення захищеності інформаційних активів (табл. 5.1.).

Рис. 5.1. Принципи забезпечення інформаційної безпеки

[1]Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность - М.: Компания АйТи; ДМК Пресс, 2004.- 384 с.

[2]Райх В.В., Тихонов В.А. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. – М.: "Гелиос АРВ", 2006. - 528 с.

Таблиця 5.1.

Розподіл рівнів захищеності інформаційних активів за категоріями господарюючих суб'єктів

Категорія господарюючого суб'єкта	Рівень захищеності
Держава	Концептуально-політичний Законодавчий Нормативно-технічний
Фінансова система: 1. суб'єкти господарювання (комерційні структури, домашні господарства); 2. фінансові посередники; 3. фінансові ринки	Адміністративний Програмно-технічний

На концептуально-політичному рівні приймаються документи, в яких визначаються напрями державної політики інформаційної безпеки, формулюються цілі та завдання забезпечення ІБ всіх господарюючих суб'єктів (табл.5.1), намічаються шляхи і засоби досягнення поставлених цілей і вирішення завдань.

На законодавчому рівні створюється і підтримується комплекс заходів, спрямованих на правове регулювання забезпечення ІБ, що відображаються у законах та інших правових актах (укази президента, постанови уряду тощо). Однією з важливих завдань цього рівня є створення механізму, що дозволяє узгодити процес розробки законів з прогресом інформаційних технологій (ІТ)[1] .

На нормативно-технічному рівні розробляються стандарти, керівні матеріали, методичні матеріали та інші документи, що регламентують процеси розробки, впровадження та експлуатації засобів забезпечення ІБ. Важливим завданням цього рівня в даний час є приведення українських стандартів у відповідність з міжнародним рівнем інформаційних технологій взагалі та інформаційної безпеки зокрема.

На рівні підприємства чи іншого господарюючого суб'єкта здійснюються конкретні заходи щодо забезпечення ІБ ділової діяльності адмі-

[1]Рамазанов С.К., Истомин Л.Ф., Припотень В.Ю. Синергетическая модель управления эколого-экономической безопасностью предприятия в условиях нестабильности.//Вестник ДДМА. – Краматорск: ДДМА, 2007. – № 2 (8). – С. 25-28.

ністративного та програмно-технічного рівня[1234567891011121314 15] . На адміністративному рівні керівництво будь-якої організації реалізує заходи загального характеру і конкретні заходи забезпечення ІБ[16]. Основою заходів загального характеру служать політика безпеки (сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих з нею ресурсів).

У числі конкретних заходів щодо забезпечення ІБ можна виділити:

– управління персоналом;

---

[1]Гришина Н. В. Организация комплексной системы защиты информации – М.: "Гелиос АРВ", 2007. - 256 с.

[2] Ивлев В. А., Попова Т.В. Процессная организация деятельности: методы и средства. (Консалтинговая компания «ВИЛ Анатех»): [Электронный ресурс]: http://www.optim:ru/comp/2001/3/anatech/anatech.asp, 12.01.2005.

[3] Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность - М.: Компания АйТи; ДМК Пресс, 2004.- 384 с.

[4] Рамазанов С.К., Истомин Л.Ф., Припотень В.Ю. Синергетическая модель управления эколого-экономической безопасностью предприятия в условиях нестабильности.//Вестник ДДМА. – Краматорск: ДДМА, 2007. – № 2 (8). – С. 25-28.

[5]Рамазанов С.К., Припотень В.Ю. Методы и информационные технологии управления предприятием в условиях нестабильностей. Монография. - Луганськ: Видво СНУ ім. В. Даля, 2006. – 236 с.

[6]Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика издательство "Гелиос АРВ", 2006. – 240 с.

[7]Садердинов А.А., Федулов А.А., Трайнев В.А. Информационная безопасность предприятия. Учебное пособие. -"Дашков и Ко", 2004. - 336 с.

[8]Сайт государственной службы специальной связи и защиты информации Украины [Электронный ресурс] http://www.dstszi.gov.ua.

[9]Северин В. А. Комплексная защита информации на предприятии. Учебник. - Городец, 2008. – 124 с.

[10]Семкин А. Н., Семкин С. Основы правового обеспечения защиты информации. - М.: "Горячая линия-Телеком", 2008. - 238 с.

[11]Симонов С. В. Методология анализа рисков в информационных системам/Конфидент. - 2011, № 1. - С. 48-53.

[12]Симонов СВ. Технологии аудита информационной безопасности// Конфидент. Защитаинформации.- 2008, № 2. - С. 36-41.

[13]Система управления информационной инфраструктурой предприятия: [Электронный ресурс]: http://www.ecoprog.ru/suii.shtml. 16.04.2005.

[14]Система управления информационной инфраструктурой: [Электронный ресурс]: http://www.incom.ua/products / Software integration/Standart- software-solutions / sysmanage/ index.shtml, 16.10.2005.

[15]Современные подходы к управлению информационной инфраструктурой: [Электронный ресурс]: www.computel.ru, 17.11.2004.

[16]Старкова Н.О., Костецкий А.Н. Проблемы количественной оценки объема интеллектуальных активов фирмы: [Электронный ресурс]:http://intel-assetshl.ru/artieles/articlell.htm, 28.05.2005.

– фізичний захист;

– підтримка працездатності;

– реагування на порушення режиму безпеки;

– планування відновлювальних робіт.

На програмно-технічному рівні реалізуються наступні механізми безпеки:

– ідентифікація та перевірка справжності користувачів;

– управління доступом;

– протоколювання й аудит[1] ;

– криптографія;

– екранування.

На рівні окремого підприємства (компанії, корпорації, фірми) окремо розглядаються питання інформаційної безпеки, пов'язані з адміністративним і програмно-технічного рівням[2].

Під загрозою інформаційній безпеці автоматизованої системи розуміють можливі дії на цю систему, які прямо чи опосередковано можуть зашкодити її безпеці[3].

Прийнято вважати, що ІБ інформаційної системи забезпечено у разі, якщо для будь-яких інформаційних ресурсів у системі підтримується певний рівень конфіденційності, цілісності та доступності[4]. Тому для інформаційних систем розглядають три основні види загроз:

– загроза порушення конфіденційності;

– загроза порушення цілісності;

– загроза відмови служб.

Саме поняття загрози в рівних ситуаціях найчастіше трактується по-різному.

Наприклад, для підкреслено відкритої організації може просто не існувати загроз конфіденційності - вся інформація вважається загально-

---

[1]Степанов Е., Корнеев И. Защита информации в офисе. – М.: "ТК Велби", 2007. - 336 с.

[2]Стрелкова Е.. Интеграция данных предприятия//Открытые системы, 2003. Апрель. С. 58-61.

[3]Тельнов Ю. Ф. Реинжиниринг бизнес-процессов. - М.: МЭСИ, 1999. -106 с.

[4]Троников И.Б. Пазухин А.В., Коробейникова Н.А. Применение интеллектуальных систем при управлении производством. В книге "Труды международных научно-технических конференций "Интеллектуальные системы (IEEE AIS'06)" и "Интеллектуальные САПР (CAD- 2006)". Научное издание в 3-х томах. М.: Изд-во Физико-математической литературы, 2006, Т.2. – С. 494-495.

доступною, а проте в більшості випадків нелегальний доступ вважається серйозною небезпекою[1]

Знання можливих загроз, а також уразливих місць захисту, яким ці загрози зазвичай погрожують, необхідно для того, щоб вибирати найбільш економічні засоби забезпечення безпеки[2,3].

Найпоширенішими і найнебезпечнішими (з точки зору розміру шкоди) є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Іноді такі помилки є погрозами (неправильно введені дані, помилка в програмі, що викликала крах системи), іноді вони створюють слабкості, якими можуть скористатися зловмисники (такі зазвичай помилки адміністрування). Згідно[4] , 65% втрат - наслідок ненавмисних помилок. Пожежі та повені можна вважати дрібницями в порівнянні з некомпетентністю і неуважністю. Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками - максимально можлива автоматизація і строгий контроль за правильністю скоєних дій.

На другому місці за розмірами збитку розташовуються крадіжки та підробки. Можна припустити, що справжній збиток набагато більше, оскільки багато організацій зі зрозумілих причин приховують такі інциденти. У більшості розслідуваних випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи та захисними заходами[5]. Це ще раз свідчить про те, що внутрішня загроза набагато небезпечніше зовнішньої.

Досить небезпечні так звані «скривджені» співробітники - нинішні і колишні. Як правило, їх діями керує бажання завдати шкоди організації-кривднику, наприклад:

– пошкодити обладнання;

---

[1]Троников И.Б., Извозчикова В.В., Матвейкин И.В. и др. Концептуальная модель управления предприятием// Изв. вузов. Приборостроение. 2008. Т. 51, № 5. С. 26—29.

[2]Троников И.Б., Коробейников А. Г., Нестерова Н. А., и др. Процессный подход при управлении качеством продукции на предприятиях, осуществляющих выпуск электронного приборного оборудования//Датчики и системы. № 6, 2008, с. 31-34.

[3]Шелупанов А.А., Шумский А.А. Системный анализ в защите информации. – М.: "Телиос АРВ", 2005. - 224 с.

[4]An Introduction to Computer Security: 'Ibe NTST Handbook. Draft — National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. 2010.

[5]Common Criteria for Information Technology Security evaluation. Version 1.0, 96,01.31.

– вбудувати логічну бомбу, яка з часом зруйнує програми та/або дані;

– внести невірні дані;

– видалити дані;

– змінити дані;

– розмістити конфіденційну або іншу корпоративну інформацію в мережі Інтернет для відкритого доступу;

– спробувати продати конфіденційну інформацію або частину бази даних(БД) конкурентам і т. д.

Ображені співробітники, навіть колишні, знайомі з порядками в організації і здатні наносити вельми великої шкоди організації. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів анулювалися.

Загрози, які виходять від навколишнього середовища, на жаль, відрізняються великою різноманітністю. У першу чергу слід виділити порушення технологічної інфраструктури - аварії електроживлення, тимчасова відсутність зв'язку, перебої з водопостачанням тощо Небезпечні, зрозуміло, стихійні лиха, громадянські заворушення та події, що сприймаються як стихійні лиха - пожежі, повені, землетруси, урагани. За даними[1], на частку вогню, води та аналогічних "ворогів" (серед яких найбільш небезпечний - низька якість електроживлення та його перебої) припадає 13% втрат, завданих інформаційним системам.

На сучасному етапі розвитку інформаційних технологій підсистеми або функції захисту є невід'ємною частиною комплексів з обробки інформації. Інформація не представляється в чистому вигляді.

На шляху до неї є хоча б яка-небудь система захисту, яку необхідно подолати атакуючої стороні. Однак не існує абсолютно стійкою системи захисту, питання лише в часі і коштах, потрібних на її подолання.

Відповідно до даних умов, прийнятною можна вважати наступну модель: захист інформаційної системи вважається переборною, якщо в ході її дослідження визначені уразливості системи.

Уразливість - це деякий невдале властивість системи, яка робить можливим виникнення і реалізацію загрози ІБ.

---

[1]An Introduction to Computer Security: 'Ibe NTST Handbook. Draft — National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. 2010.

Проведений аналіз можливих загроз показав, що інформаційна інфраструктура повинна мати властивість захищеності інформації, використовуваної в бізнес-процесах. Дана властивість характеризує здатність забезпечувати захист від несанкціонованого (навмисного чи випадкового) отримання, зміни, знищення або використання комерційної, службової або технологічної інформації, особливо в умовах рейдерських загроз.

З урахуванням компонентів бізнес-процесу, показаних на рис. 5.1, а також їх взаємозв'язків, до потенційно небезпечних ситуацій, які можуть виникнути при низькому рівні захищеності інформації, відносяться:

– несанкціонований доступ порушників (не власників та учасників) до інформації, що зберігається і оброблюваної в засобах автоматизації, з метою ознайомлення, спотворення чи знищень. Точками входу при цьому можуть бути інтерфейси і межі процесу, а також інформація, необхідна для реалізацій функцій (операцій, процедур) процесу;

– перехоплення інформації при її прийомі (передачі) по каналах зв'язку (мережі) функціями процесу, а також за рахунок розкрадання носіїв інформації;

–-знищення (зміна, спотворення) інформації за рахунок випадкових перешкод, збоїв технічних (програмних) засобів при передачі, зберіганні та обробці інформації;

– несанкціонований вплив на бізнес-процес порушників з числа власників та (або) учасників процесу.

На основі проведеного аналізу впливу інформаційної інфраструктури на реалізацію бізнес-процесів (рис. 5.2), аналізу змісту ІБ бізнесу, визначивши цілі і основні принципи функціонування інфраструктури, можна визначити низку пропонованих вимог до системи її захисту щодо бізнес-процесів.

Інформаційні активи є частиною інформаційної інфраструктури підприємства і вимагають захисту від можливих інформаційних загроз.

До складу елементів інфраструктури захисту інформації (ІЗІ) бізнес-процесів повинні бути включені засоби:

– управління доступом;

– реєстрації та обліку;

– криптографічні;

– забезпечення цілісності.

Згідно[1] встановлюється дев'ять класів захищеності автоматизованих систем від несанкціонованого доступу до інформації.

Кожен клас характеризується певною мінімальної сукупністю вимог щодо захисту.

Класи поділяються на три групи, що відрізняються особливостями обробки інформації в автоматизованій системі.

Рис. 5.2. Роль і місце інфраструктури захисту інформації в бізнес-системі

У межах кожної групи дотримується ієрархія вимог щодо захисту залежно від цінності (конфіденційності) інформації і, отже, ієрархія класів захищеності автоматизованих систем.

В роботі[2] також визначається номенклатура обов'язкових вимог, реалізація яких забезпечує рівень захисту інформації, відповідний обраному класу захищеності. Очевидно; що згідно системі класифікації, виконання всіх перерахованих вимог відповідає найвищому класу захищеності (4 А). Однак це не означає, що вказаний клас є потрібним для будь-якої системи захисту інформації. Високий рівень захищеності

[1]Северин В. А. Комплексная защита информации на предприятии. Учебник. - Городец, 2008. – 124 с.

[2]Северин В. А. Комплексная защита информации на предприятии. Учебник. - Городец, 2008. – 124 с.

може бути забезпечений компенсацією завідомо недоцільних вимог іншими засобами і, що найбільш ймовірно, організаційними заходами захисту. Так, наприклад, використання сертифікованих кріптозасобів веде до істотного підвищення вартості всієї системи захисту інформації. При цьому вартість цих коштів порівнянна з вартістю всіх інших засобів разом узятих. Тому відсутність криптосистеми або її окремих елементів може бути компенсовано всемірним обмеженням доступу до конфіденційної інформації, локалізацією та (або) відключенням інформаційних масивів від мережі, оптимізацією трафіку доступу та іншими програмними і технічними засобами, а також організаційними заходами захисту.

Разом з тим, сформульовані вимоги складають функціональну основу ІЗІ бізнес-процесів, тобто визначають обов'язковий (з урахуванням наведених вище зауважень) склад функцій за відповідними підсистемами захисту. Однак процесний підхід до організації та управління господарською діяльністю підприємства обумовлює необхідність застосування процесно-орієнтованого підходу і до формування самої-ІЗІ бізнес-процесів. З урахуванням розглянутих особливостей, структури і можливостей процесного підходу ІЗІ повинна забезпечувати:

– орієнтацію всіх процесів захисту на головний кінцевий результат - забезпечення максимального рівня захисту інформації;

– виявлення, локалізацію та усунення наслідків реалізації всіх можливих видів загроз;

– інтеграцію функцій захисту в єдиний автоматизований процес;

–-інтеграцію централізованого та ресурсозберігаючого управління захистом інформації;

–-регламентацію процесів зашиті по пріоритету, терміновості, ризикам і т.д.;

–-незалежність реалізації політики безпеки від організаційної структури підприємства;

–-реалізацію планово-попереджувальної діяльності щодо забезпечення захисту інформації бізнес-процесів;

–визначення та розмежування відповідальності конкретних заходів і засобів захисту за запобігання конкретних видів загроз;

– можливість точного визначення результатів функціонування (облік і звітність по кожному виду загроз, моніторинг поточного стану, прогноз розвитку процесів, оцінка ризиків і т.д.);

– можливість розвитку та оптимізації процесів захисту на основі самоконтролю та самоналаштованості;

– можливість адаптації до мінливих інформаційній інфраструктурі підприємства;

– мінімально можливу кількість рівнів в ієрархії управління системою захисту інформації;

– по можливості прості та зручні в експлуатації заходи та засоби захисту.

Процесно-орієнтований підхід до створення (вдосконалення) ІЗІ бізнес-процесів дозволить розглядати процес формування (розвитку) СЗІ як один з допоміжних бізнес-процесів, що забезпечують основні процеси підприємства. Це дасть можливість розробки ІЗІ в тісному взаємозв'язку з проектуванням інших бізнес-процесів, що безсумнівно збільшить їх інтегрованість, гнучкість, збалансованість і керованість.

5.2. Методи оцінки інформаційної захищеності від несанкціонованого доступу

Для оцінки інформаційної захищеності від несанкціонованого доступу (НСД), в умовах рейдерських загроз, розглянута сукупність множин:

$$H = \{h_1, h_2, .. h_f\}, S = \{s_1, s_2, ..., s_g\}, L = \{l_1, l_2, ..., l_k\},$$

$$Y = \{y_1, y_2, ..., y_q\}, U = \{u_1, u_2, ..., u_p\}, D = H \times S \times L,$$

де H - множина можливих порушників;

S - множина цілей порушників;

L - множина способів реалізації цілей дій порушників;

Y - множина факторів, що характеризують умови функціонування СЗІ;

U - множина варіантів засобів захисту;

D - множина моделей дій порушників.

Пропонується використовувати математичні моделі (ММ) функціонування СЗІ від НСД:

$$M_i : D \times Y \times U \to r, i = 1, ..., f,$$

де r - показник захищеності інформації від НСД;

f - число ММ функціонування засобів захисту.

У зв'язку з тим, що сформульована задача оцінки захищеності від НСД враховує різні типи порушників та їх дій, в основу оцінки

покладені методи прямого обчислення ймовірності деякої події, залежного від характеристик визначальних його чинників. При цьому в якості показника захищеності інформації використовується ймовірність підбору дозволеної комбінації пароля за певний інтервал часу, яка залежить від типу порушника, його мети і способу дій. Відмінною особливістю розробленого методу є врахування дій потенційних порушників як з числа штатних співробітників, так і сторонніх осіб.

Неточність і неповнота вихідної інформації призводять до необхідності застосування спеціальних методів оцінки показників захищеності інформації. До таких показників відноситься ймовірність перехоплення інформації при її прийомі (передачі). Для адекватної оцінки захищеності інформації від перехоплення використаний метод, заснований на апараті нечітких множин. Важлива гідність методів нечіткого моделювання полягає в тому, що вони не вимагають великих витрат часу і коштів у порівнянні з традиційними методами на отримання точних вихідних даних, що, може бути, в принципі, неможливо.

Процес нечіткого моделювання показника захищеності інформації від перехоплення ґрунтується на кількісному представленні вхідних і вихідних показників моделі у формі нечітких множин, які задаються на множині дійсних чисел у вигляді бальної шкали відносин.

З точки зору аналітичної обробки, найбільш зручні найпростіші випадки нечітких величин з кусково-лінійними функціями належності.

Беручи за основу для вимірювання значень показника рівня захищеності інформації від перехоплення 100-бальну шкалу відносин, пропонуються наступні значення лінгвістичних змінних, що визначають рівень якості захисту:

– дуже низький рівень якості. Цей рівень нижче мінімально необхідного відповідно до вимог до даного показника захищеності інформації від перехоплення;

– низький (початковий) рівень якості, відповідний мінімальним вимогам до показника захищеності інформації від перехоплення;

–середній рівень якості, характерний для показників захищеності інформації від перехоплення;.

– високий рівень захищеності інформації від перехоплення, характерний для добре захищених інформаційних систем;

– дуже високий рівень захищеності інформації від перехопленя, що виходить за межі 100-бальної шкали і відображає той факт, що немає межі у вдосконаленні інформаційної безпеки.

Принциповий алгоритм нечіткої оцінки якості захисту від перехоплення зводиться до отримання парних творів часткових показників якості у вигляді трикутних нечітких чисел і відповідних вагових коефіцієнтів, представлених також у вигляді трикутних нечітких чисел, з наступним складанням цих парних творів.

Неточність і неповнота вихідної інформації призводять до необхідності застосування спеціальних методів оцінки показників захищеності інформації. Перспективним напрямком для вирішення цього завдання є використання моделювання на основі використання апарату нечітких множин[1].

Важлива гідність методів нечіткого моделювання полягає в тим, що вони не вимагають великих витрат часу і коштів, але порівнянні з традиційними методами на отримання точних вихідних даних, що, може бути, в принципі, неможливо.

Поява цілої низки комерційних програмних засобів, орієнтованих на вирішення завдань нечіткого моделювання[1], свідчить про ефективність застосування методів нечітких множин для вирішення практичних завдань.

В основі методів нечіткого моделювання лежить поняття нечіткої множини (fuzzyset), що представляє сукупність елементів довільної природи, щодо яких не можна з повною визначеністю стверджувати - чи належить той чи інший елемент аналізованої сукупності даній множині чи ні.

Формально нечітка множина визначається як множина впорядкованих пар або кортежів виду:

$$A = \{< x, \mu_A(x) >\}, \forall x \in X .$$

де X - універсальна множина (універсум), що містить в рамках нечіткої множини елемент x;

$\mu_A(x)$ - функція приналежності елемента x нечіткій множині A;

$\mu_A(x) \in [0,1] \ \forall x \in X$.

Множина X представляє з себе так званий носій нечіткої множини, це звичайна (чітка) множина елементів x.

Функція приналежності (membership function) - математична функція, що визначає ступінь або впевненість, з якою елемент множини X

[1]Шелупанов А.А., Шумский А.А. Системный анализ в защите информации. – М.: "Телиос АРВ", 2005. − 224 с.

належить заданій нечіткій множині *A*. Дана функція ставить у відповідність кожному елементу *x* дійсне число з інтервалу [0,1]. Чим ближче це число до одиниці, тим більше ступінь чи впевненість, з якою елемент x належить нечіткій множині A.

Вибір функції приналежності є творчим завданням експерта або групи експертів. В принципі, вид функції приналежності може бути обраний будь-яким. Однак, для спрощення розрахунків і скорочення обсягу вихідної інформації доцільно використовувати ті з них, які допускають аналітичне представлення у вигляді простої математичної функції.

Вибір типових функцій належності повинен бути узгоджений з можливостями їх програмної реалізації у використаних інструментальних засобах.

Лінгвістична змінна характеризується найменуванням та множиною значень (термів), кожна з яких визначається своєю функцією приналежності. Прикладом лінгвістичної змінної є «Захищеність інформації від перехоплення», а значеннями цієї лінгвістичної змінної можуть бути: «Середній рівень захищеності інформації від перехоплення» з функцією приналежності $\mu_{ср}(x)$, «Високий рівень захищеності інформації від перехоплення» з функцією приналежності $\mu_{вис}(x)$ і т. д.

Набули поширення такі типи функцій належності, як кусково-лінійні Z-образні, S-образні і дзвоновидні функції приналежності.

Процес моделюванні показника захищеності інформації від перехоплення грунтується на кількісному представленні вхідних і вихідних показників моделі у формі нечітких множин, які задаються на множині дійсних чисел у вигляді бальної шкали відносин.

Задані на множині дійсних чисел нечіткі множини називають нечіткими величинами., З точки зору аналітичної обробки, найбільш зручні найпростіші окремі випадки нечітких величин з кусково-лінійними функціями належності. Залежно від виду функції приналежності, розрізняють такі нечіткі величини, як трикутне нечітке число і трапецієподібний нечіткий інтервал.

Вхідні і вихідні нечіткі величини в моделях оцінки якості можуть бути представлені також кусково-лінійною Z-подібної та кусково-лінійної S-подібною функціями належності.

Трикутне нечітке число може бути представлено у вигляді кортежу з трьох чисел:

$$A_{\Lambda} = < b, \alpha, \beta >,$$

де b - модальне значення трикутного числа, якому відповідає функція приналежності $\mu_{\Lambda}^{\Delta}(b)=1$;

α і β - лівий і правий коефіцієнти нечіткості трикутного нечіткого числа $(a=b\text{-}\alpha); c=b+\beta$.

Пропонований метод нечіткої оцінки якості захищеності інформації від перехоплення включає в себе три етапи:

1. Фазифікації первинних показників системи показників оцінки захищеності інформації від перехоплення.

2. Висновок підсумкового показника оцінки захищеності інформації від перехоплення у вигляді нечіткого числа.

3. Дефаззіфікації показника оцінки захищеності інформації від перехоплення.

Під фазифікацією (fuzzification) у розглянутому методі розуміється процес отримання значень функцій належності для термів лінгвістичних змінних, які мають первинні показники захищеності інформації, від перехоплення.

Принципово алгоритм нечіткої оцінки якості захисту від перехоплення зводиться до отримання добутків часних показників якості у вигляді трикутних нечітких чисел і відповідних вагових коефіцієнтів, представлених також у вигляді трикутних нечітких чисел, з наступним складанням цих парних добутків.

Оцінки якості захищеності інформації від перехоплення можна представити таким чином:

$$r_{ij} = \sum k_{jk}^{\Delta} r_{ijk}^{\Delta}, \forall i \in I, \forall j \in J,$$

де r_{ij} - значення узагальненого показника якості захищеності інформації від перехоплення;

r_{ijk}^{Δ} - значення k-го приватного показника якості захищеності у вигляді трикутного нечіткого числа;

k_{jk}^{Δ} - ваговий коефіцієнт k-го приватного показника якості захищеності у вигляді трикутного нечіткого числа;

J - множина інформаційних активів;

I - множина засобів захисту інформації від перехоплення;

N - множина приватних показників якості захищеності від перехоплення.

Таким чином, у пропонованому алгоритмі виведення підсумкового показника оцінки якості присутні операції множення трикутних нечітких чисел. В результаті виконання цих операцій також виходить трикутне нечітке число, розраховується згідно з наступними формулами.

Нехай b^{Δ} і g^{Δ} два трикутних нечітких числа (наприклад, показник якості та його ваговий коефіцієнт), заданих параметрично у вигляді кортежів:

$$b^{\Delta} =< a_1, \alpha_1, \beta_1 >,$$

$$g^{\Delta} =< a_2, \alpha_2, \beta_2 >.$$

Тоді парний добуток цих чисел дорівнює:

$$g_1 = g^{\Delta} b^{\Delta} =< a_3, \alpha_3, \beta_3 >,$$

де параметри a_3, α_3, β_3 визначаються таким чином:

$$a_3 = a_1 a_2$$
$$\alpha_3 = a_1 \alpha_2 - a_2 \alpha_1$$
$$\beta_3 = a_1 \beta_2 - a_2 \beta_1$$

Складання двох трикутних нечітких чисел: призводить до появи наступного трикутного числа:

$$g_1 =< a_3, \alpha_3, \beta_3 >,$$

$$g_2 =< a_4, \alpha_4, \beta_4 >.$$

призводить до появи наступного трикутного числа:

$$g_3 = g_1 + g_2 =< a_5, \alpha_5, \beta_5 >,$$

де параметри a_5, α_5, β_5 визначаються таким чином:

$$a_5 = a_3 + a_4,$$
$$\alpha_5 = \alpha_3 + \alpha_4,$$
$$\beta_5 = \beta_3 + \beta_4.$$

Дефаззифікація результатів

Підсумковий показник оцінки якості, що отримується в результаті згортки часткових нечітких показників, являє собою непарне трикутне число.

Відповідно до пропонованого методу для практичного використання підсумкового показника передбачається його дефаззіфікація

(defuzzincation), що означає отримання чіткої інтервальної оцінки або єдиного кількісного значення показника.

Для цілей дефаззіфікації пропонується використовувати поняття чіткої множини (інтервалу), найближчого до нечіткій множині (інтервалу). Характеристична функція найближчої чіткої множини стосовно нечіткій множині визначається наступним виразом:

$$\mathrm{X}_{\Lambda}(x)=\begin{cases}0,\ якщо\ \mu_{\Lambda}(x)<0.5\\ 1,\ якщо\ \mu_{\Lambda}(x)>0.5\\ 0\ або\ 1,\ якщо\ \mu_{\Lambda}(x)=0.5\end{cases}$$

де $\mu_{\Lambda}(x)$ - функція приналежності.

Характеристична функція приймає значення 1 для кожного елемента даної чіткої множини і значення 0 для всіх інших елементів, що не входять в дану множину.

Для приведення значення показника рівня якості захищеності інформації від перехоплення до єдиного числа ймовірності перехоплення, інтервальна оцінка може бути замінена середнім значенням чіткого інтервалу (медіаною) або ж повинна бути використана додаткова інформація.

Показник захищеності інформації від знищення (пошкодження) при збоях залежить від можливостей відновлювальних резервів, інформаційного та програмного забезпечення (ПЗ) інформаційної інфраструктури.

У зв'язку з тим, що перераховані кількісно-якісні параметри інформаційного і ПЗ є вихідними і залежать від структури конкретної інформаційної системи, в основу оцінки захищеності від збоїв покладені методи прямого аналітичного оцінювання ймовірності події, що полягає в успішності вирішення всього обсягу задач в умовах можливого руйнування (відновлення) ПЗ і інформаційних масивів (ІМ).

Тоді, вирази для визначення ймовірності успішного вирішення всього обсягу завдань, часу вирішення завдань, величину обсягу потоку інформації, що циркулює в комп'ютерній мережі при вирішенні кожним абонентом $\Lambda_{jhk}(j=1,2,\ldots,L;k=1,2,\ldots,K;h=1,2,\ldots,m_j)$ мають вигляд:

$$p_{jhk}=\tau_{jhk}\sum_{l=1}^{L}P_{jhkl}^{B}P_{jlhk}^{\Pi}x_{hl}\prod_{f=1}^{M}\sum_{r=l}^{L}y_{fr}(P_{lkfr}^{0}\overline{P}_{lrkf}^{\Pi})g_{jhkr},$$

$$T_{ihk}^{piш}=\frac{1}{\tau_{jhk}}\sum_{l=1}^{L}x_{hl}(T_{jlhk}+t_{jhkl}^{piш}+Q_{jhkl})t_{kl}^{B}+\sum_{f=l}^{M}q_{ijkf}\sum_{r=1}^{L}(\overline{T}_{lrkf}+\overline{Q}_{lkfr}t_{fr}^{B})y_{fr},$$

$$\Lambda_{jhk} = \lambda_{jhk} \left[\begin{array}{l} \sum_{i=1}^{L} X_{ki} \left[F_{ji} l_{jhk}^{B} + F_{ij} l_{jhk}^{0} + Q_{jhki} \sum_{l=1}^{L} \Psi_{kl} (F_{il} l_{k}^{B} + F_{li} u_{k}) \right] + \\ + \sum_{f=1}^{M} \sum_{r=1}^{L} \sum_{g=1}^{q_{jhkf}} y_{fr} \left[F_{ri} \bar{l}_{kqf}^{B} + F_{ir} l_{kqf}^{0} + \overline{Q}_{ikfr} \sum_{l=1}^{L} \phi_{fr} (F_{rl} l_{f}^{B} + F_{lr} \delta_{f}) \right] \end{array} \right].$$

де $P_{jlhk}^{\Pi}(\overline{P}_{lrhf}^{\Pi})$ ймовірність успішної передачі інформації між вузлами $j(l)$ і $i(r)$ при вирішенні h-м абонентом j-им комп'ютером (розміщеного в l-му вузлі) k-ї задачі (до f-го ІМ).

$$P_{jlhk}^{\Pi} = P_{jihk}^{B} P_{jihk}^{0}; \overline{P}_{lrkf}^{\Pi} = \overline{P}_{lrkf}^{B} \overline{P}_{lrkf}^{0}.$$

$P_{ijhk}^{B}(P_{irlj}^{B})$ - імовірності доведення запиту на рішення (на доступ до інформації) та повідомлення, що містить результати рішень (звертання) h-м абонентом (k-м ІМ) j-м комп'ютером (розміщення в l-му комп'ютері) k-ї задачі (до f-го ІМ) в i-му вузлі (що знаходиться в r-му вузлі) мережі відповідно;

$P_{jhkl}^{B}, P_{lkfr}^{0}$ - імовірність того, що k-й ІМ, що зберігається на l-му комп'ютері не буде в процесі звернення до нього h-м абонентом зруйнований або ж буде успішно відновлений, і ймовірність того, що f-й ІМ, що зберігається на r-му комп'ютері не буде в процесі звернена до нього k-го ІМ знаходиться на l-му комп'ютері зруйнований або ж буде успішно відновлений;

Q_{jhkl} - імовірність того, що k-ий ІМ, що зберігається в l-му вузлі буде зруйнований до моменту звернення до нього h-го абонента j-го комп'ютера, $Q_{jhkl} = r_{kl} + (1 - r_{kl}) g_{jhkl}$;

$\overline{Q}_{lkfr}$ - імовірність того, що f-ий ІМ, що зберігається в r-му вузлі буде зруйнований до моменту звернення до нього k-го ІМ, що зберігається на i-му комп'ютері, $\overline{Q}_{jhkl} = \bar{r}_{fr} + (1 - \bar{r}_{fr}) \bar{g}_{ikfr}$;

$T_{jlhk}(\overline{T}_{lrkf})$ - середній час передачі повідомлення з i-го (l-го) вузла мережі в j-й (r-й) при рішенні (зверненні) h-м абонентом (k-го ІМ) i-го комп'ютера (розміщеного в l-му вузлі) k-ї задачі (до f - го ІМ);

$\tau_{jhk} = 1$ якщо h-й абонент на j-му комп'ютері має право вирішувати k-у задачу, $\tau_{jhk} = 0$ в іншому випадку;

g_{jhkr} - число звернень k-го ІМ до r-го ІМ при вирішенні h-м абонентом на i-му комп'ютері.

Оцінивши всі складові, які залежать від наявності та можливостей відновного резерву, представляється можливим оцінити рівень захищеності від знищення (пошкодження) інформації при збоях. При цьому ймовірність знищення (пошкодження) інформації при збоях потрібно асоціювати з мінімальною ймовірністю рішення задачі, яка визначається можливим руйнуванням ПО, тобто

$$r_y = \min\{P_{jhk}\},\ j \in L,\ h \in m_j,\ k \in K.$$

Несанкціоноване втручання в бізнес-процес є загрозою, що принципово відрізняється від загрози несанкціонованого доступу до інформації. Загроза втручання припускає наявність порушника, що володіє в загальному випадку всіма правами доступу. Для оцінки захищеності від несанкціонованого втручання пропонується використовувати теорію ігор, яка дозволяє вирішувати завдання в умовах невизначеної інформації про дії «зловмисника» (що відповідає вказаному типу порушників). Задача розглядається як гра двох осіб: проектанта (першого гравця) проти «природи» (другого гравця), фіктивного гравця, стратегії якого нам невідомі.

Позначимо через $\tilde{A}_1$ гру, в якій перша сторона (СЗІ) вибирає варіант захисту $i \in M$, а друга сторона (система інформаційного нападу) вибирає, причому одночасно, варіант нападу $j \in N$. Ця ситуація характерна тим, що обидві сторони знають множини M, N, але їм невідомий конкретний вибір противника. В якості цільової функції ефективності першою стороною приймається відома обом сторонам функція захищеності інформації в розглянутій бізнес-системі.

Будемо вважати, що функція захищеності $R(i,j)$ визначена і обмежена на $N \times M$. Число $S_1 = \sup_{i \in M} \inf_{j \in N} R(j,i)$ є найкращий гарантований результат в $\tilde{A}_1$ для першої сторони (нижнє значення гри $\tilde{A}_1$). Аналогічно, $\tilde{A}_2$ означає гру, в якій друга сторона вибирає $j \in N$, а потім перша сторона, точно знаючи результат вибору другої сторони, виби-

рає $i \in M$. Число $S_2 = \inf\limits_{j \in N} \sup\limits_{i \in M} R(j,i)$ є найкращий гарантований результат для першої сторони в $\tilde{A}_2$ (верхнє значення гри $\tilde{A}_2$). Ігри $\tilde{A}_1$ та $\tilde{A}_2$ відповідають двом крайнім ступенями інформованості першої сторони про вибір другої сторони: в $\tilde{A}_2$ має місце точна інформація про конкретний виборі, тоді як у $\tilde{A}_1$ відомо лише, що цей вибір здійснений з множини *N*. Якщо практична реалізація величини S_1 першої сторони в $\tilde{A}_1$ ніяк не пов'язана з поведінкою другої сторони, то для реалізації S_2 в $\tilde{A}_2$ необхідне використання точної інформації про вибір другої сторони, розуміючи під реалізацією або досяжністю гарантованих фіналів їх досяжність з точністю до довільного малого $\varepsilon > 0$. Якщо $S_1 = S_2$, то функція $R(j,i)$ має узагальнену седловую крапку на $N \times M$. У цьому випадку для досягнення гарантованого результату S_2 немає необхідності в отриманні якої б то не було інформації про конкретний вибор другої сторони, і цей результат досяжний першою стороною і в $\tilde{A}_1$.

Реально ж стратегіями першої сторони в $\tilde{A}_1$, будуть всілякі функції $i(k)$, визначені на k зі значеннями в M. За аналогією з вищенаведеним найкращий гарантований результат в $\tilde{A}_1$, для першої сторони є число

$$S = \sup_{i(k)} \inf_{j \in N} \inf_{k \in K(j)} R(j, i(k)) = \sup_{i(k)} \inf_{k \in K} \inf_{j \in N_k} R(j, i(k)) = \inf_{k \in K} \sup_{i \in M} \inf_{j \in N_k} R(j,i)$$

З відомими обмеженнями число S може бути асоційоване з імовірністю захищеності від несанкціонованого втручання в бізнес-процес (протиправного захоплення підприємства).

5.3. Комплексна оцінка інформаційної захищеності підприємства

Відповідно до концептуальної моделі запропоновано метод отримання комплексної оцінки інформаційної захищеності бізнес-процесів.

Одним з основних законів розвитку систем (захисту інформації (ЗІ) є взаємозв'язок показників. При зміні одного показника, навіть найбільш важливого, його вплив на зростання узагальненого показника поступово згасає через обмеження, створювані іншими показниками, які залишаються незмінними. Постійний темп зростання узагальненого показника може бути при одночасній і пропорційній зміні всіх показників, що входять в систему. Значить, якщо оцінюється рівень конкретної ІЗІ з певними значеннями показників, то кожен з них має постійну вагомість. Якщо в новій ІЗІ, в порівнянні з базовою, змінений хоча б один показник, то змінюються вагомості всіх показників, що входять в ієрархію. З системології відомо, що описане вище явище загасання впливу одного показника на узагальнений, зазвичай характеризується показовими або експоненціальними залежностями, що мають ділянку насичення.

Цілям визначення рівня інформаційної захищеності в найбільшій мірі відповідають методи, засновані на отриманні узагальненої оцінки, шляхом агрегування одиничних показників в узагальнені за допомогою коефіцієнтів вагомості. Найбільш поширеною узагальненої оцінки є адитивна функція виду:

$$R_0 = \sum_{i=1}^{N} K_i r_i$$

де N - число показників знаходяться на нижньому рівні ієрархії;

K_i - коефіцієнт вагомості показника *i*-ї властивості.

При цьому кожна властивість може характеризуватися одним або декількома одиничними показниками.

Завдання полягає в тому, щоб виразити в узагальненому показнику певні кількості різних за якістю властивостей. Для того, щоб порівняти різні кількості різноякісних показників, їх необхідно привести до безрозмірної шкали, тобто кожному показнику, що має розмірність і свою шкалу виміру, ставиться у відповідність безрозмірний показник. Такий перехід можна здійснити, якщо допустити таке.

При функціонуванні ІЗІ кожен з *i*-их одиничних показників може залишатися постійним, приймати ряд дискретних значень або змінитися безперервно:

$$a_{i\min} < a_{ij} < a_{i\max}, \quad i = 1,\ldots,N,\ j = 1,\ldots,m,$$

де m - число дискретних значень, які показник приймає в процесі експлуатації;

$a_{i\min}, a_{i\max}$ - граничні значення показника, що визначаються технічними умовами (можливостями);

a_{ij} - j-е значення *i*-го показника.

У діапазоні $[a_{i\min}, a_{i\max}]$ кожному j-му значенню *i*-го показника відповідає ймовірність того, що це значення реалізується в процесі функціонування ІЗІ. Ця ймовірність описується функцією щільності розподілу ймовірностей $\varphi_i(a_{ij})$.

У загальному випадку діапазон зміни *i*-го показника в ІЗІ може бути менше, ніж діапазон $[a_{i\min}, a_{i\max}]$:

$$a_{iн} > a_{i\min},\ a_{iв} < a_{i\max},$$

де $a_{iн}$, $a_{iв}$ - граничні (нижнє і верхнє) значення показників *i*-ї властивості в реальної ІЗІ.

Тоді безрозмірний показник r_i, що виражає співвідношення досягнутого значення до необхідного, визначається з вираження:

$$r_i = \int_{a_{iн}}^{a_{iв}} \varphi_i(a_{ij})da_{ij}$$

Очевидно, що діапазон виміру безрозмірного показника- $0 \le r_i \le 1$

У разі рівномірного розподілу способи переходу до безрозмірних показників приймуть вигляд:

$$r_i = \frac{a_{iв} - a_{iн}}{a_{i\max} - a_{i\min}}.$$

Далі необхідно визначити коефіцієнти вагомості K_i. При цьому слід вважати, що коефіцієнт вагомості будь-якого *i*-го показника відображає відносну вагомість (важливість) однієї одиниці r_i по відношенню до інших безрозмірних показників, що знаходяться на одному рівні ієрархії.

Добуток під знаком суми узагальненого показника показує кількісний внесок кожної властивості в комплексну властивість. Будь-яка властивість ІЗІ стає реальністю, будучи відбито в якому-небудь показнику.

Отже, вагомість, характеризує важливість *i*-ї властивості по відношенню до сукупності інших властивостей, залежить від показників цих властивостей, тобто,

$$K_i = F(r_1, r_2, ..., r_N).$$

Природно, що для конкретної ІЗІ добуток $K_i r_i$ є величина постійна.

Помножники добутку $(K_i r_i)$ можуть, приймати будь-які значення в залежності від вибору системи координат, але такі, що за будь-яких перетворень

$$K_i^{j_k} r_i^{j_k} = const, \quad (5.1)$$

де j_k - номер системи координат або номер перетворення.

Вираз (5.1) ілюструє інваріантність кількісної оцінки властивості $K_i r_i$ відносно перетворень.

Якщо розглядати з позицій інваріантності (5.1) внесок кожної з двох властивостей, що входять в комплексну властивість більш високого рівня ієрархії, то очевидно, що цей внесок у загальному випадку буде різний.

Нерівноцінність вкладу ΔR також інваріантна щодо рівнянь перетворення:

$$\Delta R = K_i r_i - K_{i-1} r_{i-1}.$$

Якщо розглядати більш загальний випадок, то умові безперервності всередині діапазону зміни безрозмірних показників до умови незалежності показників відповідають не всі системи.

У цьому випадку інваріантність не існує, а, отже, застосування адитивної форми узагальненого показника неправомірне.

Якщо узагальнений показник визначається трьома, чотирма і великим числом показників, то складається система з шести, восьми і т.д. рівнянь, рішення якої для будь-якого r_{i0} має вигляд:

$$r_{i0} = 2^{N_k - 1} \sqrt{\prod_{i=1}^{N_k} r_i^{2^p}}$$

де N_k - число безрозмірних показників, що складають узагальнений показник;

p — змінний показник ступеня.

При цьому значення p визначається з квадратичної матриці:

$$\begin{vmatrix} N_k-1 & N_k-2 & N_k-3 & \dots & 0 \\ 0 & N_k-1 & N_k-2 & \dots & 1 \\ 1 & 0 & N_k-1 & \dots & 2 \\ \dots & \dots & \dots & \dots & \dots \\ N_k-2 & N_k-3 & N_k-4 & \dots & N_k-1 \end{vmatrix}$$

Тоді узагальнений показник знайдеться з виразу:

$$R_0' = \frac{R_0}{K} = \frac{1}{N_k}\sum_{i=1}^{N_k} r_{i0} = \frac{1}{N_k}\sum_{i=1}^{N_k} 2^{N_k}\sqrt{\prod_{i=1}^{N_k} r_i^{2^p}} \quad (5.2)$$

де R_0' - узагальнений показник, віднесений до вагомості K_0.

Коефіцієнт $1/N_k$ введено у формулу (5.2) для того, щоб незалежно від числа N_k, значення узагальненого показника було в межах [0,1].

Відмінною рисою цієї моделі є те, що коефіцієнти вагомості не розглядаються як постійні величини. Дійсно, чим важче забезпечити задане значення показника, тим важливіше його роль. Чим ближче показник до свого граничного значення, тим менше його вагомість.

5.4. Оптимізація системи захисту інформації на підприємстві

Комплексний показник інформаційної захищеності заданого рівня будується на основі вибору часткових показників, що оптимізуються.

Приступаючи до вирішення оптимізаційної задачі необхідно, перш за все, вирішити питання, які часткові показники захищеності від потенційних загроз повинні бути поліпшені і як ці зміни в цілому вплинуть на рівень ІБ бізнес-процесів.

Для цього необхідно дослідити функцію багатьох змінних, щоб визначити, як зміна одного з аргументів r_i впливає на функцію і знайти таку властивість, показник якої при зміні його на деяку величину δ дає найбільший приріст функції захищеності ΔR_0.

Поставлена задача відноситься до класу задач оптимізації проектно-конструкторських рішень. Для її рішення зручно використовувати добре відомий метод найшвидшого градієнтного підйому.

При цьому градієнт функції захищеності визначається з виразу

$$grad(R_0) = \left(\frac{\partial R_0}{\partial r_1}, \frac{\partial R_0}{\partial r_2}, ..., \frac{\partial R_0}{\partial r_n} \right).$$

Тоді

$$r_{11} = r_{01} + \delta \left(\frac{\partial R_0}{\partial r_1} \right);$$

$$r_{12} = r_{02} + \delta \left(\frac{\partial R_0}{\partial r_2} \right);$$

$$r_{1n} = r_{0n} + \delta \left(\frac{\partial R_0}{\partial r_n} \right).$$

У загальному випадку для визначення величини δ складається матриця

$$\begin{vmatrix} \frac{\partial^2 R_0}{\partial r_1^2} & \cdots & \frac{\partial^2 R_0}{\partial r_1 \partial r_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial^2 R_0}{\partial r_1 \partial r_n} & \cdots & \frac{\partial^2 R_0}{\partial r_n^2} \end{vmatrix},$$

норма якої визначається виразом:

$$L = \sqrt{\sum_{i,j} \left(\frac{\partial^2 R_0}{\partial r_i \partial r_j} \right)^2}.$$

Величина δ при цьому вибирається відповідно до умови $\delta \le 1/L$. Однак у випадку лінійності функції $R_0(r_1, r_2, ..., r_n)$ очевидно, що

$$\frac{\partial^2 R_0}{\partial r_i \partial r_j} = 0.$$

Тому для знаходження δ доцільно скористатися наступним рівнянням:

$$\left. \frac{\partial R}{\partial \delta} \right|_{\frac{\partial^2 R_0}{\partial \delta^2} = 0} = 0,$$

вирішуючи яке визначається величина δ, що забезпечує відшукання максимуму R_0.

Слід зазначити, що в даному випадку важливе не кінцеве значення комплексного показника (так як воно може бути задане), а динаміка його зміни та послідовність показників, що роблять найбільший вплив на зміну комплексного показника при знаходженні градієнта в кожній точці функції $R_0(r_1, r_2, ..., r_n)$.

Даючи прирости частковим показниками, можна спостерігати картину зростання, а потім зменшення важливості цих показників, послідовність переходу пріоритету важливості від одних властивостей до інших, тобто, досліджуючи градієнт функції комплексного показника, легко моделювати шлях вдосконалення і послідовність поліпшення властивостей модельованої СЗІ.

Математичний алгоритм вибору шляхів оптимізації модельованої інфраструктури захисту інформації на основі дослідження градієнта функції комплексного показника наступний.

1. Відповідно до ієрархії властивостей встановлюється вид функції

$$R_0(r_1, r_2, ..., r_n).$$

2. Задається межа зміни аргументів і крок зміни, загальний для всіх показників:

$$r_{0,i} \le r_i \le r_{i\max},$$

де $r_{0,i}$ - значення *i*-го безрозмірного показника;

$r_{i\max}$ - Найбільше можливе значення і-го безрозмірного показника.

3. Обчислюються значення функцій в точках з координатами

$$R_0(r_{0,1}, r_{0,2}, ..., r_{0,n})$$

$$R_{i\max}(r_{1,\max}, r_{2,\max}, ..., r_{n,\max})$$

4. Визначається n нових значень комплексного показника за умови, що кожному з аргументів дається прирощення δ:

$$R'_{0,1}(r_{0,1} + \delta, r_{0,2}, ..., r_{0,n})$$

$$R'_{0,2}(r_{0,1}, r_{0,2} + \delta, ..., r_{0,n})$$

.....

$$R'_{0,n}(r_{0,1}, r_{0,2}, ..., r_{0,n} + \delta)$$

де $R'_{0,i}$ - значення комплексного показника при зміні *i*-го аргументу на величину δ.

5. Перевіряється умова $r_i + \delta \le r_{i\max}$. Якщо умова не дотримується, то необхідно приймати $r_i + \delta + r_{i\max}$.

6. Знаходяться приріст функції $\Delta R'_{0,i}$ при зміні кожного *i* го показника на величину δ:

$$\Delta R'_{0,1} = R'_{0,1} - R_0$$
$$\Delta R'_{0,2} = R'_{0,2} - R_0$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\Delta R'_{0,n} = R'_{0,n} - R_0$$

7. Прирости функції ранжуються. Кожному r_i ставиться у відповідність прирощення $\Delta R'_{0,i}$.

$$\Delta R'_{0,k_1} \le \Delta R'_{0,k_2} \le \ldots \le \Delta R'_{0,k_n}$$
$$\Delta R'_{0,j} \le \Delta R'_{0,k} \le \ldots \le \Delta R'_{0,m}$$

8. Визначається максимальне прирощення $\max\{\Delta R'_{0,i}\}$.

9. Для всіх $i = 1..n$ обчислення по пунктах 4 - 8 повторюються n раз, до тих пір, поки $R'_{0,i} = R'_{0,i\max}$ при всіх $r_i = r_{i\max}$.

В результаті проведеної таким чином процедури, відбувається оптимізація показників.

Дослідження часткових збільшень функції захищеності і ранжування показників за найбільшим приростом, визначає порядок їх оптимізації, як показано на рис. 5.3.

Розрахунки були виконані за допомогою спеціального програмного засобу, розробленого на базі мови MS Visual C + +. Комплексний показник ІЗІ дозволяє оцінити систему в цілому. Однак при порівнянні різних варіантів ІЗІ на стадіях створення системи є можливість їх порівняння по всій сукупності часткових показників.

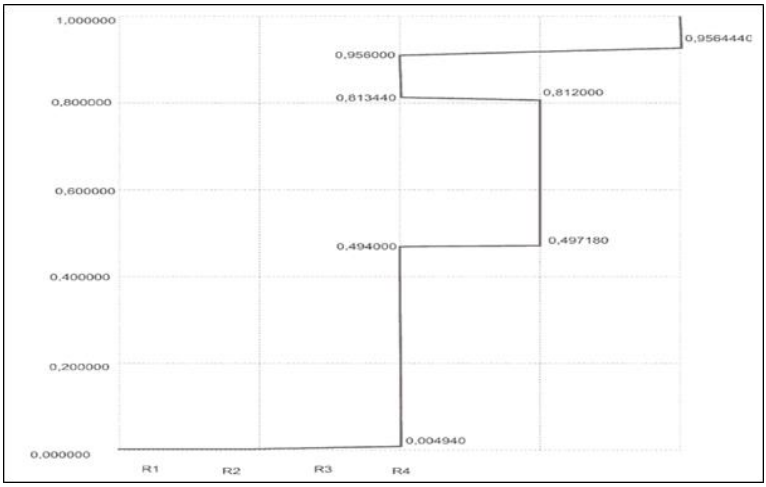


Рис. 5.3. Приклад послідовності оптимізації показників інформаційної захищеності

Алгоритм порівняння варіантів являє собою ряд послідовних етапів, що забезпечують відбір підмножини недомінуємих варіантів і виявлення кращого. Вихідними даними при цьому є матриця:

$$P = \begin{vmatrix} r_{11} & r_{12} & \dots & r_{1m} \\ r_{21} & r_{22} & \dots & r_{2m} \\ \dots & \dots & \dots & \dots \\ r_{n1} & r_{n2} & \dots & r_{nm} \end{vmatrix}$$

де r_{ij} -значення j-го показника *i*-го варіанта;

n - кількість варіантів ІЗІ;

m - кількість часткових показників.

Очевидно, що всі показники повинні бути приведені до відносних значень за формулами:

$$\bar{r}_{ij} = \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}, \quad j = 1,\dots,n,$$

якщо зростання показника підвищує якість ІЗІ

$$\bar{r}_{ij} = 1 - \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}, \quad j = 1,\ldots,n$$

якщо зростання показника знижує якість ІЗІ.

Тоді остаточно вихідна матриця буде мати вигляд:

$$\overline{P} = \begin{vmatrix} \overline{r_{11}} & \overline{r_{12}} & \ldots & \overline{r_{1m}} \\ \overline{r_{21}} & \overline{r_{22}} & \ldots & \overline{r_{2m}} \\ \ldots & \ldots & \ldots & \ldots \\ \overline{r_{n1}} & \overline{r_{n2}} & \ldots & \overline{r_{nm}} \end{vmatrix}$$

Для визначення вагових коефіцієнтів часткових показників в даному випадку доцільно скористатися ентропійними перетвореннями. Рівень ентропії кожного показника визначається по залежності:

$$H_j = \frac{1}{m} \sum_{i=1}^{m} \bar{r}_{ij} \ln(\bar{r}_{ij}), \quad j = 1,\ldots,n$$

Отже, рівень мінливості кожного показника визначиться виразом:

$$d_j = 1 - H_j, \quad j = 1,\ldots,n.$$

Тоді вагу кожного показника можна отримати за формулою:

$$\lambda_j = \frac{d_j}{\sum_{i=1}^{m} d_i}, \quad j = 1,\ldots,n$$

Таким чином, для побудови матриці рішень необхідно кожен стовпець вихідної матриці помножити на відповідний ваговий коефіцієнт. З урахуванням цього матриця рішень буде мати вигляд:

$$\widetilde{P} = \begin{vmatrix} \widetilde{r}_{11} & \widetilde{r}_{12} & \ldots & \widetilde{r}_{1m} \\ \widetilde{r}_{21} & \widetilde{r}_{22} & \ldots & \widetilde{r}_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ \widetilde{r}_{n1} & \widetilde{r}_{n2} & \ldots & \widetilde{r}_{nm} \end{vmatrix}$$

Використовуючи дану матрицю для кожної пари варіантів a_k і a_l $(k = 1,\ldots,m;\ l = 1,\ldots,m)$, обчислюється множина згоди:

$$X_{lk} = \left\{ j \middle| \tilde{x}_{kj} > \tilde{x}_{lj} \right\}.$$

Ця множина складається з індексів тих показників, за якими k-й варіант не гірше, ніж варіант l. Тому безліч незгоди складається з індексів тих показників, за якими l-й варіант перевершує k-й, тобто

$$Y_{lk} = \{1,...,n\} - X_{lk}.$$

Для побудови матриці згоди необхідно знайти індекси згоди. Індекс згоди для кожної пари варіантів обчислюється таким чином:

$$\tilde{X}_{lk} = \frac{\lambda_k X_{lk}}{\sum_{i=1}^{m} \lambda_i}, \quad k, l = 1,..., \text{m}.$$

Індекс згоди відображає важливість (перевагу) варіанта a_k по відношенню до варіанту a_l. Із знайдених індексів згоди утворюється матриця згоди S розмірності $m \times m$.

Якщо матриця згоди визначена на основі величин вагомості часткових показників, то матриця незгоди формується на основі значень показників незгоди. Індекс незгоди розраховується для кожної пари варіантів a_k і a_l за формулою:

$$d_{kl} = \frac{\max\limits_{j \in Y_{kl}} \left| \tilde{r}_{kj} - \tilde{r}_{ij} \right|}{\max\limits_{j=1,...,n} \left| \tilde{r}_{kj} - \tilde{r}_{ij} \right|}$$

З індексів незгоди складається матриця незгоди H розмірності $m \times m$.

Тоді домінуюча матриця згоди буде мати вигляд:

$$\bar{Z} = \left\| \bar{z}_{kl} \right\|,$$

де $z_{kl} = \begin{cases} 1, & якщо\ X_{kl} > \bar{X} \\ 0, & інакше \end{cases}$, $\bar{X} = \frac{\sum\limits_{k=1}^{m} \sum\limits_{l=1}^{m} x_{kl}}{m(m-1)}$.

Елементи матриці *Z* відображають факт домінування одного варіанта над іншим. Домінуюча матриця незгоди будується аналогічно матриці $\bar{Z}$:

$$\bar{Z} = \left| \bar{z}_{kl} \right|,$$

де $\bar{z}_{kl} = \begin{cases} 1, & якщо\, d_{kl} \le \bar{d} \\ 0, & інакше \end{cases}$, $\bar{d} = \dfrac{\sum_{k=1}^{m}\sum_{l=1}^{m} d_{kl}}{m(m-1)}$.

На завершення алгоритму визначається алгебраїчна матриця домінування як добуток домінуючих матриць згоди Z і незгоди $\bar{Z}$, тобто $D_A = Z \times \bar{Z}$. Щоб видалити варіанти, які домінуються іншими варіантами, потрібно вилучити ті, для яких у відповідних їм стовпчиках матриці D_A є хоча б одна одиниця.

З середини 90-х рр.. автоматизація практично всіх бізнес-процесів дозволила добитися революційного зниження, непродуктивних втрат часу на передачу результатів виконання функціональних завдань на інші робочі місця або в інші підрозділи. Стало можливим підтримувати прозорість управлінських регламентів, їх відтворюваність, що, у підсумку, до початку XXI століття дозволило забезпечити проходження стандартам якості ISO 9000 на рівні управління підприємством.

На промисловому підприємстві є локальні інформаційні системи (ІС) різного призначення, що взаємодіють між собою з метою підтримки управлінських рішень на всіх, рівнях компетенції.

Міграція локальних внутрішньофірмових комп'ютерних мереж і ІС з виходами на ІС дочірньої компанії і структурні підрозділи великого підприємства неможлива без використання ресурсів регіональних і глобальних мереж.

У результаті створюються корпоративні ІС (КІС). Подібні ІС надають зацікавленій особі можливості працювати як з корпоративної БД, так і з локальними базами інших структурних підрозділів підприємства.

Інтеграційні проекти завжди унікальні, тому і дорогі (що не завжди виправдано), однак - можна вказати типові проблеми інтеграції: синхронізація, даних, робота складових додатків і реалізація наскрізних бізнес-процесів[1].

Більшість сучасних корпоративних додатків використовують реляційні бази, як основу для збереження і доступу до прикладних і системним даними[21]. Тому часто під інтеграцією розуміють обмін

[1]Kaufman, Arnold, and Gupta, Madan. M. Introduction lo Fuzzy Arithmelic//Thomson Computer Press, 2011.

[2]The OLAP Report: Applications. WebSphere MQ Integrator. Programming Guide.

даними між БД. Метою інтеграції ставиться синхронізація джерел, даних, з якими працюють різні додатки. Синхронізація даних не означає взаємодії прикладних процесів і компонентів, що інтегруються, тому що має місце лише взаємодія компонентів зберігання даних.

Різноманітність цілей і завдань інтегрування корпоративних додатків призвело до великої різноманітності в реалізаціях програмних рішень інтеграції, що мають однотипну функціональність, архітектуру, топологію інтеграції:

Доцільно виділити наступні компоненти-інтегрованої ІС:

– транспортна інфраструктура, що прокладена між додатками;

–-адаптери та конектори, які прив'язують прикладні системи до транспортної інфраструктури;

–-інтеграційний сервер, що бере на себе обробку і виконання обчислювальних процедур і процесів, пов'язаних з інтеграцією.

Транспортна інфраструктура забезпечує надійність передачі даних між додатками і більшу гнучкість для різних сценаріїв взаємодії в порівнянні зі стандартними мережевими службами.

Інтеграційний сервер, шлюз або інтеграційний брокер, використовуваний як центральний блок звернення інтегровних систем та програм перерозподіляє, обробляє і направляє потоки інформації.

Централізоване виконання функцій обробки переданої інформації і даних також означає використання загального репозиторію для корпоративних інтеграційних бізнес-правил.

Правила із загального репозитора доступні для огляду і прозорі для розробників і системних адмі-ністраторов, можуть доповнюватися і коректуватися при зміні бізнес-процесів і складу обчислювальної середовища, що дозволяє ефективно сполучати і динамічно управляти інтегрованим рішенням.

Конструювання бізнес-системи неможливо без інформаційної інфраструктури, важливою складовою якої є захист інформаційних активів у складі активів підприємства.

Під *інформаційною інфраструктурою* слід розуміти не тільки сукупність програмно-технічних засобів та організаційно-адміністративних заходів, що забезпечують безпечну обробку даних і інформаційне забезпечення бізнес-процесів усередині підприємства,

---

[1]Threats to Computer Systems: an Overview - Computer Systems Laboratory Bulletin, March, 2009

адекватні можливості з обміну інформацією з зовнішніми організаціями, але й інформаційні системи та мережі, науково-технічне забезпечення, технічні бібліотеки і саму оброблювану інформацію.

Підтримка і захист системи управління підприємством передбачає насамперед підтримку та захист самих бізнес-процесів і розвиток інфраструктурної складової бізнес-системи і, зокрема, інформаційної, за рахунок подолання інфраструктурної та інформаційної роз'єднаності підрозділів підприємства.

Інвестиції в управління бізнес-процесами можуть приносити значні доходи за рахунок підвищення ефективності роботи і прискорення бізнес-процесів, а також за рахунок підвищення ринкової вартості компанії в частині її нематеріальних активів: інформаційних в інфраструктурної складової нематеріальних активів.

Узагальнення результатів досліджень дозволило виділити основні перспективні напрями процесного підходу, що послугувало базисом для формування нової методології оцінки і оптимізації ІЗІ бізнес-процесів.

Необхідність створення оптимальної інфраструктури сучасних промислових підприємств обумовлена жорсткими вимогами ринкової конкуренції, які змушують компанії оцінювати і впроваджувати нові методики оптимізації як основний бізнес-діяльності підприємства; так і в області ІТ та інтелектуальної власності.

Особливе значення при цьому має інформаційна інфраструктура промислових підприємств, так як помилки, допущені при її формуванні, і невміння підлаштовуватися під нові правила, які диктуються ринком, можуть спричинити значні фінансові втрати.

Поняття *інформаційних активів* слід використовувати в широкому сенсі, включивши в нього все технічне і програмне забезпечення, патенти, торгові марки і все те, що дозволяє працівникам підприємства реалізувати свій виробничий потенціал, а також відносини, що склалися між компанією і її великими клієнтами, державними структурами, іншими господарськими об'єктами.

На основі оцінки впливу зростаючих можливостей нових ІТ на підтримку та захист бізнес-процесів, стану існуючої організації ІБ, реалізації вимог до ІЗІ і вимог стандартів ІБ в сучасних бізнес-системах сформульована наукова проблема, що вирішується в (рис. 5.4).

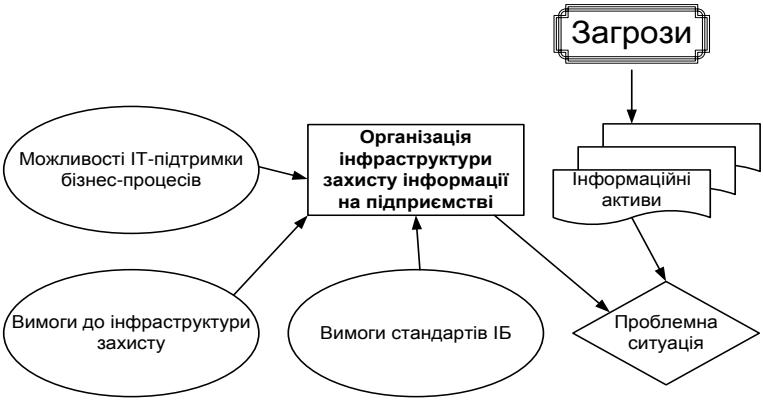


Рис. 5.4. Ідентифікація проблеми вдосконалення інфраструктури захисту інформації на підприємстві

Наукова проблема полягає у розробці методології організації ІЗІ на промисловому підприємстві як цілісної системи концептуальних положень, методів, моделей, алгоритмів і практичних рекомендацій, що забезпечують процес створення та супроводу системи захисту.

Рішення сформульованої проблеми дозволить обґрунтовано підходити до організації ІЗІ бізнес-процесів на промисловому підприємстві, а також здійснювати синтез систем захисту інформації (СЗІ).

РОЗДІЛ 6
РОЗРОБКА ІМІТАЦІЙНОЇ МОДЕЛІ ДЛЯ КОМПЛЕКСНОЇ ОЦІНКИ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ В УМОВАХ РЕЙДЕРДЕРСЬКИХ ЗАГРОЗ

6.1. Оптимізація та оцінка витрат на створення інфраструктури захисту інформації на підприємстві

З метою постановки задачі оптимізації сформулюємо наступні математичні моделі.

Модель мінімізації витрат на інфраструктуру захисту інформації (ІЗІ). Дана модель може бути представлена у вигляді задачі цілочисельного програмування з булевими (двійковими) змінними.

Нехай $x_{ij} = 1$, якщо *i*-ий, засіб захисту інформації (ЗІ) розробник вибирає для захисту j-го інформаційного активу, і $x_{ij} = 0$ - в іншому випадку (при цьому допускається, що *i*-ий засіб використовується для захисту від *i*-ої загрози). Потрібно мінімізувати витрати:

$$S = \sum_{i \in I} \sum_{j \in J} S_{ij} x_{ij} + \sum_{i \in I} S_i y_i \to \min \quad (6.1)$$

при дотриманні ряду обмежень:

$$\sum_{i \in I} \sum_{j \in J} a_j r_{ij} x_{ij} \geq R_{доп}, \quad \sum_{i \in I} x_{ij} = 1, \quad \forall j \in J \quad (6.2)$$

$$y_i = \begin{cases} 1, & якщо \sum_{j \in J} x_{ij} > 0 \\ 0, & інакше \end{cases} \quad (6.3)$$

$$x_{ij} \in \{0;1\} \quad (6.4)$$

У моделі (6.1) - (6.4) прийняті наступні позначення:

S_{ij} - витрати на захист j-го інформаційного активу i-м засобом;

S_i - витрати, загальні для всіх інформаційних активів, на захист i-м засобом;

I - множина засобів захисту інформації;

J - множина інформаційних активів, що захищається;

r_{ij} - оцінка якості захисту i-м засобом j-го інформаційного активу;

a_j - ваговий коефіцієнт j-го інформаційного активу в загальній оцінці ІЗІ, $\sum_{j \in J} a_j = 1$;

$R_{доп}$ - допустимий рівень якості ІЗІ в цілому;

y_i - двійкова змінна, що приймає значення "1", якщо *i*-ий засіб ЗІ може бути використане в ІЗІ, і "0" - в іншому випадку, причому *i*-ий засіб захисту в системі може бути використано лише один раз.

Обмеження (6.3) забезпечує обов'язковість захисту j-го інформаційного активу.

Модель максимізації рівня захищеності інформаційних активів.

Дана модель описує двоїсту задачу по відношенню до раніше розглянутої вихідної задачі. У цьому випадку обмеження на рівень якості ЗІ стає критерієм, а критерій вихідної задачі - обмеженням.

$$R = \sum_{i \in I} \sum_{j \in J} a_j r_{ij} x_{ij} \to \max$$

Таким чином, в даній моделі потрібно максимізувати рівень якості системи захисту інформації (СЗІ) при дотриманні наступних обмежень:

$$S = \sum_{i \in I} \sum_{j \in J} S_{ij} x_{ij} + \sum_{i \in I} S_i y_i \le S_{доп}, \quad \sum_{i \in I} x_{ij} = 1, \quad \forall j \in J$$

$$y_i = \begin{cases} 1, & якщо \sum_{j \in J} x_{ij} > 0 \\ 0, & інакше, \quad x_{ij} \in \{0;1\} \end{cases}$$

де $S_{доп}$ - допустима вартість системи захисту інформації.

Вибір оптимальної СЗІ повинен ґрунтуватися тільки на множині недомінірованних варіантів. Іншими словами, збільшення витрат на захист інформації має супроводжуватися підвищенням якості захисту.

Доцільно спільне використання пропонованих моделей. Так, при обмеженні на допустимі витрати на захист може бути знайдено максимальне значення якості ІЗІ. Проте в деяких випадках ця задача може мати не одне, а кілька рішень (профілів захисту). Для вибору того рішення, з числа знайдених рішень, яке вимагає мінімальних витрат на захист слід вирішити другу задачу. У ній в якості обмеження повинне бути присутнім знайдене в першій задачі значення якості ІЗІ.

У концептуальної моделі ІЗІ передбачено, що поряд з реалізацією основних функцій захисту, що визначаються типовими вимогами, система повинна мати властивості, що забезпечують захист від основних погроз. Отже, система показників ІБ повинна базуватися на оцінці властивостей системи захисту, показаних на рис. 6.1.

При цьому система показників повинна забезпечувати оцінку як по часним властивостям, так і комплексну оцінку ІБ в цілому, що показано на рис. 6.2.

Аналіз інформаційної інфраструктури бізнес-процесів, умов їх реалізації, а також ймовірних загроз дозволив сформувати систему показників ІБ бізнес-процесів, представлену на рис. 6.3.

Для обліку специфіки українських компаній оцінку вартості інформаційних активів доцільно проводити витратним методом.

Поряд з кількісною оцінкою захищеності бізнес-процесів необхідно враховувати цінність інформаційних ресурсів бізнес-процесів.

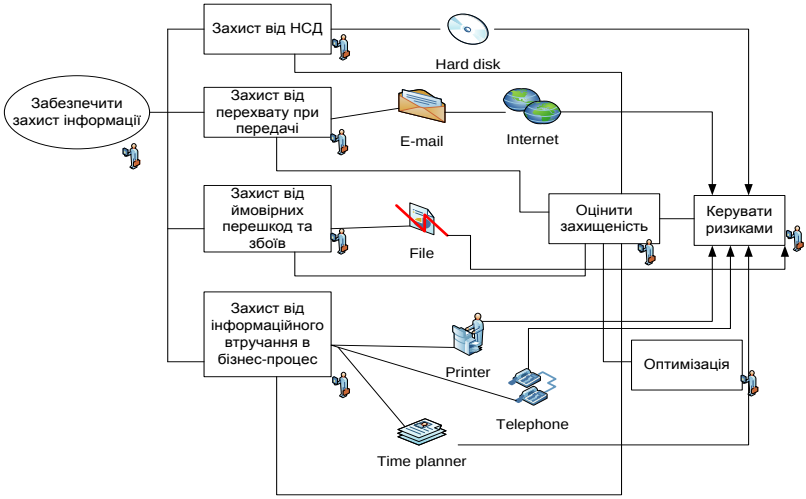


Рис. 6.1. Взаємозв'язок компонент інфраструктури захисту Інформації бізнес-процесів

Оцінка інфраструктурної частини промислового підприємства повинна бути складовою частиною оцінки бізнесу в цілому. При цьому зазвичай виділяють одноразові поточні витрати.

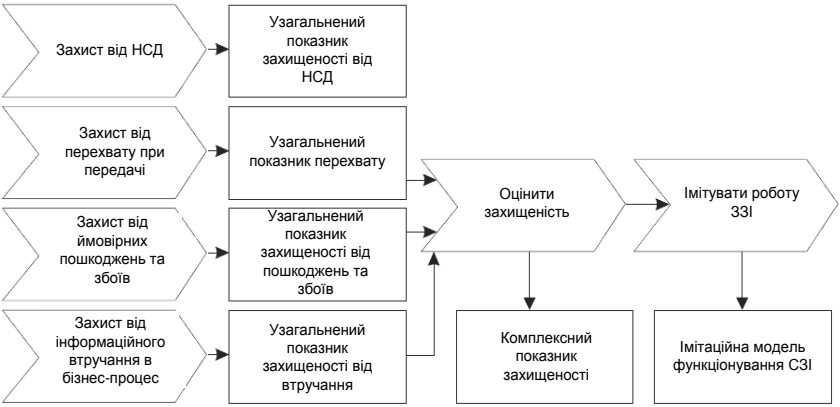


Рис. 6.2. Взаємозв'язок узагальнених показників захисту інформації та комплексного показника інформаційної захищеності бізнес-процесів

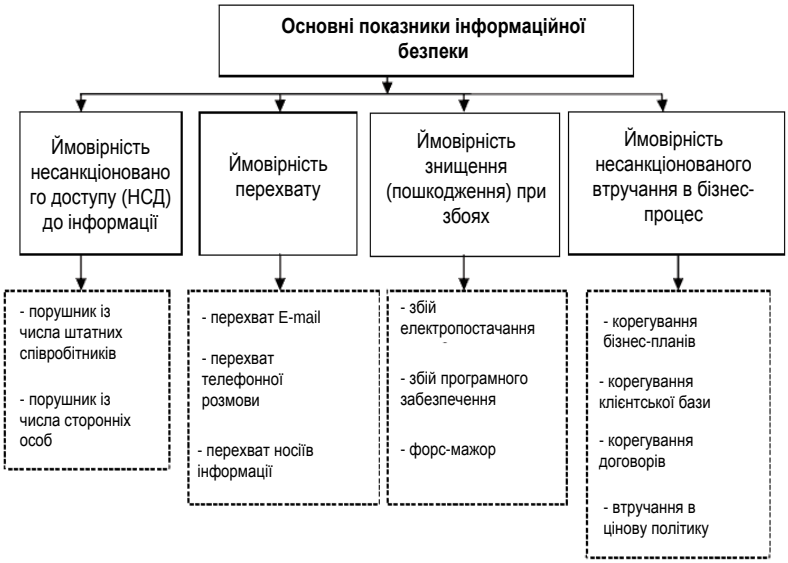


Рис. 6.3. Основні показники інформаційної безпеки

До одноразових відносяться витрати на формування політики безпеки підприємства: організаційні витрати та витрати на придбання

та встановлення засобів захисту. Неминучі витрати - це ті, які необхідні навіть якщо рівень загроз безпеки достатньо низький.

Це витрати на підтримку досягнутого рівня захищеності інформаційного середовища підприємства. Загальні витрати на безпеку складаються з витрат на попереджувальні заходи, витрат на контроль і заповнення втрат (зовнішніх і внутрішніх). Зі зміною рівня захищеності інформаційного середовища змінюються величини складових загальних витрат і, відповідно, їх сума - загальні витрати на безпеку. У ряді випадків не включаються одноразові витрати на формування політики ІБ підприємства, якщо така політика вже вироблена.

При оцінці витрат на систему безпеки на будь-якому підприємстві необхідно враховувати процентне співвідношення загальних витрат на безпеку і загального обсягу продажів.

Основним показником економічної ефективності витрат на ІЗІ промислового підприємства, як будь-якого інвестиційного проекту, є чиста приведена вартість (*NVP*) в заданий період часу *T*:

$$NVP = \sum_{t=1}^{T} \frac{\Delta if_t(R) - \Delta of_t(R)}{(1+E)^t} - K_R$$

де $\Delta if_t(R)$ - зміна вхідного грошового потоку в t -й підперіоди з урахуванням проведення заходів щодо захисту інформації;

$\Delta of_t(R)$ - зміна вихідної грошового потоку з урахуванням проведення заходів щодо захисту інформації;

K_R - необоротні та оборотні інформаційні активи ІЗІ;

E - річна норма прибутку на капітал.

Організація ІЗІ на підприємстві впливає на результати його господарської діяльності і повинна відповідати наступним граничним умовам (табл. 6.1).

Таблиця 6.1.

Граничні умови ефективності витрат на ІЗІ

Основні показники господарської діяльності підприємства	Граничні умови
Прибуток річний	$\Delta П(R) \geq C_R + K_R$

Продовження Таблиці 6.1.

Основні показники господарської діяльності підприємства	Граничні умови
Вартість підприємства (дохідний підхід)	$\sum_{t=1}^{T} \frac{if_t + \Delta if_t(R) - \Delta of_t(R)}{(1+E)^t} + \frac{PV_T + \Delta PV_T(R)}{(1+E)^T} \geq \sum_{t=1}^{T} \frac{if_t - of_t}{(1+E)^t} + \frac{PV_T}{(1+E)^T}$
Рентабельність	$\frac{П + \Delta П(R) - C_R}{Ф_{пр} + K_R} \geq \frac{П}{Ф_{пр}}$

де $\Delta П(R)$ - річний приріст прибутку в результаті заходів щодо ЗІ;

$П(R)$ -прибуток за умови проведення заходів з ЗІ за рік;

$П$ - прибуток в умовах відсутності ЗІ (базовий варіант) за рік;

C_R - річні експлуатаційні витрати на ЗІ;

$Ф_{пр}$ - вартість виробничих фондів;

PV_T - прогнозна вартість у T-ий рік (базовий варіант) в умовах відсутності заходів з ЗІ;

$\Delta PV_T(R)$ - прогнозна вартість з урахуванням проведення заходів з ЗІ;

if_t - вхідний грошовий потік;

of_t - вихідний грошовий потік;

Δif_t - Зміна вхідного грошового потоку в t -ий рік з урахуванням проведення заходів з ЗІ;

Δof_t - Зміна вихідної грошового потоку в t -ий рік з урахуванням проведення заходів з ЗІ.

6.2. Основні властивості та структура імітаційної моделі

Для комплексної оцінки пропонованих заходів і засобів захисту інформації бізнес-процесів розроблено імітаційну модель. Дана мо-

дель реалізує імітацію атак на інформаційну інфраструктуру бізнес-процесів відповідно до загальної концептуальної моделі. У той же час зазначена модель є структурним елементом схеми взаємозв'язків показників захищеності, як показано на рис. 6.4.

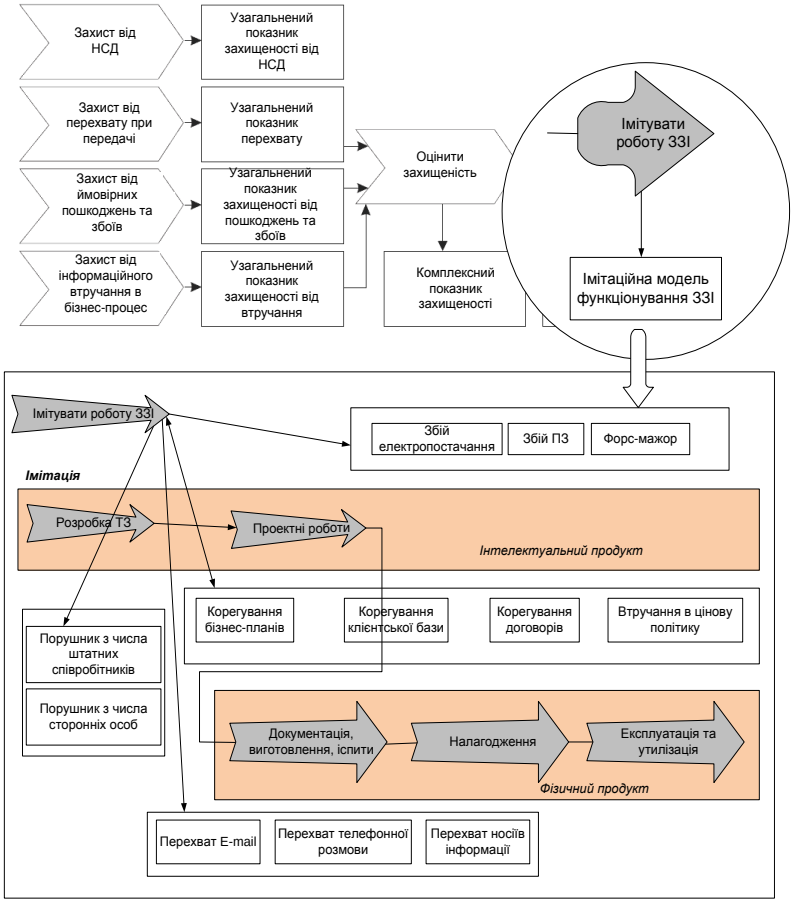


Рис. 6.4. Схема імітації функціонування інфраструктури захисту інформації бізнес-процесів

Спроби можливих атак імітуються у вигляді транзактів, що дискретно надходять, метою яких є захоплення деякого інформаційного

ресурсу. Такими ресурсами можуть бути бухгалтерські, комерційні, фінансові елементи інформації, документи планування, а також інформація, що циркулює в мережі організації.

Сукупність вступників транзактів створює вхідні потоки спроб атак на об'єкти захисту. При цьому істотними властивостями потоків є:

– тип джерела атаки;

– час надходження транзактів-атак, що підкоряється заданим законом розподілу;

– максимально можливе число атак;

– час надходження першого транзакта-атаки;

– число транзактів-атак, що одночасно надходять.

Основні обмеження і допущення, прийняті в моделі:

– передбачається, що можливі всі описані в концептуальної моделі типи загроз (несанкціонований доступ до інформації (НСД), перехоплення інформації при її передачі (отриманні), знищення (пошкодження) інформації в результаті різних видів збоїв в інформаційній інфраструктури, несанкціоноване втручання в бізнес -процес);

– кожна атака може мати на меті будь-який інформаційний ресурс чи комбінацію;

– потоки транзактів-атак є пуасонівськими з відомими законами розподілу часу між двома транзактами потоку;

– час захоплення інформаційного ресурсу є випадковою величиною з відомим законом розподілу;

– величина можливого збитку у разі доступу на певний час до конкретного інформаційного ресурсу є константою.

Імітаційна модель реалізована в системі Arena 8.0 Professional і структурно складається з блоку імітації суб'єктів захисту, що імітує навантаження атак, блоку імітації заходів і засобів захисту, що імітує функціонування цих засобів і блоку імітації об'єктів захисту, що імітує доступ до інформаційних ресурсів у разі подолання заходів і засобів захисту.

При цьому блок імітації заходів і засобів захисту реалізований у вигляді наступних модулів:

– захисту від НСД до інформації;

– захисту від перехоплення інформації;

– захисту від збоїв;

– захисту від втручання в бізнес-процес.

Модуль захисту від НСД до інформації.

Реалізує імітацію дій порушників різних категорій, а також функціонування засобів захисту інформації від несанкціонованого доступу. Виходом модуля є потік вдалих спроб НСД, який направляється до інформаційних ресурсів бізнес-процесу.

Основу *імітації захисту від перехоплення інформації* становить моделювання різного виду трафіків в мережі підприємства.

Вхідний потік задається генераторами заявок. Генератор, починаючи з заданого моменту часу, виробляє 10 кадрів,які надходять в чергу з певним інтервалом. Кадри, які видаються цим генератором, мають найвищий пріоритет.

Надалі імітують процес профілювання трафіку, що входить до комутатору. Кадри, що надходять в чергу обробляються в порядку абсолютного пріоритету із затримкою при обробці, рівної одиниці часу. Селектор спрямовує кадри, що надходять на нього, на виходи у відповідності зі значеннями ASCII кодів логічних імен вихідних дуг.

Кадри від генератора надходять на схему обробки високопріоритетних кадрів, які обслуговуються відповідно з дисципліною FIFO.

Кадри, породжені генераторами, надходять на входи-схеми зважених черг. Кожна зважена черга складається з блоку-черги, регулятора часу і селектора.

Зважені черги можуть функціонувати тільки тоді, коли в черзі відсутні пріоритетні кадри.

Обробка кадрів у зваженій черзі організована з використанням того ж самого ресурсу, що і для пріорітетних кадрів. Однак заняття цього ресурсу конкретним кадром визначається станом зважених черг: першим на обробку надійде кадр з найбільшою черги.

Таким чином відбувається диференціація інформації, що надходить в мережу (голос, рисунок, текст), яка враховується при визначенні ймовірності перехоплення. Вдала спроба перехоплення "йде" далі в інформаційну інфраструктуру бізнес-процесу.

Модуль захисту від збоїв оцінює можливість проходження транзакта-збою в блок об'єктів захисту. При цьому враховуються можливості відновлювальних резервів ІМ з урахуванням ймовірності виникнення того чи іншого типу збою. У разі проходження збою все доступніші інформаційні ресурси "захоплюються" транзактом-збоєм на час, необхідний для відновлення працездатності системи.

Модуль відстежує ігрову ситуацію, при якій гравець-зловмисник намагається перевищити свої повноваження (своєї ролі) у бізнес-процесі шляхом доступу до відповідних інформаційних ресурсів. При цьому інший гравець, що ототожнюється з відповідними організаційними заходами захисту, в плановому порядку контролює нормальний хід процесу.

Транзакти-атаки, що пройшли до об'єктів захисту "захоплюють" відповідні інформаційні ресурси на час, необхідний для здійснення відповідних дій з цими ресурсами. Це водночас є аргументом функції обчислення ризику, який може бути нанесений при вдалому здійсненні атаки. Таким чином, сумарний (сукупний) ризик обчислюється як сума часткових ризиків за всіма атакованими інформаційними ресурсами.

6.3. Синтез інфраструктури захисту інформації промислового підприємства

Як показує досвід практичної роботи, для ефективного захисту автоматизованої системи (АС) підприємства, необхідно вирішити ряд організаційних завдань:

– створити спеціальний підрозділ, що забезпечує розробку правил експлуатації АС, визначальне повноваження користувачів по доступу до ресурсів цієї системи, яка здійснює адміністративну підтримку технічних засобів захисту інформації (правильну настройку, контроль і оперативне реагування на сигнали про порушення встановлених правил доступу,що надходять, аналіз журналів реєстрації подію безпеки і т п.);

– розробити технологію забезпечення інформаційної безпеки, що передбачає порядок взаємодії підрозділів організації з питань забезпечення безпеки при експлуатації АС і модернізації її програмних і апаратних засобів;

– впровадити дану технологію шляхом розробки і затвердження необхідних нормативно-методичних та організаційно-розпорядчих документів (концепцій, положень, інструкцій і т. п,).

Застосування додаткових засобів захисту інформації зачіпає інтереси багатьох структурних підрозділів організації. Не стільки навіть тих, в яких працюють кінцеві користувачі АС, скільки підрозділів, відповідальних за розробку, впровадження і супровід прикладних за-

дач, за обслуговування та експлуатацію засобів обчислювальної техніки. Тому розроблювана технологія забезпечення інформаційної безпеки повинна забезпечувати:

– диференційований підхід до захисту різних автоматизованих робочих місць (АРМ) і підсистем (рівень захищеності повинен визначатися з позицій розумної достатності з урахуванням важливості оброблюваної інформації і розв'язуваних задач);

– уніфікацію варіантів застосування засобів захисту інформації на АРМ з однаковими вимогами до захисту;

– реалізацію дозвільної системи доступу до ресурсів АС;

– мінімізацію, формалізацію (в ідеалі автоматизацію), реальну виконуваність рутинних операцій і узгодженість дій різних підрозділів з реалізації вимог розроблених положень та інструкцій, не створюючи великих незручностей при вирішенні співробітниками своїх основних задач;

– облік динаміки розвитку АС, регламентацію не тільки стаціонарного процесу експлуатації захищених підсистем, але і процесів їх модернізації, пов'язаних з численними змінами апаратно-програмної конфігурації АРМ;

– мінімізацію необхідного числа фахівців відділу захисту інформації.

Для впровадження технології забезпечення інформаційної безпеки корпоративних бізнес-процесів необхідно розробити:

– Концепцію забезпечення інформаційної безпеки. Даний документ визначає загальну систему поглядів в організації на проблему захисту інформації в АС і шляхи вирішення цієї проблеми з урахуванням накопиченого досвіду і сучасних тенденцій її розвитку.

– Положення про категоруванні. Даний документ визначає порядок категорування ресурсів і вимоги, що захищаються, щодо захисту ресурсів різних категорій.

– План захисту АС. Даний документ визначає комплекс конкретних організаційно-технічних заходів щодо захисту інформації, а також незаконного втручання в процес функціонування конкретної АС. План захисту включає опис технології обробки даних в підсистемі, що захищається, аналіз загроз та оцінку ризику нанесення збитку, правила експлуатації системи, необхідний набір інструкцій посадовим особам (інструкція користувачеві АС, інструкція адміністратору безпеки АС і т.д.), визначає порядок взаємодії підрозділів та посадових осіб при

внесенні змін до списків користувачів і програмно-апаратну конфігурацію АРМ, а також визначає розподіл обов'язків і порядок складання, ведення та використання формулярів ресурсів. що захищаються (інформації, АРМ, задач і програмних засобів) в процесі розвитку АС.

Для вирішення зазначених задач необхідно визначити інформаційну інфраструктуру захисту, тобто здійснити синтез даної системи, ґрунтуючись на загальній інфраструктурі бізнес-процесів.

У результаті аналізу діяльності підприємства були виявлені шість базових технологій роботи і чотири загальних, а також виділено чотири перспективних технології роботи.

Загальні технології - це функціональні модулі, що описують закінчений процес, який повторюється не менше ніж у двох базових технологіях і існує тільки спільно з ними.

Загальні технології, що є невід'ємними частинами базових, включають: консультування; розмитнення/замитнення товарів; рекламу і маркетинг; сертифікацію.

Базові технології роботи включають не менше однієї загальної технології.

Технології роботи визначаються характером діяльності підприємства і існують незалежно від її організаційно-штатної структури. Кожна технологія роботи складається з функцій, що виконуються послідовно і паралельно, які можуть різним чином конфігуруватися під конкретного виконавця і будь-яка посадова особа за допомогою механізму повноважень. Повноваження регулюють доступ користувачів до прикладних задач, до інформації БД і до узагальнених даних, які характеризують стан процесів діяльності підприємства.

Прикладна задача являє собою програмний модуль, що підтримує якийсь логічно закінчений процес, спрямований на облік даних і полегшення виконання користувачами їх обов'язків в рамках технології роботи.

Будь-яка технологія роботи підприємства включає кілька прикладних задач, логічно ув'язаних між собою шляхом використання в кожній наступній прикладній задачі результатів задач попередніх, що зберігаються в корпоративній базі даних.

Як приклад наведемо прикладні задачі по базовій технології постачання устаткування. До них відносяться:

– облік клієнтів підприємства (підтримання довідника клієнтів в актуальному стані);

– облік обладнання і його специфікації (підтримання довідника обладнання в актуальному стані);

– підготовка прайс-листів на обладнання;

– облік заявок на закупівлю обладнання;

– підготовка комерційних пропозицій;

– підтримка процесу узгодження з клієнтом предмета угоди;

– формування, облік і контроль виконання бізнес-плану на поставку обладнання;

– формування, облік і контроль схеми оплати за обладнання;

– формування схеми лінії (перелік необхідного обладнання);

– формування, облік і контроль станів договорів (додатків) на поставку, виробництво, сертифікацію, доставку та страхування обладнання;

– забезпечення розрахунків з клієнтами підприємства;

– облік інформації та документів по етапах поставки обладнання (замовлення устаткування, виробництво, сертифікація, страхування, доставка, монтаж, наладка, здача в експлуатацію та навчання персоналу замовника випуску на ньому продукції);

– облік платежів клієнтів компанії;

– підтримка процесу гарантійного обслуговування;

– підготовка матеріалів, що підтримують процес навчання;

– підтримка документообігу між АРМ посадових осіб.

Інформаційна система підприємства являє собою розгалужену мережу, що об'єднує локальні та віддалені робочі місця користувачів. Основними елементами ІС є:

– локальна обчислювальна мережа (ЛОМ) центрального офісу підприємства;

–локальна обчислювальна система (ЛОС) філії;

– інтегрована база даних.

ЛОС Центрального офісу підприємства і філії реалізується на основі архітектури "клієнт-сервер", що об'єднує автоматизовані робочі місця співробітників служб і підрозділів.

Групи АРМ виділяються за функціональною ознакою, з урахуванням виконання виділених базових, загальних і перспективних бізнес-процесів, перспективної організаційної структури підприємства, і орієнтуються на дерево функцій перспективної діяльності підприємства.

У процесі виконаного об'єднання потоків вхідних і вихідних документів сформовано чотири типові групи документів:

– договірні документи;

– первинні бухгалтерські документи;

– документи підтримки бізнес-процесів;

– звітні документи.

Кожна група документів залежно від технології роботи характеризується унікальним, властивим тільки їй, переліком документів. Наприклад, для технології поставки обладнання вхідними та вихідними документами будуть наступні:

– договірні документи;

– первинні бухгалтерські документи;

– документи підтримки бізнес-процесів.

Процедури документообігу призначені для автоматизації процесів розробки, узгодження і виконань документів між службами та посадовими особами підприємства. Кожна процедура документообігу визначає схему взаємодії АРМ по кожній групі вхідних і вихідних документів, а також етапність і спрямованість дій виконавців та посадових осіб.

6.4. Система моніторингу та шляхи вдосконалення інфраструктури захисту інформації

Моніторинг інфраструктури захисту інформації бізнес-процесів являє собою комплекс заходів і заходів (організаційних, технічних і правових), спрямованих на проведення спостережень, оцінки і прогнозу змін в інформаційній інфраструктурі та її компонентах.

Необхідність використання моніторингу визначається тим, що стандартні засоби і механізми захисту інформації недостатні, оскільки зазвичай забезпечують тільки базові функції, не дозволяючи контролювати їх виконання і працездатність інформаційної системи в цілому. Так, практично у всіх інформаційних системах, як мінімум, необхідно відстежувати спроби реєстрації в системі, помилки в програмному забезпеченні (ПЗ), факти доступу до ресурсів, нештатні ситуації, зниження рівня захищеності та багато іншого.

Моніторинг призначений для виконання функцій контролю функціонування інформаційних систем, систем передачі даних, засобів і механізмів захисту. Ефективність моніторингу залежить від правильної його організації. Попереднє вивчення, оперативний контроль, ана-

ліз та забезпечення механізмів реагування дозволяє не тільки виявити факт комп'ютерної атаки або порушення працездатності, а й сформувати комплекс заходів та заходів з попередження, локалізації та усунення наслідків.

Основним завданням системи моніторингу є контроль правильної реалізації політики безпеки, а також формування параметрів і оцінка стану інформаційної безпеки бізнес-процесів.

Поняття моніторинг включає в себе такі базові принципи:

– спостереження за факторами впливу і станом інформаційних систем; оцінку фактичного стану інформаційної системи (ІС); прогноз стану ІС та оцінку прогнозованого стану; забезпечення реагування.

Система моніторингу включає в себе наступний комплекс заходів: вибір технічних засобів і методів аналізу; методи збору, реєстрації та протоколювання; протоколювання; аналіз; реагування; подання та поширення інформації.

Для забезпечення моніторингу використовуються як технічні (технологічні), так і організаційні і правові методи. До технічних методів належать: аналіз захищеності; виявлення несанкціонованої активності; контроль інформаційних потоків; протоколювання та реєстрація.

Організаційні заходи щодо забезпечення моніторингу безпеки включають:

– створення та експлуатацію системи забезпечення реагування та відновлення, що забезпечує обмеження масштабів збитку інформаційної інфраструктурі на об'єктах підвищеного ризику (потенційно-небезпечних об'єктах) і життєзабезпечення населення;

–створення та експлуатацію системи обміну інформацією про факти та методи, комп'ютерних нападів і несанкціонованих вторгнень в СЗІ;

– розробку вимог (профілів) з безпеки інформації, що враховують особливості функціонування інформаційних систем на об'єктах;

– розробку програми співробітництва з міжнародними профільними Центрами (CIAC, CERT, FIRST та інші) в частині обміну інформацією про факти та методи комп'ютерних нападів і несанкціонованих вторгнень в СЗІ.

При цьому має бути забезпечено взаємодію між експертами, що працюють в області інформаційної безпеки, організована підготовка та атестація фахівців, розроблено комплекс методичного забезпечення.

Координуючу роль при організації системи моніторингу повинні виконувати Центри компетенції, спеціалізовані структури, організовані в єдину систему.

В Україні на проблеми забезпечення моніторингу інформаційної безпеки почали звертати увагу тільки останнім часом, однак за кордоном вже накопичено певний досвід. При цьому роботи в даному напрямку ведуться як громадськими, так і державними організаціями (напр. Computer Incident Advisory Capability, U. S, Department of Energy (CIAC), Forum of Incident Response and Security Team (FIRST), Computer Emergency Response Team (CERT) Coordination Center), так і комерційними.

В якості основних вимог до систем, що забезпечує моніторинг інформаційної безпеки можуть бути висунуті наступні:

– повнота виявлення атак;

– висока продуктивність і масштабованість;

– мінімум помилкових тривог;

– вміння пояснювати причину тривоги;

– інтеграції з системою управління та іншими сервісами безпеки;

– наявність технічної можливості віддаленого моніторингу інформаційної системи.

Повнота виявлення атак являє собою очевидну вимогу. Не настільки очевидна вимога високої продуктивності обумовлено бажанням і необхідністю забезпечити умови; при яких система моніторингу сама не породжувала б відмову в обслуговуванні при зростанні потоку подій безпеки, викликаний, в тому числі, і збільшенням об'єму (масштабованість) контрольованих програмно-апаратних засобів. Висока продуктивність комп'ютерів і пропускна здатність сучасних каналів зв'язку навіть при досить малої інтенсивності помилкових тривог, наприклад 10^{-7}, призводити до того, що адміністратор безпеки повинен реагувати на десятки атак в годину. Власне ці умови породжують вимогу необхідності пояснення причини атаки, як засобу, що допомагає адміністратору відрізнити помилкову тривогу від реальної атаки. При реалізації функцій управління і сервісів безпеки необхідно уникнути дублювання зібраних даних та вироблених над ними попередні операцій обробки, наприклад, очищення даних, обчислення середніх значень, що вимагає інтеграції цих компонентів. Нарешті, організація

відмовостійкості та віддаленого управління системою моніторингу обумовлюють останнє з перерахованих вище вимог.

У системах моніторингу інформаційної безпеки використовуються дві основні стратегії (напрямки) збору даних:

– збір даних про поведінку апаратно-програмних засобів;

– збір даних про поведінку додатків і користувачів.

У разі використання першої стратегії збираються дані, що виробляються компонентами СЗІ, такі як значення полів переданих пакетів, кількість пакетів різних протоколів, послідовності системних викликів, інтенсивності звернень до системних викликів, поля записів у базах даних, поля в прийнятих пакетах, вектори переривань і так далі . При цьому з пакетів може виділятися вміст різних мережевих рівнів, вироблятися дефрагментація пакетів для отримання можливості аналізу їх повного вмісту та виконуватися реконструкція потоків пакетів для отримання можливості обліку інформації про розвиток атаки.

При використанні другої стратегії збираються дані, що представляють собою послідовності команд, які видаються кожним користувачем або додатком, інтенсивності видачі команд і звернень до зовнішніх пристроїв для різних часових інтервалів, а також інші дані, що характеризують поведінку користувача або програми.

До зібраних даних пред'являються такі основні вимоги:

– повнота, як забезпечення збору всіх значень необхідних даних, наприклад, всіх системних викликів без пропусків, що виникають через недосконалість застосованого методу і особливостей операційної системи;

– достовірність, як забезпечення неспотвореності даних, наприклад, за відмов устаткування і дій зловмисників;

– своєчасність, як можливість отримання доступу до даних в реальному часі з метою вироблення адекватної реакції у відповідь.

Опис за допомогою адекватної математичної моделі поведінки одного з параметрів системи, групи параметрів або всієї системи в цілому дозволяє аналітично або за допомогою чисельного моделювання дати відповіді на питання про реальні терміни експлуатації системи, ефективності налаштування її параметрів, надійності, захищеності та ряду інших характеристик.

Цифрові телекомунікаційні системи та розподілені обчислювальні комплекси на відміну від технічних засобів попередніх поколінь за своєю архітектурою і принципам, функціонування можуть відносно

невеликими додатковими витратами надавати дослідникам гігантські обсяги інформації про процеси, що відбуваються в них. Вже на перших етапах вивчення цієї інформації фахівці стали звертати увагу на те, що одержувані ними дані за своєю природою помітно відрізняються від тих, з якими вони стикалися раніше при передачі сигналів, в теорії масового обслуговування, електротехніки та інших практично значущих напрямках. Роботи з цієї тематики стали з'являтися у пресі з початку 90-х років минулого століття. До основних особливостей даних, які зазвичай відзначаються в даній предметній області належать:

– стохастичность більшості досліджуваних характеристик, обумовлена самими принципами роботи систем, а не перешкодами і помилками вимірювань;

– відсутність стаціонарності багатьох процесів як в «широкому сенсі» слова (змінюється середнє значення і коваріаційна функція), так і у «вузькому» (зміна характеру одновимірних і багатовимірних розподілів з часом);

– відсутність розподілу Гаусса в розподілах характеристик і можливості опису розподілу яким-небудь з добре відомих параметричних сімейств розподілу ймовірностей;

– часте засмічення даних нехарактерними значеннями;

– самоподібність даних, що приводить до фрактальним процесам.

Зазначені особливості даних різко скорочують можливості застосування до їх аналізу традиційних математичних алгоритмів, ставлять під сумнів доцільність застосування так званих ефективних алгоритмів і алгоритмів, розрахованих на характер розподілу Гауса випадкових відхилень.

Одночасно виникає потреба в спочатку більш складних за своєю структурою алгоритмах аналізу даних навіть у порівняно простих ситуаціях, наприклад, усереднення за часом для стаціонарного процесу. Для нестаціонарного процесу з зазначеними вище особливостями доводиться замінювати однофакторной моделлю для локально стаціонарних ділянок ряду, а замість середнього значення (нестійкого до викидів) використовувати в цій моделі медіану.

Коротко основні вимоги до математичних методів і алгоритмів, необхідним для аналізу даних моніторингу комп'ютерних телекомунікаційних систем, можна сформулювати наступним чином: стійкість (робастність) до різних можливих відхилень даних від вихідних при-

пущень; свобода від, як правило, невідомого розподілу даних; більш детальний облік на рівні моделі можливої динаміки зміни процесу.

Здійснюючи моніторинг різних телекомунікаційних і розподілень обчислювальних систем, вирішуючи різні актуальні завдання аналізу мережевого трафіку протягом останніх років[1] були розроблені та апробовані на практиці нові математичні методи і алгоритми аналізу даних, що відповідають зазначеним вище вимогам. Зокрема були розроблені та реалізовані на практиці алгоритми: робастної знаковою процедури оцінки і прогнозу динаміки зростання завантаження магістральних каналів телекомунікаційних мереж[2]; однофакторного знакового оцінювання внутрішньодобових коливань швидкості передачі даних кінцевим користувачам; оцінювання мережевої активності користувачів комп'ютерних мереж[3] ; виділення статистичними методами нехарактерною мережевій діяльності в задачах активного аудиту[4].

Практика використання різних методів аналізу даних в системах моніторингу показує, жоден з існуючих методів не дає прийнятних значень помилок першого і другого роду, а також те, що різні методи дають на одних і тих же даних різну величину помилок. Причому метод, що дає найменшу помилку, різний для різних даних. Це є підставою для спроби побудови багатокомпонентної системи моніторингу, в якій використовується спільна робота декількох систем моніторингу, які застосовують різні методи виявлення атак. Ідея полягає в тому, щоб використовувати для аналізу даних саме ту систему моніторингу, яка найкращим чином підходить для цих даних. Для комбінування результатів декількох систем моніторингу в складі багатокомпонентної системи моніторингу повинен використовуватися вирішувач.

Представляється, що нейромережі можуть використовуватися не тільки як апарат для виявлення атак, але і як засіб побудови вирішувачів, створення яких є основною проблемою при розвитку багатокомпонентних систем моніторингу.

---

[1]Степанов Е., Корнеев И. Защита информации в офисе. – М.: "ТК Велби", 2007. - 336 с.

[2]Common Criteria for Information Technology Security evaluation. Version 1.0, 96,01.31.

[3]Степанов Е., Корнеев И. Защита информации в офисе. – М.: "ТК Велби", 2007. - 336 с.

[4]Threats to Computer Systems: an Overview - Computer Systems Laboratory Bulletin, March, 2009.

У своїй роботі система моніторингу використовує дані штатних журналів реєстрації, подій операційних систем і систем управління базами даних типових і спеціалізованих додатків у складі АС, засобів і підсистем забезпечення інформаційної безпеки, а також спеціалізованих засобів збору первинних даних моніторингу.

Збір та аналіз матеріалів виконується таким чином, що на елементи контрольованої системи не виявляється ніяких блокуючих впливів.

Основною функцією, що реалізується системою моніторингу, є автоматизований аналіз первинних даних моніторингу з метою оцінки стану інформаційної безпеки контрольованої системи. У рамках реалізації цієї функції система моніторингу забезпечує: автоматизоване налагодження журналів реєстрації подій підконтрольних ОС/СУБД на фіксацію даних, необхідних для проведення моніторингу контрольованої системи; зняття первинних даних моніторингу з об'єктів спостереження; первинну фільтрацію даних аудиту; виділення параметрів, що характеризують дії суб'єктів, і збереження їх в базу даних системи моніторингу; розбір даних журналів реєстрації подій в оперативному режимі; відображення поточного стану контрольованої системи; аналіз діяльності суб'єктів у базисі використаних ними ресурсів, що відображаються на дані аудиту; проведення деталізованих розслідувань діяльності спостережуваних суб'єктів за період їх роботи; графічне представлення результатів аналізу даних аудиту; формування звітних форм за результатами розслідування діяльності спостережуваних суб'єктів; перегляд і роздруківку всіх формованих звітних форм.

Структура системи моніторингу наведена на рис. 6.5.

Рис. 6.5. Структура системи моніторингу

Наведена структура може бути використана в практичній діяльності.

6.5. Імітаційна модель вірогідності реалізації загроз інформаційній безпеці підприємства

Розглянута раніше система містить безліч вузлів та відгалужень, у зв'язку з чим для детального її вивчення окремо розглядається кожен сегмент.

Експертною комісією виділені загрози, які можуть бути реалізовані. У табл. 6.2 представлено фрагмент переліку таких загроз з імовірностями їх настання.

Загальна схема функціонування імітаційної моделі наступна. Документ рухається за своїм маршрутом, на якому розташовані точки настання загроз. Документ, проходячи точку настання загрози, або продовжує рух до наступного робочого місця і фіксується факт нереалізації загрози, або з імовірністю настання загрози потрапляє на альтернативний шлях руху і фіксується факт настання загрози. Якщо загроза, що настала, перешкоджає подальшому просуванню документа, то цикл закінчується і в лічильник загроз, що наступили, додається одне значення. Якщо загроза не перешкоджає подальшому просуванню, то в лічильник загроз, що наступили, також додається одне значення, але документ продовжує рух.

Для визначення ймовірності настання загроз при побудові моделі використані експериментальні дані (табл. 6.2):

Загальна схема настання загроз представлена на рис. 6.6.

Для отримання найбільш достовірних результатів було прийнято рішення використовувати 1 000 000 одиниць модельного часу, що, в середньому, дозволяє згенерувати 5 000 000 документів.

Таблиця 6.2.

Імовірності настання загроз

Номер загрози	Найменування загрози	Імовірність настання загрози
1	Вихід з ладу апаратно-програмних засобів	0,1
2	Збій системи електропостачання	0,1
3	Ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи	0,25

Продовження таблиці 6.2.

Номер загрози	Найменування загрози	Імовірність настання загрози
4	Загроза крадіжки і фальсифікації внутрішніми порушниками	0,1
5	Несанкціонований доступ до інформації зовнішніми порушниками, що зберігається і обробляється в засобах автоматизації, з метою ознайомлення, спотворення чи знищень	0,1
6	Перехоплення інформації при її прийомі (передачі)	0,1
7	Стихійне лихо	0,1
8	Знищення (зміна, спотворення) інформації за рахунок випадкових перешкод, збоїв технічних (програмних) засобів при передачі, зберіганні та обробці інформації	0,1
9	Несанкціонований вплив внутрішніх порушників	0,05

У результаті багаторазово проведених дослідів виявлено, що кількість завершених документів становить 43,09% від кількості згенерованих. На наступному етапі в побудовану модель додані ймовірності реалізації загроз (табл. 6.3), визначені експертною комісією. Дані ймовірності додані у вигляді точки реалізації загрози, розташованої на альтернативному шляху просування документа.

Таблиця 6.3.

Імовірність реалізації загроз

Номер загрози	Найменування загрози	Імовірність реалізації загрози (*Експертні оцінки*)
1	Вихід з ладу апаратно-програмних засобів	0,1
2	Збій системи електропостачання	0,25

Продовження таблиці 6.2

Номер загрози	Найменування загрози	Імовірність реалізації загрози (*Експертні оцінки*)
3	Ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи	0,5
4	Загроза крадіжки і фальсифікації внутрішніми порушниками	0,1
5	Несанкціонований доступ до інформації зовнішніми порушниками, що зберігається і обробляється в засобах автоматизації, з метою ознайомлення, спотворення чи знищень	0,25
6	Перехоплення інформації при її прийомі (передачі)	0,25
7	Стихійне лихо	0,25
8	Знищення (зміна, спотворення) інформації за рахунок випадкових перешкод, збоїв технічних (програмних) засобів при передачі, зберіганні та обробці інформації	0,1

Після додавання ймовірностей реалізації загроз модель прийняла такий вигляд (рис. 6.7). Результатом додавання ймовірностей реалізації загроз стало збільшення до 88,92% згенерованих документів, які завершили рух до кінцевої точки, від кількості, що надійшли.

Наступним етапом стало додавання в систему ймовірностей реалізації загроз при наявності додаткової системи захисту.

Система захисту додана також у вигляді точки, розташованої на шляху реалізації загрози. Ймовірності реалізації загроз за наявності захисту також запропоновані експертами (табл. 6.4).

В результаті схема реалізації загроз прийняла вигляд, представлений на рис. 6.8.

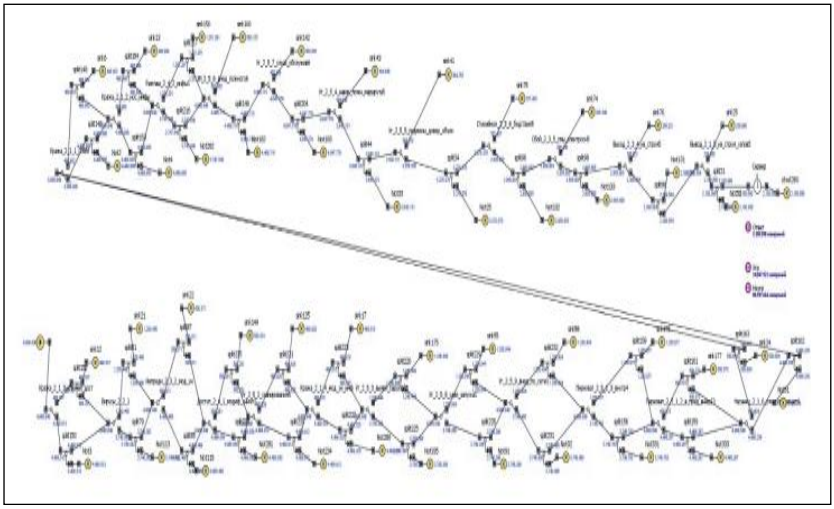


Рис. 6.6. Загальна схема настання загроз

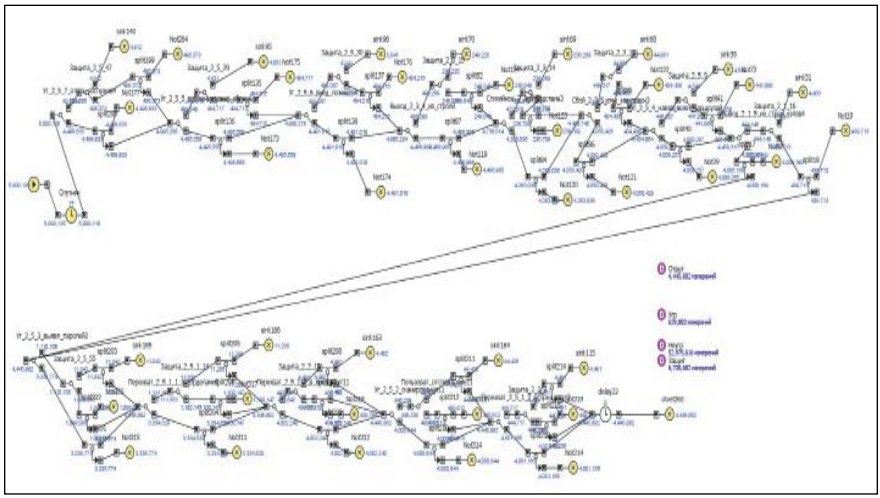


Рис. 6.7. Схема реалізації загроз

Таблиця 6.4.

Імовірність реалізації загрози за наявності захисту

Номер грози	Найменування загрози	Імовірність алізації загрози (*Екс - пертні оцінки*)
1	Вихід з ладу апаратно-програмних засобів	0,5
2	Збій системи електропостачання	0,1
3	Ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи	0,5
4	Загроза крадіжки і фальсифікації внутрішніми порушниками	0,1
5	Несанкціонований доступ до інформації зовнішніми порушниками, що зберігається і обробляється в засобах автоматизації, з метою ознайомлення, спотворення чи знищень	0,01
6	Перехоплення інформації при її прийомі (передачі)	0,01
7	Стихійне лихо	0,01
8	Знищення (зміна, спотворення) інформації за рахунок випадкових перешкод, збоїв технічних (програмних) засобів при передачі, зберіганні та обробці інформації	0,01
9	Несанкціонований вплив внутрішніх порушників	0,01

У результаті проведених експериментів встановлено, що до робочого місця надходить 97,95% згенерованих документів, при середній кількості загроз, що реалізувалися, на один документ 0,026, що рівносильно однієї реалізованої загрозі на 39 документів, що поступили. Відсоток реалізованих загроз від кількості реалізованих, нереалізованих і загроз, що не наступили склав 0,2.

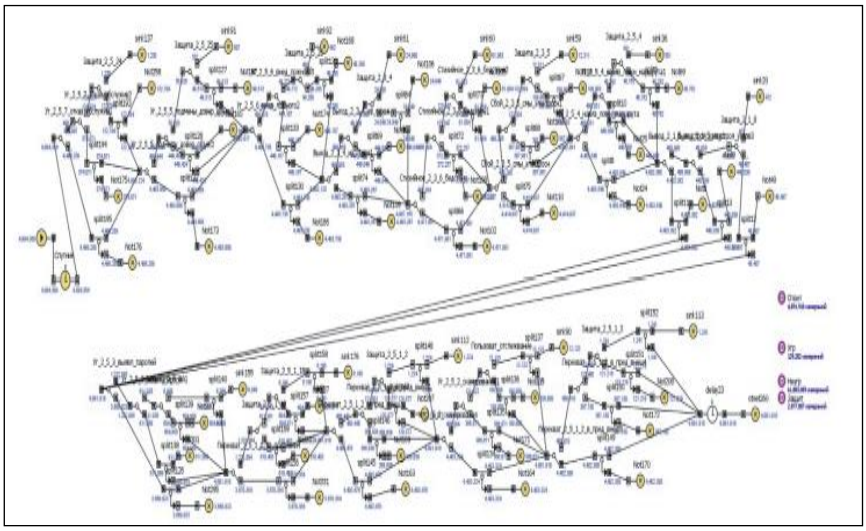


Рис.6.8. Схема реалізації загроз при наявності системи захисту

З метою виявлення загроз, які найбільш значимо впливають на кінцевий результат, результати реалізації загроз розглянуті окремо від інших результатів вимірювань (табл. 6.5).

Таблиця 6.5.

Відсоток кількості реалізованих загроз

Номер загрози	Найменування загрози	Кількість загроз із захистом	Процент кількості загроз із захистом від загальної кількості
1	Вихід з ладу апаратно-програмних засобів	24960	23,963
2	Збій системи електропостачання	12311	11,819

Продовження Таблиці 6.5

Номер загрози	Найменування загрози	Кількість загроз із захистом	Процент кількості загроз із захистом від загальної кількості
3	Ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи	61963	59,490
4	Загроза крадіжки і фальсифікації внутрішніми порушниками	507	0,486
5	Несанкціонований доступ до інформації зовнішніми порушниками, що зберігається і обробляється в засобах автоматизації, з метою ознайомлення, спотворення чи знищень	1110	1,065
6	Перехоплення інформації при її прийомі (передачі)	1224	1,175
7	Стихійне лихо	492	0,472
8	Знищення (зміна, спотворення) інформації за рахунок випадкових перешкод, збоїв технічних (програмних) засобів при передачі, зберіганні та обробці інформації	501	0,481
9	Несанкціонований вплив внутрішніх порушників	1089	1,045

Проведені експерименти з імітаційної моделі показали, що до найбільш імовірних загроз відносяться:

– ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи - 59,49% від загальної кількості загроз, що реалізувалися;

– вихід з ладу апаратно-програмних засобів - 23,96%;

– збій системи електропостачання - 11,819%.

– перехоплення інформації при її прийомі (передачі) - 1,175%.

З метою оцінки якості і значущості захисту від кожної загрози, яка, на думку експертної комісії, може наступити, з моделі по черзі забирався додатковий захист від кожної загрози і проводилися вимірювання.

Отримані результати вимірювань представлені в табл. 6.6.

Таблиця 6.6.

Результати вимірювань

Номер загрози	Кількість документів	Кількість завершених документів без інцидентів	Кількість реалізованих загроз	Кількість нереалізованих загроз	Кількість нереалізованих загроз внаслідок захисту	Кількість загроз, реалізованих за відсутності захисту
1	5004910	4877560	154190	61799198	2048685	49943
2	5003060	4789537	239928	61248833	1935840	123117
3	4999970	4835475	191280	61476302	1997640	124135
4	5007475	4856558	177781	61529762	2016343	49854
5	4997500	4894671	251281	61916330	1959505	122881
6	4994540	4891885	735148	61879219	1475212	611745
7	4995535	4894067	735484	61908465	1473383	612318
8	5004825	4853402	178383	61541698	2015855	48793
9	4993975	4890926	251022	61871221	1957135	122124

На основі отриманих результатів були знайдені (табл. 6.7): відсоток кількості завершених документів без інцидентів від кількості, що надійшли в систему; відсоток кількості загроз, що реалізувалися від загальної кількості реалізованих і нереалізованих загроз; відсоток

кількості загроз, реалізація яких відвернена системою захисту, від загальної кількості реалізованих і нереалізованих загроз; відсоток кількості реалізованих загроз, захист від яких не враховувалася під час проведення експерименту, від загальної кількості реалізованих загроз.

Проаналізувавши результати, представлені в табл. 6.7, можна виділити загрози, відсутність захисту від яких найбільш очевидно впливає на кінцевий результат.

Таблиця 6.7.

Результати чисельних розрахунків

Номер загрози	Відсоток пройдених документів без інцидентів	Відсоток кількості реалізованих загроз	Відсоток кількості загроз, реалізація яких відвернена системою захисту, від загальної кількості загроз	Відсоток кількості реалізованих загроз за відсутності захисту від загрози, від кількості реалізованих загроз
1	97,455	0,249	3,307	32,390
2	95,732	0,390	3,148	51,314
3	96,710	0,310	3,239	64,897
4	96,986	0,288	3,268	28,042
5	97,942	0,404	3,152	48,902
6	97,945	1,174	2,356	83,214
7	97,969	1,174	2,352	83,254
8	96,974	0,289	3,266	27,353
9	97,937	0,404	3,150	48,651

Зниження завершених документів без інцидентів до 95,73% призводить відсутність захисту від загрози збою системи електропостачання відповідно.

Відсутність захисту від інших загроз впливає на кінцевий результат в менш значній мірі (не більше 1%). Крім зазначеної загрози можна відзначити загрозу «Ненавмисні помилки користувачів, опера-

торів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи», «Загроза крадіжки і фальсифікації внутрішніми порушниками», «Знищення (зміна, спотворення) інформації за рахунок випадкових перешкод», відсутність захисту від яких призводить до збільшення відсотка реалізованих загроз від кількості всіх врахованих загроз до 1,26%.

Ефективність засобів захисту також можна оцінити, порівнявши відсоток реалізації конкретної загрози від загальної кількості реалізованих загроз з відсотком кількості реалізованих загроз, захист від яких не враховувався під час проведення експерименту, від загальної кількості реалізованих загроз (табл. 6.8).

Таблиця 6.8.

Порівняння відсотків реалізації загроз

Номер загрози	Найменування загрози	Відсоток реалізації загрози за наявності захисту	Відсоток реалізації загрози за відсутності захисту
1	Вихід з ладу апаратно-програмних засобів	23,963	32,390
2	Збій системи електропостачання	11,819	51,314
3	Ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи	59,490	64,897
4	Загроза крадіжки і фальсифікації внутрішніми порушниками	0,486	28,042
5	Несанкціонований доступ до інформації зовнішніми порушниками, що зберігається і обробляється в засобах автоматизації, з метою ознайомлення, спотворення чи знищень	1,065	48,902
6	Перехоплення інформації при її прийомі (передаіе)	1,175	83,214
7	Стихійне лихо	0,472	83,254

Продовження таблиці 6.8.

Номер загрози	Найменування загрози	Відсоток реалізації загрози за наявності захисту	Відсоток реалізації загрози за відсутності захисту
8	Знищення (зміна, спотворення) інформації за рахунок випадкових перешкод, збоїв технічних (програмних) засобів при передачі, зберіганні та обробці інформації	0,481	27,353
9	Несанкціонований вплив внутрішніх порушників	1,045	48,651

Проаналізувавши результати, представлені в табл. 6.8, можна зробити висновок, що в цілому система захисту від реалізації загроз є ефективною. Ймовірність реалізації таких загроз, як погрози виходу з ладу апаратно-програмних засобів та нанесення ненавмисних помилок користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи, досить велика і, в той же час, наявність захисту кардинальним чином не впливає на загальний результат.

Відсутність ефективного захисту обумовлено тим, що ймовірність реалізації даних загроз носить спонтанний характер і в дуже малому ступені залежить від регульованих факторів.

Запропонована система інформаційної безпеки не може бути спроектована одного разу, оскільки вона динамічна, то необхідно проводити постійний моніторинг і виявляти недоліки для подальшого вдосконалення.

ВИСНОВКИ

Процес протидії рейдерським захопленням підприємств досить трудомісткий, судові позови можуть розглядатися довгі місяці, роки. Виявлення на ранніх стадіях розпочатого рейду, при своєчасних відповідних діях, запорука успішної протидії «загарбникам». Забезпечення належного рівня безпеки підприємства доцільно розпочати з відповідних заходів щодо інформаційної безпеки підприємства, збереження комерційної таємниці, а також іншої важливої фінансової документації.

Для ефективної боротьби із рейдерством потрібно докласти спільних зусиль як з боку влади, так і з боку бізнес-структур і громадськості. Основними напрямами дій повинні стати: вдосконалення законодавства в галузі корпоративного управління та усунення прогалин в господарському процесуальному законодавстві, які дають змогу здійснювати протиправні дії; встановлення санкцій або кримінальної відповідальності за дії, що наносять шкоду вітчизняним підприємствам; регулювання судової системи, детальна перевірка кожної справи; підвищення правової культури та свідомості пересічних громадян та суб'єктів підприємницької діяльності; подолання корупції в урядових структурах.

Крім цього, необхідно також проводити профілактичні заходи на підприємстві (наприклад, юридичний аудит). В комплексі, ці заходи дозволять оперативно реагувати на рейдерські посягання та унеможливлять їх в подальшому. Також це позитивно вплине на рівень економічної безпеки підприємництва.

Дані пропозиції будуть мати позитивний результати за умов, якщо управління системою забезпечення захисту підприємства буде максимально наближене його менеджментом до вирішення тих проблем , заради яких сформована наведена система, а також з урахуванням ситуації, яка склалась навколо конкретного суб'єкту господарської діяльності.

Монографія розрахована на широке коло науковців, представників органів влади та самоврядування, практикуючих юристів, економістів, аспірантів та студентів навчальних і наукових закладів, які займаються проблемами рейдерства тощо.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абалкин Л. И. Экономическая безопасность России: угрозы и их отражение / Л. И. Абалкин // Вопросы экономики. – 1994. – № 12. – С. 4-13.
2. Акимов В.А. Оценка и прогноз стратегических рисков России: теория и практика / Право и безопасность. – 2004. – № 1. – С. 17.
3. Александров І.О. Моделі економічної динаміки і система національних розрахунків. – Донецк: ІЕП НАН України, 1998. – 100с.
4. Амитан В.Н. Экономическая безопасность: концепция и основные модели // Економічна кібернетика. - 2009. – №3-4. – С. 13-20.
5. Андреев В., Здирук К. «ИВК Юпитер»: реализация корпоративной политики безопасности //Открытые системы. Июль-август 2003. – С. 43-46.
6. Анисимов С. Рейдерство в России. Особенности национального захвата. СПб.: Невский проспект, «Вектор», 2007. – 217 с.
7. Анохин В.С. Предпринимательское право: Учебник. М.: ВЛАДОС, 1999. – 369 с.
8. Баканов М.И. Теория экономического анализа: Учебник / Баканов М.И., Шеремет А.Д. – М.: Финансы и статистика, 2006. – 220 с.
9. Барановский В.К. Концепция перехода Украины на модель устойчивого развития // Проблемы теории и практики управления. – 1998. - №5. – С. 23-24.
10. Басовский Л. Е. Прогнозирование и планирование в условиях рынка, Учебное пособие. - М.: ИНФРА-М, 2001. – 260с.
11. Батченко Л.В. Методика системної діагностики впливу стану зовнішньоїторгівлі на зміну рівня економічного суверенітету України / Л.В. Батченко, О.О. Ашурков, О.Г. Ткаченко ; НАН України, Ін-т економіко-правових досліджень. — Донецьк : Юго-Восток, 2012. – 77 с.
12. Баутов А.Н. Эффективность защиты информации /Открытые системы. Июль-август 2003. С. 56-60.
13. Белов М. Информация - новый вид финансовых активов/Банковские технологии 1997: [Электронный ресурс]: http:/www.bizcom.ru/rus/b 1 /1997/nr2/l 7.html, 30.10.2004.
14. Березин А.С., Петренко С.А. Построение корпоративных защищенных виртуальных частных сетей//Конфидент: Защита информации. - 2001. - № 1. – С. 54-61.

15. Берназ П.В. Рейдерство в Україні: визначення поняття / П.В. Берназ, О.О. Середа // Проблеми цивільного та господарського права. – 2008. – № 1. – С. 82-84.

16. Бетелина В.Б., Галатенко. В. Основы информационной безопасности. Курс лекций-(3-е издание). - "Интернет-университет информационных технологий", 2006. – 208 с.

17. Бєліков О. Рейдерство в Україні – реалії сьогодення // Юридичний журнал. – 2007. – № 4. – С. 105-109.

18. Бироваш М. Силовой прием / М. Бироваш // Бизнес. – 2007. – № 6. – С. 24-27.

19. Бокс Дж., Дженкинс Г. Анализ временных рядов. Прогноз и управление. – М.: Мир, 1994.

20. Большая Советская Энциклопедия. Гл.ред. А.М. Прохоров. Изд. 3-е. В 30 т. Т. 28. – М.: Советская Энциклопедия, 1978. – С. 138.

21. Борисов Ю. Корпоративное рейдерство как социально-экономическое явление в мировой экономике : аналитический доклад. – М. : Первый институт корпоративного права, 2007. – 122 с.

22. Боровиков В.П., Ивченко Г.И. Прогнозирование в системе STATISTICA в среде Windows. Основы теории и интенсивная практика на компьютере: Учеб. пособие. – М.: Финансы и статистика, 2000. – 384 с.

23. Бочарников В.П., Релецкий С.М., Захаров К. В. и другие. Риски во внешнеэкономической деятельности предприятий. – К.: ИНЭКС, 1997. — 170 с.

24. Бруевич Н. Г. Количественные оценки надежности изделий, в сборнике: Основные вопросы теории и практики надежности - М.,1971 – 122 с.

25. Бусленко Н.П. Моделирование сложных систем. М.: Главная редакция физико-математической литературы изд-ва «Наука», 1968. – 356с.

26. Вакханалия стоп : украинским рейдерам светят новые перспективы [Електронне джерелео]. – Інтернет видання Інформаційної агенції « ЛІГАБізнесінформ». – № 103 (744). – 2008. – Режим доступу: www.times.liga.net//articles/gs013450.html.

27. Варналій З. С., Мазур І. І. Рейдерство в Україні: Передумови та шляхи подолання // Стратегічні пріоритети. – 2007. – № 2 (3). – С. 129-136.

28. Варналій З., Мазур І. Основні передумови та шляхи подолання рейдерства в Україні. Аналітична записка Національного інституту стратегічних досліджень / З. Варналій, І. Мазур [Електронний ресурс]. – Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу: http://old.niss.gov.ua/Monitor/juli/1.htm

29. Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – 384с.

30. Веблен Т. Теория праздного класса. М.: Прогресс, 1984. – 368 с.

31. Великий тлумачний словник сучасної української мови / Укл. і голов.ред. В.Т. Бусел. – К., 2002. – 1440 с.

32. Вечканов Г. С. Экономическая безопасность : учеб. / Григорий Сергеевич Вечканов. – СПб. : Питер, 2007. – С.31-32.

33. Виленский П.Л., Лившиц В.Н., Смоляк С.А.: Оценка эффективности инвестиционных проектов: Теория и практика. Учебное пособие. – 2-е изд., перераб. и доп. – М.: Дело, 2002 – 251 с.

34. Вихорев С, Кобцев Р. Как определить источники угроз // Открытые системы.-2002, № 7-8.-С. 6-11.

35. Вицин С.Е. Системный подход и преступность / Академия МВД СССР. – М., 1980. - 139 с.

36. Вірченко В.В. Передумови та методи недружнього поглинання суб`єктів господарювання / В.В. Вірченко // Теоретичні та прикладні питання економіки. – 01/2011. – Вип.24 . – С. 236-244.

37. Вітлінський В. В., Верченко П. І. Аналіз, моделювання та управління економічним ризиком: Навч.-метод. посібник для самост. вивч. дисц. – К.: КНЕУ, 2000 – 15 с.

38. Вітлінський В.В. Аналіз, оцінка і моделювання економічного ризику. – К.: Деміур, 1996. – 212 с.

39. Вітлінський В.В., Наконечний С.І., Шарапов О.Д. Економічний ризик і методи його вимірювання: Підруч. – К.: ІЗМН, 1996. – 400 с.

40. Волокитин А.В., Маношкин А.И., Солдатенков А.В. и др. Информационная безопасность государственных организаций и / коммерческих фирм; Справочное пособие,- М.: НТЦ «ФИОРД - ИНФО», 2009. - 272 с.

41. Воронкова А.Э., Козаченко А.В., Рамазанов С.К., Хлапенов Л.Е. Современные технологии управления промышленным предприятием. – Киев: Лібра . 2007. – 254 с.

42. Гайкович В., Ершов Д. Основы безопасности информационных технологий. - М.:МИФИ, 1995.-94 с.

43. Гапоненко В.Ф., Беспалько АЛ., Власков А.С. Экономическая безопасность предприятий. Подходы и принципы. – М .: Издательство «Ось-89», 2007. - 208 с.

44. Геєць В. Економічні реформи в Україні: моделі, реалії та уроки // Банківська справа. – 1996. – №4. – С. 26-33.

45. Гиг Дж. Ван. Прикладная общая теория систем. – М.: Мир, 1981. – С. 345.

46. Глушевський В.В. Методологічні основи концепції управління ризиками підприємницької діяльності / В.В. Глушевський // Фінанси України. − 2009. − № 9. − С. 116-124.

47. Головань І. В. Рейдерство – модний термін чи зручна ширма? // Вісник господарського судочинства. – 2008. – № 6. – С. 127.

48. Господарський Кодекс України від 16.01.2003 р. № 436 – IV // Офіційний вісник України. – 2003. – № 11. – Ст. 462.

49. Гражданское право: Учебник / Егоров И.Д., Елисеев И.В., Иванов А.А. и др. / Под ред. Ю. К. Толстого, А. П. Сергеева. Ч. II. М.: «ПРОСПЕКТ», 2000 . – С. 496

50. Грек Б.М., Грек Т.Б. Поняття та історичні передумови розвитку рейдерства в Україні / Б.М. Грек, Т.Б. Грек / Адвокат. – 2010. – № 9. – С. 29-34.

51. Гришина Н. В. Организация комплексной системы защиты информации - "Гелиос АРВ", 2007 г. – 256 с.

52. Гуман Е.О. Развитие организационно-экономического механизма защиты предпринимательской структуры от угрозы рейдерства : диссертация ... кандидата экономических наук : 08.00.05 / Гуман Екатерина Олеговна; [Место защиты: Ин-т экономики УрО РАН].- Екатеринбург, 2010.- 277 с.

53. Гуторова Н. Щодо встановлення кримінальної відповідальності за рейдерство // Юридичний радник.– 2007. – № 2. – С. 6-9.

54. Декарт Р. Избранные сочинения. - М.: Наука, 1970. – С. 508.

55. Дикань В.Л. Куркін М.В. Роль конкурентної розвідки у боротьбі із недружніми поглинаннями в Україні // Вісник економіки транспорту і промисловості №28, 2009. – С. 28-32.

56. Дмитрієв І.А. Управління ризиком рейдерських захоплень : [монографія] / І.А. Дмитрієв, В.Ю. Несторенко. − Х. : ХНАДУ, 2011. − 164 с.

57. Добровольский В.И. Ответственность рейдера по российскому законодательству / В.И. Добровольский. – М.: Волтерс Клувер, 2010. – 168 с.

58. Донцова Л.В, Никифорова Н.А. Анализ финансовой отчетности – 2-е изд.- М.: Дело и сервис, 2004. — 102 с.

59. Дорошук А.А., Трибуха М.В. Система регулювання рейдерства в Україні / А.А. Дорошук, М.В. Трибуха // Економіка: реалії часу. – 2011. – № 1. – С. 170-176.

60. ДСТУ 2293-99. Охорона праці. Терміни та визначення основних понять. – К.: Держстандарт, 1996. – 19 с. Введено в дію наказом Держстандарту України від 26.03.1999 р. № 164.

61. Дульський О.О. Рейдерство – нова загроза державній та економічній безпеці України // Боротьба з організованою злочинністю і корупцією. – 2009. – № 11. – С. 87-96.

62. Економіко-математичні моделі оцінки фінансового стану суб'єктів господарювання: монографія / О.М. Тридід, О.Г. Тижненко, Л.О. Тижненко. – К.: УБС НБУ, 2009. – 213 с.

63. Економічний суверенітет держави та напрями його правового забезпечення : монографія / за ред. О. О. Ашуркова ; НАН України, Ін-т економіко-правових досліджень. – Донецьк : Юго-Восток, 2012. – 406 с.

64. Ельбрехт В. Еволюція страхування / В. Ельбрехт // Вісник Запорізького юридичного інституту. – 2004 - № 2 (27). – С. 71.

65. Еникеева Л.А., Стельмашонок Е.В. Инфраструктурная составляющая нематериальных активов как объект оценки и защиты.// Экономика и промышленная политика России: Труды Ш Международной научно- практической конференции. 14-19 июня 2004 г. СПб.: Издательство Политехнического университета. 2004. - С. 525-528.

66. Еникеева Л.А., Стельмашонок Е.В. Методологические подходы к оценке информационных активов как инфраструктурной составляющей нематериальных активов.//Актуальные проблемы экономики и новые технологии преподавания (Смирновские чтения): Мате-

риалы IV международной научно-практической конференции (15-16 марта 2005 г, Санкт-Петербург) Т.2,-СПб.: Издательство Политехнического университета. 2005.- с. 181-183.

67. Єріна А. М. "Статистичне моделювання та прогнозування", Навчальний посібник. – К.: КНЕУ, 2001. – 170 с.

68. Єфименко А. Рейдерство або ринок контролю [Електронний ресурс] / А. Єфименко // Юридичний журнал. Видавнича організація "Юністіан". – Режим доступу: http://justinian.com.ua/article.php?id=3072.

69. Жаліло Я. А. Економічна стратегія держави: теорія, методологія, практика / Ярослав Анатолійович Жаліло. – К. : НІСД. 2003. – 224 с.

70. Желнорович А. В. Рейдерство в России – показатель институционального дефицита российской экономики / А. В. Желнорович // Российская юстиция. – 2007. – № 8. – С. 15-23.

71. Житомирский В.С. Рейдерство: явление, причины, профилактика, защита / В.С. Житомирский. − СПб.: Ленинградская торгово-промышленная палата, 2006. − 54 с.

72. Забезпечення фінансової безпеки на мікро- та макрорівнях : кол. монограф. / [кол. авт. ; ред. : О.А. Бурбело]; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2014. – 336 с.

73. Забродский В., Капустин Н. Теоретические основы оценки экономической безопасности отрасли и фирмы // Безнес-информ. – 1999. – № 15-16. – С. 35-37.

74. Заец А.М. Минимизация риска утраты права собственности, вызванного рейдерством, путем использования титульного страхования / А.М. Заец // Вестник Российской правовой академии (г. Москва, Российская Федерация). – 2014. – № 1. – С. 26-29.

75. Заєць О.М. Економічна безпека страхового ринку України / О.М. Заєць // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2013. – № 1. – С. 277-282.

76. Заєць О.М. Страхування ризиків підприємництва − ефективний шлях поліпшення економічної безпеки держави / О.М. Заєць // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2014. – спец. вип. № 3. – С. 170-173.

77. Заєць О.М., Шурінов М.В. Захист права власності на нерухоме майно за допомогою використання титульного страхування /

О.М. Заєць, М.В. Шурінов // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2013. – № 3. – С. 239-246.

78. Закон України «Про державну реєстрацію речових прав на нерухоме майно та їх обмежень» від 01.07.2004 1952-IV // Відомості Верховної Ради України. − 2004. − № 51. − ст. 553.

79. Закон України «Про страхування» від 04.10.2001 р. № 2745 – III (із змін. та доп.) // Право і практика. – 2009. - № 4. – С. 3 – 38.

80. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. -М.: Горячая линия-Телеком, 2000. - 452 с.

81. Земцова Ю. Сестрички Exxon Mobile / Ю. Земцева / Слияния и поглощения. – 2006. – № 9. – С. 104-109.

82. Ивлев В.А., Попова Т.В. Процессная организация деятельности: методы и средства. (Консалтинговая компания «ВИЛ Анатех»): [Электронный ресурс]: http://www.optim:ru/comp/2001/3/anatech/anatech.asp.

83. Игнатишин Ю. Слияние и поглощение: стратегия, тактика, финансы / Юрий Игнатишин. − СПб. : Издательский дом «Питер», 2005. − 201 с.

84. Идельсон В.Р. Страховое право. – М.: Анкил, 1993. – С. 3

85. Иеринг Р. Цель в праве. − СПб., 1881. − С. 109-110.

86. Ильичев А.В. Эффективность проектируемой техники: Основы анализа. – М.: Машиностроение, 1991. – 336 с.

87. Ионцев М. Г. Корпоративные захваты : слияния, поглощения, гринмэйл : [монографія] / М. Г. Ионцев. – М. : Ось-89, 2008. – 272 с.

88. ИСО/МЭК 15408-99 «Критерии оценки безопасности информационных технологий».

89. Іванов В.Л. Управління економічною стійкістю промислових підприємств (на прикладі підприємств машинобудівного комплексу): Монографія. – Луганськ: Вид-во СНУ ім. В. Даля, 2005. – 265с.

90. Калюжний Р.А., Заєць О.М. Теоретичні концепції еволюції механізму регулювання страхової діяльності в Україні / Р.А. Калюжний, О.М. Заєць // Юридичний вісник Національного авіаційного університету. – 2015. – № 2 (35). – С. 20-25.

91. Кендэлл М. Временные ряды. – М.: Финансы и статистика, 1981.

92. Киреев А.Ю. Рейдерство в Российской экономике: сущность, тенденции и возможности противодействия. Автореф. дис. … канд. экон. наук: 08.00.05 / А.Ю. Киреев. – М., 2008. – 22 с.

93. Клапків М.С. Страхування фінансових ризиків. Монографія. − Тернопіль: Економічна думка, Карт-бланш. − 2002. − 570 с.

94. Ковалев В.В., Волкова О.Н. Анализ хозяйственной деятельности предприятия.– М.: ТК Велби, 2002. – 34 с.

95. Ковальчук К.Ф. Методи інтелектуальної підтримки прийняття економічних рішень // Автореф. дис. д-ра екон. наук. — К.: НАН України ІК ім. В.М.Глушкова, 1996. — 32с.

96. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения / А. В. Козаченко, В. П. Пономарев, А. Н. Ляшенко. – К. : Либра, 2003. – 280 с.

97. Козаченко А.В., Пономарев В.П. Методические основы оценки уровня экономической безопасности предприятия // Региональные перспективы. — №2-3(9-10).-С. 104-106.

98. Козачок В.И., Гребенев С., Семкин С., Беляков Э. Основы организационного обеспечения информационной безопасности объектов информатизации. - "Гелиос АРВ", 2005 г. – 192 с.

99. Колєсник М.А. Рейдерство в Україні: Загальна характеристика та основні тенденції розвитку [Електронний ресурс] // Право і безпека. – 2011. – № 1. – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/pib/2011_1/PB-1/PB-1_16.pdf

100. Колпаков П.А. Концептуальные основы экономической безопасности фирмы : автореф. дис. канд. екон. наук / П.А. Колпаков. — М., 2007.— 25 с.

101. Кольцова И. В., Рябых Д. А. Практика финансовой диагностики и оценки проектов. — М.: ООО «И.Д. Вильямс», 2007. — 416 с.

102. Коммерческое право: Учебник / Под ред. В.Ф. Попандопуло, В.Ф. Яковлевой. С-П.: Изд.-во СПб. ун-та, 1998. – С. 275.

103. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия.- СПб.: БХВ-Петербург; 2003. - 752 с.

104. Коробчинський О.Л. Методика формування системи економічної безпеки підприємства // Актуальні проблеми економіки. — 2009. – № 4 . — С. 41-45.

105. Котляр Э. Гринмейл: русская версия [Електронне джерело] // Журнал «Консультант». - 2005. - № 5. - Режим доступу: http://www.cfin.ru/investor/ao/ prevent_greenmail.shtml?printversion.

106. Криничанский К. В. Рынок слияний и поглощений как среда реализации функции стимулирования предпринимателей и менеджеров / К. В. Криничанский // Менеджмент в России и за рубежом. – 2007. – № 3. – С. 115-118.

107. Крюков М.М., Сидоренко Е.М. Переход к устойчивому развитию экономики: системный подход и моделирование //Вест МГУ. Сер. Экономика. – 1997. – №4. – С. 89-107.

108. Кузнецов А.А. Защита деловой информации. - "Экзамен", 2008. – 255 с.

109. Лазуренко В.И. Рейдерсво : слияние и поглощение: монография / В.И. Лазуренко, Я.Н. Ломакин, Ю.В. Лазуренко. − М. : ТУКБИ, 2009. − 232 с.

110. Ларина И.Е. Экономика защиты информации : Учебное пособие. – М.: МГИУ, 2007. – 92 с.; С. 6.

111. Леоненков А В. Нечеткое моделирование в среде MATLAB и fuzzy ТБСИ. -СПб : БХВ-Петербург. 2009. - 736 с.

112. Липаев В.В. Стандарты на страже безопасности информационных систем// РС WECC/RR -2000. -№ 30. - С. 34-40.

113. Лопашенко Н. Рейдерство/ Н. Лопашенко // Законность. - 2007. - № 4. - С. 7-12.

114. Лянной Г. Система экономической безопасности предприятия // BOS — журнал о личной и коммерческой безопасности. — 2006. - №7. – С. 16-19.

115. Лященко М. Загальна характеристика рейдерства в Україні [Електронний ресурс] / Ляшенко М. — Режим доступу : http://www.kspu.edu/FileDownload.ashx?id=776fad03-832a-4a02-9c9d-86404b407b25.

116. Макайкин М. Что такое рейдерство? [Электронный ресурс] / Михаил Макайкин // Юридический блог "Юридический ликбез" – Режим доступа: http://www.svem.ru /blog/likbez/639. html.

117. Макарчук І.М. Рейдерство, як одна з форм тіньової економіки держави та його наслідки [Електронний рисурс] // Економічний вісник університету. Збірник наукових праць. – 2010. – № 1. – Режим доступу:
http://archive.nbuv.gov.ua/portal/soc_gum/evu/2010_15_1/Makarch.pdf.

118. Мак-Мак В.П. Служба безопасности предприятия (организационно-управленческие и правовые аспекты деятельности). - М: Мир безопасности, 1999. – 6 с.

119. Мак-Мак В.П. Служба безопасности предприятия. – М.: Баярд, 2003.– 10 с.

120. Максимов Д.А. Модели и методы оценки и управления экономической безопасностью предприятия // Автореф. Дис. кандидата екон. наук. – М.: Рос. эконом. ун-т им. Г.В. Плеханова, 2011 – с 19-22 дис. ... кандидата экономических наук : 08.00.13 / Максимов Денис Алексеевич; [Место защиты: Рос. эконом. ун-т им. Г.В. Плеханова].- Москва, 2011.- 24 с.

121. Малкж А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб, пособие для вузов,- М: Горячая линия, Телеком, 2004. – 280 с.

122. Мамутов В.К. Правове забезпечення економічного суверенітету в умовах міжнародної інтеграції : розділ до доповіді з дослідницького проекту «Національний суверенітет України в умовах глобалізації» / В.К. Мамутов; НАН України; Інститут економіко-правових досліджень. — ІЕПД НАН України, 2011. — 100 с.

123. Мамутов В. Рейдерство в законі / В. Мамутов // Дзеркало тижня. – 2008. – № 38.

124. Манахов С.А., Акжигитов Р.И., Сычев П.Г. О международном опыте по противодействию преступлениям на рынке ценных бумаг, в том числе противоправным корпоративным захватам имущественных комплексов юридических лиц // Аналитический обзор. – М.: Следственный комитет при МВД России, 2009. – С. 5.

125. Мартынов С.Г. Гражданско-правовые механизмы защиты от недружественных поглощений хозяйственных обществ : диссертация ... кандидата юридических наук : 12.00.03 / Мартынов Сергей Геннадьевич; [Место защиты: Российская академия народного хозяйства].- Москва, 2011.- 173 с.

126. Матвеев Н. Экономическая безопасность предприятия : дисс. ... канд. экон. наук. – М. : Изд-во "Лотос", 1999. –20 с.

127. Медынский В.Г., Илъдеменов С.В. Реинжиниринг инновационного предпринимательства: Учеб. пособие/Под ред. проф. В.Л. Ирикова. М.:ЮНИТИ, 1999. -414 с.

128. Медынский В.Г., Илъдеменов С.В. Реинжиниринг инновационного предпринимательства: Учеб. пособие/Под ред. проф. В.Л. Ирикова. – М.: ЮНИТИ, 1999. - 414 с.

129. Мельник Т. Кількісний аналіз оцінки ризику // Фінанси України. – 2000. – № 9. – С. 63-67

130. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем: Пер. с англ. М.: Мир, 1973. – 344с.

131. Мищенко А.В., Попов А.А. Модели управления портфелем ценных бумаг. - М.: Рос. экон. Академия, 1999. – 38с.

132. Морозов Н. П., Чернокнижный С. Б. Защита деловой информации для всех. – М.: "ИД "Весь"', 2003. -160 с.

133. Мухина А. Блеф, замешанный на коррупции (17 апреля 2008 года, г. Саратов) / А. Мухина // "Газета "Богатей". – 2008. – № 15 (440). – Электронный ресурс: Режим доступа: http://www. bogatej.ru/bogatej/print.php?fr=440&article=22042008120838&art_id=0.

134. Національний суверенітет України в умовах глобалізації: Національна доповідь. – К.: Парламентське вид-во, 2011. – 112 с.

135. Нехорошев Ю.С. Экономика России в XXI веке: Сборник научных трудов VII Все-российской научно-практической конференции «Фундаментальные проблемы модернизации экономики России» / Под ред. Г.А. Барышевой, Л.М. Борисовой; Национальный исследовательский Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2010. – С. 153-156.

136. Нижник В.М. Економічна дипломатія та економічна безпека України: Навчальний посібник / В.М. Нижник. – Хмельницький: ХНУ, 2007. – 299 с.

137. Норт Д. Институциональные изменения: рамки анализа // Вопросыэкономики. - № 3 - С.6-17.

138. Норт Д. Інституції, інституційна зміна та функціонування економіки. – К.: Основи, 2000. – 189 с.

139. Овчинский В. Рейдеромафия / В. Овчинский // Огонек. – 2007. – № 16. – С. 18-21.

140. Ожегов С.И. Словарь русского языка. – М., 1978. – 710 с.

141. Осипенко О.Б. Защита компании от недружественного поглощения и корпоративного шантажа. – М.: Юркнига, 2005. – 237 с.

142. Основы экономической безопасности. (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. М., 1997. – 138 с.

143. Основы логистики. Функциональные области логистического управления. - Таганрог: Изд-во ТТИ ЮФУ, 2009. – 79 с.

144. Партыка Т.Л., Попов И.И. Информационная безопасность (2-е издание). – "Форум", 2007. – 368 с.

145. Паславський І. Основні етапи протидії українському бізнесу. Роль і позиції ЗМІ / І. Паславський // Вісник Львівського університету. – 2011. – Вип.34. – С. 158-172.

146. Пастернак-Таранушенко Г.А. Економічна безпека держави. Статики процесу забезпечення / Геннадій Адольфович Пастернак-Таранушенко ; за ред. Б. Кравченка. – К.: Кондор, 2002. – 302 с.

147. Пацурія Н.Б. Страхове право України: Навчальний посібник / Н.Б. Пацурія. – К.: ЮрІнком Інтер, 2006. – С. 30.

148. Персональный сайт ведущего украинского специалиста в области защиты информации Домарева В. В.[Электронный ресурс] http://www.security.ukrnet.net.

149. Петраков А., Мельников В., Клейменов С. Информационная безопасность и защита информации (3-е издание): «Academia», 2008. – 336 с.

150. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность - М.: Компания АйТи, ДМК Пресс, 2004.- 384 с.

151. Петров Юрий Владимирович. Особенности реализации экономических интересов предприятия (фирмы) в транзитарной экономике России : Дис. ... канд. экон. наук : 08.00.01. Тамбов, 2000. – 147 с.

152. Підскунова О. В. Аналіз та оцінка фінансових ризиків діяльності малих підприємств // Фінанси України. - 2007 . – № 8 . – С. 119–129

153. Полушкин О.А. Рейдерство: пути решения актуальных проблем // Закон и право. – 2008. – № 2. – С. 62.

154. Понятие рейдерства. Факторы [Электронный ресурс]. - Real Estate Development Group. – Режим доступа : http://www.red-develop.com/ru/informaciya/analitika /115.html.

155. Попов А.И. Экономическая теория: Учебник для вузов. 4-е изд. – СПб.: Питер, 2006. – 544 с.

156. Потапов В.Я. Оценка и прогноз опасностей и угроз современной России // Право и безопасность. – 2003. – № 3-4. – С. 11.

157. Предборський В.А. Економічна безпека держави: Монографія. – К.: Кондор, 2005. – 391 с.

158. Привлечение и защита инвестиций станут приоритетом в работе украинского правительства [Електронне джерело] – Офіційний портал інформаційної агенції «УНІАН». – Режим доступу: http://www.unian.net/news/577585-arbuzov-poobeschal-evropeyskim-poslam-iskorenit-reyderstvo-v-ukraine.html

159. Про затвердження Ліцензійних умов провадження страхової діяльності від 28.08.2003 р.: Розпорядження Державної комісії з регулювання ринків фінансових послуг № 40 // www.radagov.ua.

160. Противодействие недружественным поглощениям: Научно-практическое пособие. – М.: ОЛМА-ПРЕСС, 2006. – 352 с.

161. Пыльский В.В. Рейдерство: место и значение коррупции / В.В. Пыльский / Наука-2010 : сб. науч. ст. В 2 ч. Ч. 1 / ГрГУ им. Я. Купалы ; редкол.: А.Ф. Проневич (отв. ред.) [и др.]. – Гродно : ГрГУ, 2010. – 370 с.

162. Радванська Н.В. Рейдерство як загроза економічній безпеці підприємства та держави // Вісник Хмельницького національного університету. – 2011. – № 2. – С. 204-206.

163. Райх В.В., Тихонов В.А. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. - "Гелиос АРВ", 2006. – 528 с.

164. Райхер В.К. Общественно-исторические типы страхования. – М.: ЮКИС, 1992 . – 19 с.

165. Рамазанов С.К. Многокритериальное управление безопасностью предприятия в условиях смешанной неопределенности /Важке машинобудування. Проблеми та перспективи розвитку: НПК, Краматорськ, ДДМА, 2007 р.: материалы – V, 2007. – С. 103-104.

166. Рамазанов С.К., Истомин Л.Ф., Припотень В.Ю. Синергетическая модель управления эколого-экономической безопасностью предприятия в условиях нестабильности.//Вестник ДДМА. – Краматорск: ДДМА, 2007. – № 2 (8). – С. 25-28.

167. Рамазанов С.К., Припотень В.Ю. Методы и информационные технологии управления предприятием в условиях нестабильностей. Монография. - Луганськ: Вид-во СНУ ім. В. Даля, 2006. – 236 с.

168. Рамазанов С.К., Степаненко О.П., Тимашова Л.А. Методи антикризового управління: Монографія. – Луганськ: Вид-во СНУ імені В.Даля, 2004. – 192 с.

169. Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика издательство "Гелиос АРВ", 2006. – 240 с.

170. Рахматуллин Р.К. Особенности ценообразования на продукцию сельского хозяйства в условиях развитой рыночной экономики // ИНИОН РАН «Новая литература по социальным и гуманитарным наукам. Депонированные научные работы», раздел «Экономика». – № 11. – 1999.

171. Рейдерство : витоки, процедури, способи запобігання : монограф. / О.А. Бурбело, Г.В. Козаченко, Ю.С. Погорелов, С.О. Бурбело ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. − Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. − 184 с.

172. Рейдерство в Україні: загрози та шляхи протидії. — К., 2010. — 148 с.

173. Рейдерство как социально-экономический и политический феномен современной России. Отчет о качественном социологическом исследовании. Исследование центра политических технологий 20.05.2008 // сайт Компромат.ш [Электронный ресурс]. Режим доступа: http://compromat.ru/main/mixl/raiderycpt.htm

174. Рейдерство шляхом банкрутства: поради щодо запобігання [Електронний ресурс]. – Офіційний сайт щотижневої інформаційно-правової газети «Правовий тиждень». – Режим доступу: http://legalweekly.com.ua/index.php?id=16061&show=news&newsid=121409.

175. Ризики, безпека, кризи і сталий розвиток в економіці: методології, моделі, методи управління та прийняття рішень : Кол. монографія / Під заг. ред. проф. С.К. Рамазанова. − Луганськ : Вид-во «Ноулідж», 2012. − 948 с.

176. Роль страхування у забезпечені економічної безпеки : монографія / [О.А. Бурбело, С.В. Єськов, С.М. Андросов, О.М. Заєць] ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2011. – 176 с.

177. Румянцев В., Путятина Л. Методологические проблемы адаптации товаропроизводителей к рынку // Проблемы теории и практики управления, 1994. –№6. – С. 69–73.

178. Савицкая Г.В. Анализ хозяйственной деятельности предприятий. – М.: Экоперспектива, 2007. – 301 с.

179. Садердинов А.А., Федулов А.А., Трайнев В.А. Информационная безопасность предприятия. Учебное пособие. -"Дашков и Ко", 2004. - 336 с.

180. Садовский В.Н. Основания общей теории систем. М.: Наука, 1974. – 254 с.

181. Сайт государственной службы специальной связи и защиты информации Украины [Электронный ресурс] http://www.dstszi.gov.ua.

182. Северин В. А. Комплексная защита информации на предприятии. Учебник. - Городец, 2008. – 124 с.

183. Семкин А. Н., Семкин С. Основы правового обеспечения защиты информации. - "Горячая линия-Телеком", 2008. – 238 с.

184. Сенчагов В.К. Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. 2-е изд. – М.: Дело, 2005. – 896 с.

185. Серебровский В. И. Избранные труды по наследственному и страховому праву / В. И. Серебровский. – М.: Статут (в серии «Классика российской цивилистики»), 1997. – 442 с.

186. Симаков С. Рейдерство по-украински (краткий очерк) // Юридичний радник. – 2006. – № 6 (14). – С. 23-25.

187. Симонов С. В. Методология анализа рисков в информационных системам//Конфидент. – 2011. – № 1. – С. 48-53.

188. Симонов СВ. Технологии аудита информационной безопасности// Конфидент. Защита информации. – 2008. – № 2. - С. 36-41.

189. Система управления информационной инфраструктурой-предприятия: [Электронный ресурс]: http://www.ecoprog.ru/suii. shtml. 16.04.2005.

190. Система управления информационной инфраструктурой: [Электронный ресурс] : http://www.incom.ua/products/Software integ ration/Standart- software-solutions/sysmanage/index.shtml, 16.10.2005.

191. Скиданова Л.А. Рейдерство как социально-экономический феномен: автореферат диссертации на соискание ученой степени кандидата социологических наук: специальность 22.00.03 «Экономическая социология и демография» / Скиданова Лилия Алексеевна; [Моск. гос. ун-т им. М. В. Ломоносова]. - Москва: 2010. - 23 с.

192. Сметанкина Ю. Что такое рейдерство? / Ю. Сметанкина // Власть. – 2007. – № 1. – С. 37-42.

193. Современные подходы к управлению информационной инфраструктурой: [Электронный ресурс]: www.computel.ru, 17.11.2004.

194. Современный экономический словарь [Электронный ресурс] Режим доступа: http://slovari.yandex.ru/dict/economic/article/

195. sesl/ses-2317.htm

196. Старкова Н.О., Костецкий А.Н. Проблемы количественной оценки объема интеллектуальных активов фирмы: [Электронный ресурс]: http://intel-assetshl.ru/artieles/articlell.htm, 28.05.2005.

197. Старостіна А. Підприємницькі ризики та регуляторна політика держави / А. Старостіна, В. Кравченко // Вісник Київського національного університету імені Т. Шевченка. − 2009. − № 113-114. − С. 11-14.

198. Степанов Е., Корнеев И. Защита информации в офисе. – М.: "ТК Велби", 2007. - 336 с.

199. Страхування в системі економічної безпеки / Керівник авт. кол. проф. Р.І. Тринько (монографія). – Львів: ЛьвДУВС, 2008. – С. 90.

200. Страхування: Підручник / Керівник авт. кол. і наук. ред. С. С. Осадець. — К: КНЕУ, 2006. — 528 с.; Плиса В. Й. Страхування: підручник / В. И. Плиса. — К: Кравале, 2010 — 472 с.

201. Стрелкова Е.. Интеграция данных предприятия//Открытые системы, 2003. Апрель. С. 58-61.

202. Тамбовцев В. Л. Экономическая безопасность хозяйственных систем : структура проблемы / В. Л. Тамбовцев // Вестник МГУ. Сер. 6. Экономика. – 1995. – С. 14-18.

203. Тарханова З.Э. Функционирование института рейдерства в РФ: автореферат дис.... кандидата экономических наук: 08.00.01 / Тарханова Зарина Эльбрусовна; [Место защиты: Сев.-Осет. гос. ун-т им. К.Л. Хетагурова]. - 22 с.

204. Тельнов Ю. Ф. Реинжиниринг бизнес-процессов. - М.: МЭСИ, 1999. -106 с.

205. Тивончук І. О. Особливості рейдерства в Україні / І. О. Тивончук, Г. Я. Глинська // Вісник Національного університету «Львівська політехніка». Менеджмент та підприємництво в Україні : етапи становлення і проблеми розвитку : зб. наук. праць. – Львів : НУ «Львівська політехніка», 2008. – № 624. – С. 146–150.

206. Тимофєєва Т.О. Розробка механізму щодо забезпечення економічної безпеки залізничного транспорту: автореф. дис. канд. екон. наук: 08.00.03 — економіка та управління національним господарством / Т.О. Тимофєєва; Укр. держ. акад. залізн. трансп. — Х., 2009. — 20 с.

207. Тимошенко О.В. Страхування фінансових ризиків як фактор забезпечення фінансових ресурсів підприємства / О.В. Тимошенко // Економічний простір. − 2013. − № 71. − С. 135-143.

208. Тіньова економіка: сутність, особливості та шляхи легалізації : [монографія] / [за ред. З. С. Варналія]. – К. : НІСД, 2006. – 576 с.

209. Троников И.Б. Пазухин А.В., Коробейникова Н.А. Применение интеллектуальных систем при управлении производством. В книге "Труды международных научно-технических конференций "Интеллектуальные системы (IEEE AIS'06)" и "Интеллектуальные САПР (CAD- 2006)". Научное издание в 3-х томах. М.:Изд-во Физико-математической литературы, 2006, Т.2.-580 с.

210. Троников И.Б., Извозчикова В.В., Матвейкин И.В. и др. Концептуальная модель управления предприятием// Изв. вузов. Приборостроение. 2008. – Т. 51. – № 5. – С. 26-29.

211. Троников И.Б., Коробейников А. Г., Нестерова Н. А., и др. Процессный подход при управлении качеством продукции на предприятиях, осуществляющих выпуск электронного приборного оборудования // Датчики и системы. 2008. – № 6. – С. 31-34.

212. Уемов А.И. Системный подход и общая теория систем. М.: Наука, 1978. – 196с.

213. Фаенсон, М.И. Рейдерство (недружественный захват предприятий): практика современной России / М.И. Фаенсон, А.А. Пиманова. – М.: Издательство «Альфа-Пресс», 2007. – 120 с.

214. Федоров А.Ю. Рейдерство и корпоративный шантаж: монография. – М.: Волтерс Клувер, 2010. –480 с.

215. Ханк Дж., Райтс А. Бизнес-прогнозирование, 7-е издание: Пер. с английского. – М.:"Вильямс", 2003. – 656с.

216. Ходжсон Дж. Экономическая теория и институты. – М.: Дело, 2003. – 464 с.

217. Цивільне право України: В 2-х томах. Т.2. Підручник / За ред. д-ра юрид. наук, проф. Є.О. Харитонова; канд. юрид. Наук Н.Ю. Голубєвої. – Х.: ТОВ «Одіссей», 2008. – С. 402.

218. Цивільний кодекс України // Відомості Верховної Ради України. − 2003. − № 40-44. − С.356.

219. Цінні папери: підручник / За ред. В.Д. Базилевича. – К.: Знання, 2011. – 161 с.

220. Шаваев А.Г. Система борьбы с экономической разведкой. М.: Изд-во «Правовое просвещение». 2000. – 240 с.

221. Шапочка М. К., Рибіна О.І. Проблеми та напрямки реструктуризації залізничної інфраструктури // Вісник Хмельницького національного університету. – 2010. – № 2, т.2. – С.44-48.

222. Шахов В.В. Страхование. – М: ЮНИТИ, 1997. – 15 с.

223. Шевченко І. Особливості формування економічної безпеки підприємства // Наука молода. - 2010. - №10. – С. 178-181.

224. Шелупанов А.А., Шумский А.А. Системный анализ в защите информации. - Гелиос АРВ", 2005.- 224 с.

225. Шемчук В. Рейдерство та корупція / В. Шемчук // Вісник прокуратури. – 2006. – № 11. – С. 14.

226. Шинкаренко В.Г. Економічна безпека автотранспортних підприємств та їхня роль у роботі господарського комплексу України / В.Г. Шинкаренко // Збірник наукових праць НТУ. — 2009. Режим доступу до статті:http://www.nbuv.gov.ua/portal/natural/Vntu/

227. 2009_19_1/pdf/81.pdf.10.

228. Шлемко В.Т., Бінько І.Ф. Економічна безпека України: сутність і напрямки забезпечення. – К.: НІСД, 1997. – С. 3.

229. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. — СПб, 1999. – 36 с.

230. Шніт А.В. Про посилення законодавчої бази антирейдерської спрямованості // Європейські перспективи. – 2011. - № 1. – Ч.1. – С. 117-121.

231. Экономика и организация безопасности хозяйствующих субъеков, 2-е изд. – СПб.: Питер, 2004. – 288 с.

232. Экономическая безопасность Российской Федерации: учеб. для вузов: в 2 ч. – СПб., 2001. – С. 72-73.

233. Яременко О.Ф. Аспекти побудови паспорта загроз підприємства // Вісник Хмельницького національного університету. – 2011. – №2. – Т.1. – С. 14-20.

234. Ярочкин В.И. Коммерческая информация фирмы. - М.: Ось-89, 1997. – 168 с.

235. Ярочкин В.И. Секьюритология - наука о безопасности жизнедеятельности. - М.: "Ось-89", 2000. – 151 с.

236. Ястремський О.І. Моделювання економічного ризику. – К.: Либідь, 1992. – 176 с.

237. Aalen O.O., Murka C., Gjessing H.K. Survival and event history analysis: A process point of view. – New York, NY: Springer, 2008.

238. An Introduction to Computer Security: 'Ibe NTST Handbook. Draft — National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. 2010.

239. Barber S., Jennison C. Symmetric tests and confidence intervals for survival probabilities and quantiles of censored survival data // Biometrics - 1999, vol. 55, pp. 430–436.

240. Common Criteria for Information Technology Security evaluation. Version 1.0, 96,01.31.

241. Ettore Croci. The Market for partial corporate control in Europe: The evidence about corporate raiders. 2004. [Электронный ресурс] / Ettore Croci. – Режим доступу: http://www.eea-esem.com/papers/eea-esem/2004/185/ettore_croci_corp_raiders.pdf.

242. Information Technology Security Evaluation Criteria (ITSEC). Harmonized Criteria of France- Germany- the Niderhmds - the United KingDom. Department of Trade and Industry, London, 2010

243. Kaufman, Arnold, and Gupta, Madan. M. Introduction lo Fuzzy Arithme- lic/Thomson Computer Press, 2011.

244. Lawrence M. Salinger. Encyclopedia of white-collar and corporate crime. — SAGE, 2005. — P. 263.

245. The OLAP Report: Applications. WebSphere MQ Integrator. Programming Guide. Threats to Computer Systems: an Overview - Computer Systems Laboratory Bulletin, March 2009

246. The OLAP Report: Applications. WebSphere MQ Integrator. Programming Guide.

247. Threats to Computer Systems: an Overview - Computer Systems Laboratory Bulletin, March, 2009.

248. Title insurance in the United States // [Електронний ресурс] http://en.wikipedia.org/wiki/Title_insurance_in_the_United_States.

249. W.E Hawden.- Functional program testing and analysis - N.Y.: McCrawHiil, 2011.

250. Zaiets O.M. Title Insurance − Method of Counteraction of Corporate Raid / O.M. Zaiets // European Reforms Bulletin. − 2015. − № 1. − P. 48-51.

Наукове видання

Колектив авторів:
Бурбело О.А., Рамазанов С.К.,
Заєць О.М., Гудіма Т.С., Кузьменко О.М

Науковий редактор:
Бурбело О.А. – Східноукраїнський національний університет імені Володимира Даля, доктор економічних наук, професор.
Рамазанов С.К. – завідувач кафедрою економічної кібернетики Східноукраїнського національного університету імені Володимира Даля, заслужений діяч науки і техніки України, доктор економічних наук, доктор технічних наук, професор.

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА В УМОВАХ РЕЙДЕРСЬКИХ ЗАГРОЗ

Монографія

Українською мовою

В авторській редакції

Здано до набору 7.12.2015. Підписано до друку 10.12.2015.
Формат 60х84 1/16. Папір офсетний. Гарнітура Times.
Друк лазерний . Умов. друк. арк. 16,62. Обл.-вид. арк. 17,91.
Наклад 500 прим. Вид. № 3038. Зам. № 1508.
Ціна договірна

Видавництво «СНУ імені Даля»
Свідоцтво про реєстрацію серія КВ № 15607-4079 ПР від 18.08.2009 р.
93400, м. Сєвєродонецьк, проспект Радянський 59-а
тел. +38(06452) 40342