

**ФІНАНСОВА БЕЗПЕКА СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА
В УКРАЇНІ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ**

Леся Яструбецька

ЛЕСЯ ЯСТРУБЕЦЬКА



**ФІНАНСОВА БЕЗПЕКА СУБ'ЄКТІВ
ПІДПРИЄМНИЦТВА В УКРАЇНІ
В УМОВАХ ГІБРИДНИХ ЗАГРОЗ**



**FINANCIAL SECURITY OF BUSINESS ENTITIES IN UKRAINE
IN CONDITIONS OF HYBRID THREATS**

LESYA YASTRUBETSKA

LESYA YASTRUBETSKA



**FINANCIAL SECURITY
OF BUSINESS ENTITIES IN UKRAINE
IN CONDITIONS OF HYBRID THREATS**





*Львівський національний університет
імені Івана Франка*

*Присвячено Героям України,
які віддали своє життя в боротьбі
за рідну землю та захисникам, які сьогодні
ведуть боротьбу проти окупаційної
російської армії, а також усім незламним
і нескореним в протидії гібридним агресіям*

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ЛЕСЯ ЯСТРУБЕЦЬКА

**ФІНАНСОВА БЕЗПЕКА СУБ'ЄКТІВ
ПІДПРИЄМНИЦТВА В УКРАЇНІ
В УМОВАХ ГІБРИДНИХ ЗАГРОЗ**

Монографія

Львів
2022

УДК [658.14-027.45:330.131.] (477)

Рецензенти:

доктор економічних наук, професор Є. Є. Іонін
(Донецький національний університет імені Василя Стуса);
доктор економічних наук, професор Ю. В. Пасічник
(Національний науковий центр “Інститут аграрної економіки”);
доктор економічних наук, професор В. Ф. Піхоцький
(Територіальне управління Рахункової палати по Львівській, Волинській та
Тернопільській областях).

*Рекомендовано до друку Вченою радою Львівського національного
університету імені Івана Франка
(протокол № 16/6 від 30.06.2021 року)*

Яструбецька Л. С.

Фінансова безпека суб'єктів підприємництва в Україні в умовах гібридних загроз:
монографія. Львів : ЛНУ ім. Івана Франка, 2022. 370 с.

ISBN 978-617-10-0686-7

У монографії обґрунтовано теоретико-методологічні та практичні аспекти забезпечення фінансової безпеки суб'єктів підприємництва в Україні. Виявлено вплив гібридних загроз на рівень фінансової безпеки ділових одиниць й проведено аналіз таких гібридних фінансових конфліктів в підприємницькій діяльності, як рейдерство, фінансове шахрайство працівників, недобросовісна конкуренція, корупція. Досліджено деформації інформаційного середовища суб'єктів господарювання в умовах діджиталізації і деструктивні інституційні трансформації внаслідок війни. Розроблено рекомендації щодо протидії гібридним загрозам у функціонуванні суб'єктів підприємництва й визначено стратегічні напрями зміцнення їх фінансової безпеки.

Монографія призначена для наукових працівників, викладачів, аспірантів, студентів, фінансистів-практиків, державних службовців, а також усіх, хто цікавиться проблемами управління фінансовою безпекою суб'єктів підприємництва в Україні.

УДК [658.14-027.45:330.131.](477)

© Яструбецька Л. С., 2022

© Львівський національний університет
імені Івана Франка, 2022

ISBN 978-617-10-0686-7

ЗМІСТ

ПЕРЕДМОВА	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УМОВАХ ГІБРИДНИХ ЗАГРОЗ	11
1.1. Сутність та класифікація інтересів суб'єктів підприємництва ...	11
1.2. Фінансова безпека як інтегральна характеристика суб'єктів підприємництва	19
1.3. Загрози фінансовій безпеці суб'єктів підприємництва	34
1.4. Гібридні фінансові конфлікти суб'єктів підприємництва як дестабілізуючий чинник фінансової безпеки	44
РОЗДІЛ 2. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ЧИННИКІВ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ	81
2.1. Концептуальні підходи до вивчення чинників фінансової безпеки суб'єктів підприємництва в Україні	81
2.2. Використання сучасних методів виявлення закономірностей у забезпеченні фінансової безпеки суб'єктів підприємництва	88
2.3. Метод історичної абдукції в дослідженні гібридних фінансових конфліктів	95
2.4. Вибір інструментів аналізу та прогнозування стану фінансової безпеки суб'єктів підприємництва в умовах гібридних загроз.....	103
РОЗДІЛ 3. СТРУКТУРНО-КОМПОНЕНТНИЙ АНАЛІЗ ГІБРИДНИХ ФІНАНСОВИХ КОНФЛІКТІВ У СФЕРІ ФУНКЦІОНУВАННЯ ІНСТИТУТУ ВЛАСНОСТІ В УКРАЇНІ	118
3.1. Фінансове шахрайство працівників як загроза безпечному функціонуванню суб'єктів підприємництва в Україні	118
3.2. Рейдерство як конфліктна форма перерозподілу власності в Україні	144
3.3. Недобросовісна конкуренція як системна проблема забезпечення фінансової безпеки суб'єктів підприємництва в Україні.....	176
3.4. Критичні наслідки фінансових небезпек у формі корупції.....	186

РОЗДІЛ 4. ВПЛИВ ДЕСТРУКТИВНИХ ІНСТИТУЦІЙНИХ ТРАНСФОРМАЦІЙ НА ФІНАНСОВУ БЕЗПЕКУ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ	199
4.1. Інформаційне середовище суб'єктів фінансових відносин як об'єкт захисту	199
4.2. Оцінювання впливу персоналу на інформаційну складову фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних загроз.....	208
4.3. Чинник кіберзлочинності в гібридних фінансових конфліктах.....	214
4.4. Військові агресії як багатомірна криза забезпечення фінансової безпеки суб'єктів підприємництва в Україні	225
РОЗДІЛ 5. КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА СТРАТЕГІЧНІ ОРІЄНТИРИ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ	235
5.1. Стратегічне оцінювання рівня фінансової безпеки суб'єктів підприємництва в Україні	235
5.2. Концептуальні аспекти формування механізму управління фінансовою безпекою суб'єктів підприємництва в Україні в умовах гібридних загроз.....	245
5.3. Типові сценарії впровадження організаційно-економічних заходів протидії гібридним фінансовим конфліктам в діяльності суб'єктів підприємництва в Україні	257
5.4. Пріоритетні напрями трансформації інституційно- правового забезпечення фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних загроз	289
ВИСНОВКИ	305
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	311
ДОДАТКИ	

ПЕРЕДМОВА

Глобальна ситуація у сфері безпеки зазнала суттєвих і радикальних змін, пов'язаних передусім з появою нового типу загроз безпеці міжнародного середовища, окремих країн та суб'єктів підприємництва й зумовивши перехід до використання гібридних важелів впливу на досягнення бажаних результатів фінансових конфліктів. В Україні це пов'язано з багатолітньою гібридною війною росії, що перейшла в гостру форму – військову агресію, спричинивши незворотні інституційні трансформації в суспільстві через виникнення новітніх загроз, породжених воєнним станом, досвіду протидії яким ще повною мірою не напрацьовано. Ця гібридна війна прямо чи опосередковано зумовила необхідність переформатування підходів до управління фінансовою безпекою як держав, так і суб'єктів підприємництва. Водночас складність загроз фінансовій безпеці ділових одиниць значною мірою посилено фінансовою кризою та невизначеністю, зумовленою постпандемічним періодом. Окрім того, зниження рівня фінансової безпеки суб'єктів господарювання спричиняють такі деструктивні чинники, як недосконалість нормативно-правового забезпечення фінансової діяльності вітчизняних суб'єктів підприємництва в умовах трансформаційних змін, неефективність механізму захисту прав власників, наявність корупційних схем на різних ланках державної влади, випадків недобросовісної конкуренції та фінансового шахрайства в підприємницькій діяльності, зростання рівня тінізації економіки. З огляду на сказане вище, вирішення проблем, пов'язаних із забезпеченням фінансової безпеки суб'єктів господарювання в умовах гібридних загроз, на сьогодні набуває особливої актуальності.

Дослідженню протистоянь гібридного типу присвятили свої праці такі вітчизняні та іноземні вчені: О. Базалук, В. Бірчак, В. В'ятрович, В. Горбулін, Р. Додонов, Є. Магда, В. Мартинюк, М. Нікіфоров, С. Рябенко, Р. Бернсбі, Е. Броу, Е. Геллендорн, Х. Е. Гоеманс, Ф. Гофман, К. Каунерт, Дж. А. Ларсен, Г. Лассвелл, Г. Ласконьяріас, В. Мічлін-Шапір, А. Рач, Ш. Р. Рівз, Е. Фолі, О. Фрідман та інші.

Вагомий внесок у розвиток теорії і практики забезпечення фінансової безпеки на рівні держави зробили такі науковці: Г. Аніловська, В. Антипов, О. Барановський, З. Варналій, Д. Ванькович, О. Воробйова,

В. Гаращук, В. Геєць, Н. Демчишак, В. Дем'янишин, Е. Дмитренко, С. Дмитров, А. Єжов, А. Єпіфанов, М. Єрмошенко, Я. Жаліло, З. Живко, С. Задорожний, О. Замасло, Є. Іонін, О. Колодізев, В. Корнєєв, М. Крупка, М. Мельник, В. Молодик, А. Мухатаєв, Е. Невмержицький, Д. Нікитенко, С. Онищенко, Г. Пазєєва, О. Підхонний, В. Піхоцький, В. Предборський, О. Пугач, Б. Пшик, І. Рєвак, С. Рєверчук, О. Саєнко, Г. Ситник, О. Терещенко, О. Терещук, М. Флейчук, В. Шлемко, М. Штангрет та ін.

Значний вклад у вирішення проблем забезпечення фінансової безпеки суб'єктів підприємництва зробили такі вчені: Д. Андрєєв, Б. Андрушків, О. Безух, Я. Бережний, Ю. Берлач, М. Білик, І. Бланк, О. Бойкевич, Л. Буряк, З. Варналій, Т. Васильців, Ю. Вовк, В. Волошин, О. Гарагонич, О. Глущенко, В. Грушко, І. Дмитрієв, В. Домбровський, Р. Друзін, П. Дудкін, А. Єфименко, Д. Зеркалов, М. Камлик, В. Каркавчук, Н. Кирич, В. Коваленко, М. Кужелев, В. Кузьомко, О. Ляшенко, Л. Малюта, І. Медведєва, І. Мойсеєнко, Т. Мостенська, Н. Невмержицька, В. Нєстеренко, Н. Норіцина, О. Пластун, М. Погосова, А. Поддерьогін, І. Сівчук, О. Сороківська, О. Стащук, І. Стойко, М. Суганяка, В. Фучеджи, Г. Швиданенко та ін.

Незважаючи на широке висвітлення у науковій літературі проблем, пов'язаних із забезпеченням фінансової безпеки як на рівні держави, так і на мікроекономічному рівні, не всі аспекти цієї складної багатоаспектної проблематики з'ясовані, а окремі з них залишаються недостатньо розробленими й потребують подальших наукових досліджень. Особливо це стосується уточнення понятійно-термінологічного апарату, зокрема визначення сутності фінансової безпеки суб'єктів підприємництва та ролі гібридних загроз в її забезпеченні. Актуальним є дослідження рейдерства, як одного з найбільш небезпечних гібридних фінансових конфліктів в підприємницькій діяльності, розкриття об'єктів, схем і технологій рейдерських атак та формування теоретико-методологічного й практичного інструментарію з організації протидії протиправним захопленням ділових одиниць в Україні. Невідкладного вирішення в умовах діджиталізації вимагають проблеми фінансової безпеки суб'єктів підприємництва, пов'язані з кадровими та інформаційними загрозами, які своєю чергою, зумовлюють виникнення й поширення фінансового шахрайства, випадків корупції і недобросовісної конкуренції. Потребують вивчення питання формування системи управління фінансовою безпекою

суб'єктів підприємництва на рівні держави й на рівні окремих ділових одиниць, зокрема розроблення інструментів їх стратегічного оцінювання в умовах гібридних загроз.

Результати дослідження подані у п'яти розділах, в яких послідовно висвітлено нові підходи до обґрунтування теоретико-методологічних основ, виявлення особливостей та аналізу чинників забезпечення фінансової безпеки суб'єктів підприємництва й розроблення концептуальних засад і стратегічних орієнтирів управління фінансовою безпекою ділових одиниць в Україні в умовах гібридних загроз.

У першому розділі узагальнено та поглиблено сучасний понятійно-термінологічний апарат забезпечення фінансової безпеки суб'єктів підприємництва, розкрито взаємозв'язки макро і мікрорівневих складових фінансової безпеки. Здійснено класифікацію загроз фінансовій безпеці ділових одиниць й обґрунтовано вплив загроз гібридного типу на забезпечення її належного рівня.

Другий розділ розкриває концептуально-методологічні основи вивчення чинників забезпечення фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних загроз. Відтак, аргументовано необхідність врахування при дослідженні проблем фінансової безпеки як фінансового, так і соціально-психологічного підходів та обґрунтовано вибір інструментів оцінювання та прогнозування стану фінансової безпеки ділових одиниць.

У третьому розділі здійснено структурно-компонентний аналіз гібридних фінансових конфліктів у сфері функціонування інституту власності в Україні, зокрема досліджено фінансове шахрайство працівників, рейдерство, випадки недобросовісної конкуренції та корупції у підприємницькій діяльності.

Четвертий розділ присвячений дослідженню впливу діджиталізації і деструктивних інституційних трансформацій на фінансову безпеку ділових одиниць, розкриттю кадрової складової й чинника кіберзлочинності в гібридних фінансових конфліктах.

У завершальному розділі визначено концептуальні засади й стратегічні орієнтири управління фінансовою безпекою суб'єктів підприємництва в Україні. Відтак, запропоновано напрями стратегічного оцінювання рівня фінансової безпеки ділових одиниць й подано пропозиції щодо формування механізму управління їх фінансовою безпекою в умовах

гібридних загроз. Обґрунтовано інструменти й методи підвищення ефективності державного регулювання в даній сфері з метою зміцнення фінансової безпеки суб'єктів підприємництва.

Розроблені в монографії концептуально-методологічні та теоретико-організаційні підходи до розуміння чинників забезпечення фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних загроз дали змогу обґрунтувати окремі напрями протидії гібридним фінансовим конфліктам в підприємницькій діяльності, що може бути корисним для наукових працівників, викладачів, аспірантів, студентів, державних службовців, фінансистів-практиків, фахівців у галузі фінансової безпеки та усіх інших читачів, які цікавляться актуальними проблемами фінансової безпеки суб'єктів підприємництва в Україні.

РОЗДІЛ 1.

ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1. Сутність та класифікація інтересів суб'єктів підприємництва

Кожне суспільство характеризується складністю переплетення різноманітних інтересів, рівень взаємоузгодженості яких зумовлює подальший розвиток як окремих індивідів та суб'єктів підприємництва, так і держави та суспільства.

У науковій літературі на сьогодні ще не вироблено єдиного погляду на розуміння сутності поняття “інтерес”. Інтереси пов'язують з потребами, однак не ототожнюють з ними. Зокрема, є тлумачення інтересу як усвідомленої потреби або системи потреб [195, с. 9]. Згідно з таким підходом, інтерес, відображаючи єдність усіх потреб, спрямований на відносини й життєві умови загалом, тоді як потреби орієнтовані на предметні цілі.

У сучасних економічних словниках інтересом визначено поняття, що характеризує важливе, значуще, потрібне для індивіда, сім'ї, колективу, групи, класу, нації, суспільства в цілому [52, с.151]. Одночасно інтерес тлумачать як головну рушійну силу економічних суб'єктів, яка має форму матеріальних, духовних, грошових та майнових інтересів.

Вивчення інтересів ділових одиниць набуває виняткової актуальності в умовах довготривалого кризового періоду, зумовленого пандемією Covid-19 та багатолітньою гібридною війною РФ в Україні. Кризові явища змінюють як взаємні очікування учасників ринку в розвитку критичних процесів, так і співвідношення в економічних інтересах різних груп суб'єктів економічних відносин.

У фаховій вітчизняній літературі нами виявлено низку наукових підходів до визначення поняття “економічні інтереси”, зокрема такі:

– економічні інтереси – категорія, що відображає об'єктивно зумовлені матеріальні потреби людей, що втілюються в життя через активну діяльність, є її спонукальними мотивами, рушійною силою в досягненні певних економічних результатів, що відповідають рівню

розвитку продуктивних сил і призначені для задоволення матеріальних потреб [52, с.151–152].

– економічний інтерес – реальний, зумовлений відносинами власності та принципом економічної вигоди мотив і стимул соціальних дій щодо задоволення динамічних систем індивідуальних потреб суб'єктів господарської діяльності [210, с.50];

– економічні інтереси – усвідомлене прагнення економічних суб'єктів задовольняти певні потреби, що є об'єктивним спонукальним мотивом їхньої господарської діяльності [73, с. 51].

Різноманіття тлумачень поняття “економічні інтереси, запропоноване науковцями, дає змогу зробити висновок, що передусім ці інтереси передбачають прагнення суб'єктів господарювання задовольняти певні потреби, усвідомлення яких стає спонукальним мотивом до пошуку способів їх забезпечення і досягнення мети. По-друге, реалізація економічних інтересів зумовлена місцем їхніх носіїв у системі соціально-економічних відносин і є суб'єктивно-об'єктивним процесом цілеспрямованої економічної діяльності, у процесі якої конкретний суб'єкт намагається зберегти або поліпшити економічний стан, підвищити свій соціальний статус, забезпечити реалізацію потреб, характер і способи задоволення яких детерміновані наявною системою суспільних відносин.

У структурі економічних інтересів залежно від суб'єктів виділяють інтереси індивіда, корпорації, суспільства, держави. Водночас реальним носієм будь-якого інтересу завжди є індивід. На думку О. Підхонного, самостійного явища інтересу групи не існує [195, с. 9]. Погоджуємося з баченням ученого, що, попри те, що різні приватні інтереси членів групи, взаємодіючи, породжують певний усереднений результат, його не можна розглядати просто як “середньозважену величину” різних інтересів. Рівень інтересу однієї групи, зазвичай, відрізняється від рівня інтересу іншої групи, суспільства загалом. Окрім того, груповий інтерес не є суттєвою й стабільною характеристикою, оскільки зі зміною складу групи або інтересів хоча б одного її члена рівень групового інтересу також змінюється. Водночас узгодження економічних інтересів ділових одиниць між собою є запорукою економічного розвитку. Адже економічне зростання є показником дієвості процесів саморегулювання в довготривалому періоді, оскільки їхня основа – це узгодження інтересів приватних економічних суб'єктів із суспільним інтересом та

між собою, а вони, відповідно, ґрунтуються на потребі постійного росту [79, с. 45].

Щодо економічних інтересів суб'єктів підприємництва, то важливою складовою їх частиною є фінансові інтереси. Під час визначення фінансових інтересів економічних суб'єктів учені, які вивчають проблеми фінансової безпеки, наголошують на їхній специфіці. На їхню думку, фінансові інтереси є проявом економічних відносин підприємства та суперечностей його фінансової діяльності [75, с. 23].

Погоджуємось із баченням щодо розуміння фінансових інтересів тих науковців, які враховують чинник безпеки у визначенні цього поняття. Зокрема, І. Бланк вважає, що фінансові інтереси суб'єктів підприємництва є формою прояву їхніх об'єктивних потреб у сфері фінансової діяльності, збалансованих з потребами інших суб'єктів економічних відносин, задоволення яких забезпечує реалізацію основних цілей фінансової діяльності на кожному етапі фінансового розвитку [19, с. 27–28]. Вважаємо такий підхід доцільним та важливим у контексті забезпечення фінансової безпеки, оскільки науковець акцентує на важливості збалансування інтересів ділових одиниць з інтересами інших учасників ринку, що є невід'ємною складовою зміцнення їхньої фінансової безпеки.

Чинник безпеки врахувала також Т. Загорельська, яка вважає, що фінансові інтереси суб'єктів підприємництва, з одного боку, є орієнтиром їх розвитку, а з іншого, – вони відображають характер економічних відносин та їхню потребу у безпечному й перспективному розвитку в нестабільному зовнішньому середовищі [82, с.169].

Відтак, фінансові інтереси є чинниками виникнення й розвитку фінансових відносин та водночас характер цих відносин визначає рівень реалізації фінансових інтересів.

Різноманіття тлумачень змісту поняття “фінансові інтереси” дає змогу зробити висновок, що ця категорія має складну, багатогранну та різнопланову природу, дослідження якої допомогло нам виділити низку таких основних його сутнісних характеристик:

- фінансові інтереси пов'язують об'єкт, тобто те, на що спрямований інтерес, і суб'єкт – того, хто конкретно має цей інтерес;
- суб'єктами фінансових інтересів ділових одиниць є особи, що здійснюють контроль їхньої фінансово-господарської діяльності. До них

належать власники, керівництво чи інші уповноважені особи суб'єктів підприємництва;

– фінансові інтереси відображають потреби ділових одиниць, задоволення яких забезпечує реалізацію основних цілей їхньої фінансово-господарської діяльності;

– фінансові інтереси зумовлені об'єктивною потребою забезпечення необхідними фінансовими ресурсами для здійснення ефективної фінансово-господарської діяльності;

– реалізація фінансових інтересів є результатом спільного бачення власників та менеджменту суб'єкта підприємництва;

– фінансові інтереси реалізуються завдяки використанню певних фінансових інструментів (технологій);

– фінансові інтереси суб'єктів підприємництва є змінними в часі, їх уточнюють на кожному з етапів їхнього розвитку;

– фінансові інтереси ділових одиниць можуть не узгоджуватися з фінансовими інтересами інших суб'єктів мінливого конкурентного ринкового середовища (покупців та замовників, постачальників, ділових партнерів, кредиторів, конкурентів) та інтересами їхніх працівників.

Задля більш повного розуміння змісту поняття “фінансові інтереси” вважаємо доцільним здійснити їх групування за такими класифікаційними ознаками (рис. 1.1):

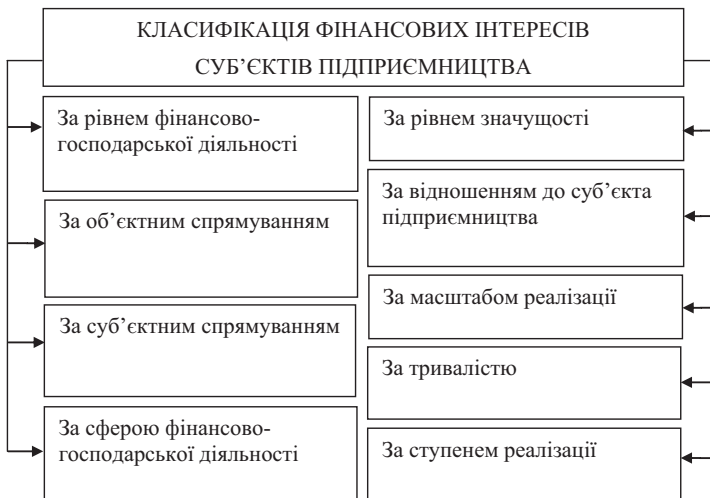


Рис. 1.1. Класифікація фінансових інтересів суб'єктів підприємництва

Джерело: розробила автор

1. За рівнем фінансово-господарської діяльності:
 - фінансові інтереси суб'єкта підприємництва загалом;
 - фінансові інтереси окремих структурних підрозділів;
 - фінансові інтереси окремих проектів.
2. За об'єктним спрямуванням:
 - забезпеченість капіталом;
 - інвестиційна активність;
 - максимізація прибутку;
 - оптимізація відрахувань до бюджету;
 - зростання ринкової вартості акцій.
3. За суб'єктним спрямуванням:
 - фінансові інтереси власників;
 - фінансові інтереси керівництва суб'єкта підприємництва;
 - фінансові інтереси персоналу.
4. За сферою фінансово-господарської діяльності:
 - у сфері інвестиційної діяльності;
 - у сфері кредитної діяльності;
 - у сфері емісійної діяльності;
 - у сфері інноваційної діяльності;
 - в інших сферах фінансової діяльності.
5. За рівнем значущості:
 - головний фінансовий інтерес;
 - пріоритетні фінансові інтереси.
 - другорядні фінансові інтереси.
6. За відношенням до суб'єкта підприємництва:
 - внутрішні фінансові інтереси;
 - зовнішні фінансові інтереси.
7. За масштабом реалізації:
 - оперативні фінансові інтереси;
 - тактичні фінансові інтереси;
 - стратегічні фінансові інтереси.
8. За тривалістю:
 - короткотермінові фінансові інтереси;
 - довготермінові фінансові інтереси
9. За ступенем реалізації:
 - нереалізовані фінансові інтереси;

- частково реалізовані фінансові інтереси;
- реалізовані фінансові інтереси.

Важливим класифікаційним критерієм є рівень значущості фінансових інтересів. Відтак, захист фінансових інтересів суб'єктів підприємництва передбачає передусім чітку ідентифікацію головного та пріоритетних фінансових інтересів. На думку І. Бланка [19, с. 32], головний фінансовий інтерес ділових одиниць безпосередньо пов'язаний з основною метою їхнього функціонування, визначення якої описують моделі фінансового менеджменту (табл. 1. 1.).

Таблиця 1.1

**Моделі визначення головного фінансового інтересу
суб'єктів підприємництва**

№ п/п	МОДЕЛЬ	ХАРАКТЕРИСТИКА	НЕДОЛКИ
1	2	3	4
1.	Модель максимізації прибутку	Ґрунтується на теоретичних підходах класичної економічної теорії, зокрема, на висновку А. Сміта про те, що максимізація прибутку окремих суб'єктів господарювання призводить до максимізації суспільного добробуту. Уперше цю цільову модель сформулював французький економіст А. Курно в 1938 р.	Максимізація прибутку не завжди забезпечує необхідні темпи економічного розвитку підприємств. Високий прибуток може бути використаний на цілі поточного споживання, унаслідок чого підприємство не матиме джерела фінансових ресурсів для розвитку. Окрім того, високий рівень прибутковості може досягатися за високого рівня фінансового ризику, а також у разі погіршення інших показників фінансового стану, генеруючи загрозу банкрутства.
2.	Модель мінімізації трансакційних витрат	Ґрунтується на теоретичних підходах основоположника неінституціоналізму Р. Коуза. Суб'єкт підприємництва розглядають як систему складної мережі комерційних контрактів.	Критерій мінімізації трансакційних витрат не забезпечує комплексної економії ресурсів ділових одиниць. Окрім того, будь-яка економія витрат не може становити глобальну ціль функціонування суб'єктів господарювання, оскільки не пов'язана з розвитком.
3.	Модель максимізації обсягу продаж	Цей цільовий критерій відображає результати ділової активності суб'єктів господарювання, генерує максимізацію їхнього прибутку, сприяє активізації маркетингових зусиль та удосконаленню технології виробництва.	Споживчий вибір товарів є функцією мінливого конкурентного ринкового середовища й може нівелювати зусилля суб'єктів господарювання у ринковому просуванні товарів. Недоліком цієї моделі є також те, що хоча її цільова функція пов'язана зі зростанням доходів ділових одиниць, вона, однак, практично не пов'язана з економією витрат.
4.	Модель максимізації темпів зростання продажів	Цільовою функцією моделі є темпи зростання обсягу продажів. Однак у цій моделі наявні і темпи зростання операційного прибутку, і основні пропорції його розподілу. Перевага цієї моделі – чітке спрямування на стратегічну перспективу.	Модель може успішно функціонувати лише за умови незмінного попиту й цін на продукцію, що в умовах невизначеності, притаманній ринковій економіці, є неможливим.

Продовження таблиці 1.1

5.	Модель забезпечення конкурентних переваг	Відображає результати діяльності практично всіх основних служб суб'єктів підприємництва.	Конкурентна перевага як поняття характеризує відносно становище ділових одиниць у масштабах конкретної галузі, тоді як значна частина середніх і великих підприємств – багатогалузеві.
6.	Модель максимізації доданої вартості	Додана вартість охоплює усі витрати ділових одиниць з виробництва та реалізації продукції, а також прибуток. Перевагою такого підходу є те, що забезпечується максимізація економічних інтересів не лише працівників та керівництва, а й власників суб'єктів підприємництва.	Сфера застосування цільової функції цієї моделі має обмежений характер – її можуть використовувати лише підприємства, що випускають ексклюзивну продукцію. Це пов'язано з тим, що можливий конфлікт інтересів виробників й кінцевих покупців продукції, які не завжди готові платити вищу ціну за продукцію.
7.	Модель максимізації ринкової вартості суб'єкта підприємництва	Модель отримала пріоритетний розвиток у США, Європі, Японії та інших країнах й передбачає, що всі управлінські рішення в будь-якій сфері діяльності ділових одиниць повинні бути спрямовані, на забезпечення постійного зростання їхньої вартості на ринку.	

Джерело: побудовано на основі [19]

Проблема співвідношення та пріоритетності фінансових інтересів суб'єктів підприємництва є дискусійною.

Однак чимало вчених головним фінансовим інтересом ділових одиниць в умовах ринкової економіки вважають максимізацію їхньої ринкової вартості. Дана модель має такі переваги:

- визначає власників як основних суб'єктів у сфері фінансових інтересів;
- інтегрує поточні та перспективні цілі розвитку ділових одиниць, об'єднує цілі та завдання усіх їхніх служб;
- є критерієм ефективності використання капіталу суб'єктів підприємництва;
- забезпечує ефективний контроль інвесторів за діями менеджерів суб'єктів підприємництва шляхом надання більш об'єктивної інформації про результати діяльності порівняно з іншими оцінними показниками.

Одночасно з визначенням головного фінансового інтересу суб'єкта підприємництва вважаємо необхідним окреслення його пріоритетних фінансових інтересів, серед яких важливими є такі:

- достатність фінансових ресурсів на усіх етапах життєвого циклу суб'єкта підприємництва;
- фінансова стійкість суб'єкта підприємництва в процесі його розвитку;
- підвищення рентабельності діяльності;
- високий рівень інвестиційної активності та ефективності інвестицій;
- інноваційність фінансово-господарської діяльності суб'єкта підприємництва;
- нейтралізація загроз фінансово-господарській діяльності суб'єкта підприємництва;
- запобігання фінансовим кризам та швидка ліквідація у випадку їхнього виникнення.

Реалізація визначених фінансових інтересів ділових одиниць потребує окреслення основних завдань для їхнього досягнення (табл. 1.2).

Таблиця 1.2

Завдання для реалізації окремих фінансових інтересів підприємств

ФІНАНСОВИЙ ІНТЕРЕС	ЗАВДАННЯ
Зростання ринкової вартості суб'єкта підприємництва	Зростання ринкової ціни акцій суб'єкта підприємництва
	Поліпшення торгової марки суб'єкта підприємництва
	Підвищення рівня ділової репутації суб'єкта підприємництва
Максимізація прибутку суб'єкта підприємництва	Ефективне податкове планування
	Оптимізація дивідендних виплат
	Стимулювання продуктивності праці
	Розвиток виробництва
	Свочасне і повне повернення кредитів
	Зниження собівартості
Забезпечення суб'єкта підприємництва основним і оборотним капіталом	Забезпечення ефективності комерційної діяльності
	Підвищення рівня рентабельності
	Підвищення рівня ліквідності
Забезпечення суб'єкта підприємництва інвестиціями	Розвиток виробництва суб'єкта підприємництва
	Впровадження інновацій у господарську діяльність

Джерело: розробила автор

Фінансові інтереси ділових одиниць та стратегічна ціль їхньої діяльності є взаємозумовленими та взаємовизначальними. Тому несвоечасність і часткова реалізація головного й пріоритетних фінансових

інтересів або цілковита неможливість їхнього забезпечення можуть не лише призвести до негативних наслідків для поточного функціонування суб'єкта підприємництва і перспектив його фінансових відносин з іншими учасниками ринку, але й перешкодити досягненню стратегічної цілі функціонування загалом.

Відтак, важливим в умовах нових викликів і загроз безпечному функціонуванню суб'єктів підприємництва, спричинених пандемією Covid-19, гібридною війною росії та повномасштабним вторгненням агресора в Україну 24 лютого 2022 року є не лише визначення головного й пріоритетних фінансових інтересів, але й управлінська гнучкість зміни такої пріоритетності в кризових умовах.

1.2. Фінансова безпека як інтегральна характеристика суб'єктів підприємництва

Результати проведеного наукового дослідження розуміння сутності фінансових інтересів суб'єктів підприємництва дали змогу підтвердити їх тісний взаємозв'язок із поняттям “фінансова безпека”, яке своєю чергою перебуває у взаємозв'язку з низкою супутніх безпекових термінів, таких як “національна безпека”, “міжнародна безпека”, “економічна безпека”, “інформаційна безпека”, “кадрова безпека”, “виробнича безпека”, “екологічна безпека” тощо.

Потреба усвідомлення необхідності забезпечення безпеки як захисту інтересів людини і суспільства виникла в момент формування суспільства і держави. З того часу поняття “безпека” постійно еволюціонувало впродовж різних історичних епох та політичних систем. У дослідженнях науковців знайшли своє відображення підходи філософів античності до тлумачення поняття “безпека”, зокрема Платон розумів безпеку “як запобігання шкоди державі” та пропонував створення “соціально стійкої системи безпеки, де б головне місце займав моральний стан суб'єктів діяльності і наголошував, що порушення законів ставить під загрозу безпеку особи, станів та держави”. Аристотель уважав державу, особливо з демократичним ладом засобом гарантування безпеки індивідів та регулювання суспільної діяльності за допомогою законів з метою самозбереження. На думку Епікура, держава й закон є наслідком договору між людьми про їхню взаємну безпеку [109]. Це дає підстави зробити висновок, що

трансформація змісту концепту “безпека” відбувалася внаслідок розвитку філософських, соціологічних та інших учень впродовж усього історичного періоду розвитку людства. В цьому контексті, погоджуємось із думкою вчених [165, с. 22], що безпека передбачає складне соціально-політичне явище, що акумулює в собі багатогранну життєдіяльність, накопичений історичний досвід, зрештою, уподобання і культуру кожної людини (індивіда), суспільства, держави, загалом земної цивілізації.

Тлумачний словник української мови подає визначення безпеки як стану, коли кому-, чому-небудь ніщо не загрожує [272, с. 137].

У сучасних дослідженнях безпеку визначають як стан збереження та захищеності сталого існування та розвитку об’єкта (системи), за якого ймовірність змін, спричинених зовнішніми чи внутрішніми впливами, будь-яких параметрів (характеристик) функціонування є мінімальною [48, с.20].

Подальший розвиток суспільства зумовив потребу розширення поняття “безпека” із виокремленням із нього самостійних об’єктів наукового пізнання, а саме національної й економічної складових. На наш погляд, це вдало аргументував О. Уєвер, який відзначив, що безпека – це здатність суспільства зберігати специфічний характер, незважаючи на умови, що змінюються, та реальні або віртуальні загрози, тобто це здатність підтримувати сталість традиційних схем мови, культури, об’єднань, ідентичності, державних і релігійних практик, враховуючи прийнятні зміни [397, с. 67]. У цьому тлумаченні поняття “безпека” враховано складові, що, на наш погляд, пояснюють зміст національної безпеки.

У вітчизняному законодавстві національну безпеку визначено як “захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз” [243].

Щодо тлумачення поняття “економічна безпека”, то у фаховій літературі існує низка підходів до його розуміння. Зокрема, на думку З. Варналія, економічна безпека є сукупністю взаємопов’язаних структурних елементів з вертикальними (мега-, макро, мезо- та мікрорівнями) та горизонтальними (виробнича, фінансова, інвестиційна, енергетична, науково-технічна, продовольча, соціальна й зовнішньоекономічна безпека) рівнями [26]. Погоджуємося з думкою

вченого, оскільки вважаємо значною перевагою цього підходу врахування інтересів систем різного рівня з одночасним акцентуванням на взаємозв'язку їхніх структурних елементів.

Дослідник М. Єрмошенко визначає економічну безпеку держави як такий стан економічного механізму країни, який характеризується збалансованістю і стійкістю до негативного впливу внутрішніх та зовнішніх загроз, його здатністю забезпечувати на основі реалізації національних економічних інтересів сталий і ефективний розвиток вітчизняної економіки й соціальної сфери [75].

Під економічною безпекою В. Мунтіян розуміє стан захищеності економічних інтересів особи, суспільства і держави, розвитку достатнього оборонного потенціалу, що сприятиме стійкому й ефективному функціонуванню економіки в режимі розширеного відтворення, як створення передумов для підтримки і покращення рівня життя громадян, задоволення корінних інтересів у виробничо-економічній, фінансовій, зовнішньоекономічній, технологічній, енергетичній, продовольчій та інших економічних сферах [163, с. 10]. У цьому визначенні імпонує врахування важливості розвитку достатнього оборонного потенціалу, що на сьогодні, в умовах військової агресії росії набуває нової вагомості й становить пріоритетне значення. Оскільки повномасштабне вторгнення агресора в Україну підтвердило необхідність врахування цієї складової у тлумаченні поняття “економічна безпека” з огляду на те, що наявність достатнього оборонного потенціалу держави є базовою основою зміцнення її безпеки в цілому й економічної, зокрема.

Економічну безпеку держави Г. Пастернак-Таранушенко тлумачить як стан держави, за яким вона забезпечена можливістю створення і розвитку умов для плідного життя її населення, перспективного розвитку економіки у майбутньому та у зростанні добробуту її мешканців [191, с. 99]. На нашу думку, економічна безпека держави полягає не лише у створенні і розвитку умов для нормального життя її населення й перспективного розвитку економіки, її зміст в умовах гібридних агресій та іноземних військових інтервенцій має тлумачитися ширше й охоплювати різні сфери життєдіяльності держави.

Щодо поняття “фінансова безпека”, то ми виявили, що від початку циркулювання цього терміна в науковому обігу значна частина вітчизняних науковців розглядала фінансову безпеку переважно на

макрорівні, відображаючи у формулюванні лише окремі аспекти фінансової безпеки суб'єктів підприємництва. Зокрема, на думку О. Барановського, “фінансова безпека” – це [11, с. 28]:

- важлива складова частина економічної безпеки держави, що ґрунтується на незалежності, ефективності і конкурентоспроможності фінансово-кредитної сфери України, яка відображається через систему критеріїв і показників її стану, що характеризують збалансованість фінансів, достатню ліквідність активів і наявність необхідних грошових і золотовалютних резервів;

- ступінь захищеності фінансових інтересів на всіх рівнях фінансових відносин;

- рівень забезпеченості громадянина, домашнього господарства, верств населення, підприємства, організації, установи, регіону, галузі, сектора економіки, ринку, держави, суспільства, міждержавних утворень, світового співтовариства фінансовими ресурсами, достатніми для задоволення їхніх потреб і виконання зобов'язань;

- стан фінансової, грошово-кредитної, валютної, банківської, бюджетної, податкової, розрахункової, інвестиційної, митно-тарифної та фондової систем, а також системи ціноутворення, для якого характерні збалансованість, стійкість до внутрішніх і зовнішніх негативних впливів, здатність відвернути зовнішню фінансову експансію, забезпечити фінансову стійкість (стабільність), ефективне функціонування національної економічної системи та економічне зростання;

- стан фінансових потоків в економіці, для якого характерна збалансованість і наявність апробованих механізмів регулювання і саморегулювання;

- якість фінансових інструментів і послуг, що запобігає негативному впливу можливих прорахунків і прямих зловживань на фінансовий стан наявних і потенційних клієнтів, а також гарантує (у разі потреби) повернення вкладених коштів.

О. Івашко визначив фінансову безпеку з таких позицій [98, с. 61–66]:

- захищеність фінансових інтересів на всіх рівнях фінансових відносин (з позицій ієрархічності фінансових відносин);

- певний рівень незалежності, стабільності й стійкості фінансової системи країни в умовах впливу на неї зовнішніх і внутрішніх

дестабілізуючих факторів, що становлять загрозу фінансовій безпеці (з позицій рівня фінансової незалежності та стабільності);

- здатність фінансової системи держави забезпечити ефективне функціонування національної економічної системи й стале економічне зростання (з позицій функціонального підходу).

Учені В. Даценко, Н. Шевченко фінансову безпеку держави охарактеризували як такий стан бюджетної, боргової, грошово-кредитної, банківської, валютної систем економіки країни, страхового та фондового ринків, який характеризується стійкістю до внутрішніх і зовнішніх негативних загроз; достатністю та ефективним розподілом фінансових ресурсів держави, здатністю гарантувати ефективне функціонування та розвиток національної економічної системи [58].

На думку Г. П'ятницької, І. Федулової [258], фінансова безпека – це:

- невід'ємна складова економічної безпеки країни (або держави), що характеризує такий стан її фінансової системи, за якого формуються умови для забезпечення банківської, боргової, бюджетної, валютної, грошово-кредитної безпеки та безпеки небанківського фінансового сектора, які необхідні для стабільного розвитку країни навіть в умовах фінансових криз (з позицій складової економічної безпеки);

- захищеність фінансових інтересів на всіх рівнях фінансових відносин як усередині країни, так і на міжнародній арені (з позицій ієрархічності та неоднорідності фінансових відносин);

- визначений (або цільовий) рівень фінансової стабільності, за наявності якого країна може забезпечити результативне виконання всіх стратегічно важливих завдань у межах реалізації своїх оперативних, тактичних і стратегічних планів соціально-економічного розвитку (з позицій цільового підходу);

- здатність підтримувати в країні такий стан роботи фінансової системи та забезпечення фінансовими ресурсами, що навіть за умови високої ймовірності та рівня фінансових ризиків не виникає реальних загроз для подальшого розвитку країни та соціально-економічної стабільності в ній (з позицій здатності до задовільної фінансової підтримки та забезпечення).

Під фінансовою безпекою М. Єрмошенко розуміє стан фінансово-кредитної сфери держави, якому властива збалансованість і якість

системної сукупності фінансових інструментів, технологій і послуг, стійкість до внутрішніх і зовнішніх негативних чинників (загроз), здатність цієї сфери забезпечувати захист національних фінансових інтересів, достатні обсяги фінансових ресурсів для суб'єктів господарювання і населення загалом [75].

Науковці В. Геєць, М. Кизим, Т. Клебанова [158] під фінансовою безпекою визначили стан фінансової, грошово-кредитної, валютної, банківської, бюджетної, податкової систем країни, який характеризується збалансованістю, стійкістю до внутрішніх і зовнішніх негативних впливів, здатністю забезпечити ефективне функціонування національної економічної системи та її зростання.

Натомість О. Підхонний розглядає фінансову безпеку як узагальнену характеристику можливих наслідків конфлікту інтересів учасників фінансових угод [195, с. 52]. Ми частково погоджуємося з цим визначенням, оскільки вважаємо, що безпека пов'язана з різними аспектами конфліктології й наявність конфлікту інтересів зумовлює проблеми забезпечення безпеки. Водночас, на нашу думку, тлумачення фінансової безпеки держави потребує врахування ширшого переліку характеристик.

Аналіз наукових підходів до розуміння поняття “фінансова безпека” і “фінансова безпека держави” дав можливість виявити лише окремі аспекти фінансової безпеки ділових одиниць у поглядах тих учених, які акцентували на розумінні фінансової безпеки як ступеня захищеності фінансових інтересів на всіх рівнях фінансових відносин. Водночас стрімкий розвиток наукових досліджень у сфері фінансової безпеки в останні роки спричинив розширення напрацювань учених у напрямі забезпечення фінансової безпеки суб'єктів підприємництва. Хоча погляди науковців на тлумачення сутності поняття “фінансова безпека” на мікроекономічному рівні, як і у випадку з його макрорівневим визначенням також доволі відрізняються.

Зокрема, І. Бланк аналізує фінансову безпеку ділових одиниць з погляду кількісно і якісно детермінованого рівня їх фінансового стану, що забезпечує стабільну захищеність їхніх пріоритетних збалансованих фінансових інтересів від ідентифікованих реальних і потенційних загроз зовнішнього і внутрішнього характеру, параметри якого визначені на основі їхньої фінансової філософії і створюють необхідні передумови фінансової підтримки стійкого зростання в поточному і перспективному періодах [19, с. 24].

На думку А. Єпіфанова, фінансова безпека – це стан підприємства, що [291, с. 22]:

- дає змогу забезпечити фінансову рівновагу, стабільність, платоспроможність і ліквідність підприємства в довготерміновому періоді;

- задовольняє потреби підприємства у фінансових ресурсах для його стійкого розширеного відтворення;

- здатний протистояти небезпекам, спроможним завдати фінансової шкоди підприємству або змінити всупереч бажанню структуру капіталу чи примусово ліквідувати підприємство;

- забезпечує достатню гнучкість у разі ухвалення фінансових рішень;

- захищає фінансові інтереси власників підприємства.

Нам імпонує такий підхід у частині внесення у визначення фінансової безпеки ділових одиниць спроможності забезпечити їх фінансову рівновагу й протистояти загрозам, здатним завдати фінансової шкоди. Водночас вважаємо, що на сьогодні фінансова безпека повинна враховувати не лише фінансову складову, але й поведінкові аспекти ухвалення управлінських рішень та дій зловмисників, що можуть спричинити як фінансові, так і репутаційні збитки для діяльності суб'єктів підприємництва.

Зокрема, О. Воробйова вважає, що “фінансова безпека суб'єкта господарювання – це узагальнююча характеристика стану його фінансів на встановлену дату, яка свідчить про фінансові можливості та спроможність виконувати зобов'язання і ефективно функціонувати в умовах нестабільності, невизначеності та різних фінансових і господарських ризиків” [40, с. 6].

Н. Краснокутська, Г. Коптева розглядають фінансову безпеку підприємств як комплексну характеристику стану захищеності фінансових інтересів підприємства і їх узгодженості із наявним потенціалом та заявленими цілями, що дає змогу протистояти різним негативним факторам у процесі фінансово-господарської діяльності [130, с. 17–18].

М. Погосова розуміє під фінансовою безпекою підприємства комплексну характеристику його функціонування, що відображає потребу в захисті фінансових інтересів, яка існує об'єктивно за умови постійного впливу реальних і потенційних загроз макро-, мезо- та внутрішнього середовища, а також зумовлює потребу формування його спроможності реалізовувати свої інтереси в процесі взаємодії з контрагентами системи фінансових відносин [208, с. 7].

Попри те, що розглянуті визначення схожі між собою тим, що фінансову безпеку розуміють як узагальнюючу комплексну характеристику функціонування ділових одиниць, в останньому враховано важливий, на наш погляд, фактор – спроможність реалізовувати інтереси ділових одиниць у процесі взаємодії з їхніми контрагентами.

Дослідниці І. Багровецька та Л. Козак уважають, що “фінансова безпека підприємства – це важлива складова частина економічної безпеки, що базується на незалежності, ефективності і конкурентоспроможності господарюючого суб’єкта, яка відображається через систему критеріїв і показників його фінансового стану, що характеризують збалансованість фінансів, достатню ліквідність активів і наявність необхідних резервів” [114, с. 99].

Подібною думки дотримується й О. Судакова, яка тлумачить фінансову безпеку як важливу складову тієї частини економічної безпеки підприємства, яка ґрунтується на незалежності, ефективності й конкурентоспроможності фінансів підприємства, що відображається через систему критеріїв і показників його стану, котрі характеризують таке: збалансованість фінансів, достатню ліквідність активів, наявність необхідних грошових резервів, фінансову стійкість (стабільність); рівень забезпеченості підприємства фінансовими ресурсами, достатніми для задоволення його потреб і виконання зобов’язань; якість фінансових інструментів і послуг, що запобігає негативному впливу можливих прорахунків і прямих зловживань на фінансовий стан підприємства; ступінь захищеності фінансових інтересів на всіх рівнях фінансових відносин [280, с. 142].

На думку С. Мельника під фінансовою безпекою підприємства необхідно розуміти стан, при якому через ефективне використання всіх наявних ресурсів та прийняття адекватних, в кожній конкретній ситуації, управлінських рішень, формується рівновага, підтримується стійкість і стабільність, забезпечується надійність системи для досягнення поставлених цілей та завдань, реалізації стратегії розвитку шляхом застосування заходів своєчасного розпізнавання викликів, уникнення/зменшення ризиків, протидії/адаптації до негативного впливу загроз [152, с. 27].

Поняття фінансової безпеки підприємств Н. Бондарчук та М. Гуменчук тлумачать як їхній фінансово-економічний стан, що сприяє забезпеченню захищеності фінансово-економічних інтересів від негативних факторів зовнішнього та внутрішнього середовища і створенню необхідних

фінансово-економічних умов для безперервної успішної діяльності та сталого розвитку підприємства [23]. На наш погляд, цей підхід не повною мірою відображає сутність досліджуваного поняття, оскільки в ньому акцентується на можливостях, що сприяють захищеності ділових одиниць від негативних факторів внутрішнього й зовнішнього середовища, однак не враховують спроможність протидії загрозам, які ними генеруються.

Водночас здатність протидіяти внутрішнім і зовнішнім загрозам, на нашу думку, є однією із визначальних характеристик фінансової безпеки. Дехто з науковців при тлумаченні досліджуваного поняття враховує її, зокрема такі:

- фінансова безпека підприємства – це стан фінансової захищеності та забезпеченості бізнес-процесів, що сприяє запобіганню або попередженню внутрішніх та зовнішніх фінансових загроз та дозволяє забезпечити стабільне функціонування та розширене відтворення з мінімальними фінансовими втратами для підприємства [156, с. 164];

- фінансова безпека підприємства – гранична умова фінансової стабільності або граничний стан фінансової стійкості, яку має забезпечувати підприємство для реалізації своєї стратегії, протистоячи внутрішнім і зовнішнім загрозам [176, с. 225];

- фінансова безпека підприємства – складова його економічної безпеки, яка полягає у наявності такого його фінансового стану, який характеризується: збалансованістю і якістю фінансових інструментів, технологій і послуг; стійкістю до загроз; здатністю підприємства забезпечувати реалізацію фінансових інтересів, також місії і завдань достатніми обсягами фінансових ресурсів; а також спрямованістю на ефективний і сталий розвиток [167, с. 165];

- фінансова безпека підприємства – такий фінансовий стан підприємства, який характеризується, по-перше, збалансованістю і якістю сукупності фінансових інструментів, технологій і послуг, що використовуються підприємством; по-друге, стійкістю до внутрішніх і зовнішніх загроз; по-третє, здатністю фінансової системи підприємства забезпечувати реалізацію його фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів; по-четверте, забезпечувати ефективний і сталий розвиток цієї фінансової системи [106, с. 174];

- фінансова безпека підприємства – це стан захищеності фінансових інтересів підприємства на всіх рівнях його фінансових відносин від впливу

внутрішніх і зовнішніх загроз, який забезпечує його самозбереження та розвиток у поточній та стратегічній перспективах [162, с. 197];

– фінансова безпека підприємства – діяльність з управління ризиками та захисту інтересів підприємства від зовнішніх і внутрішніх загроз з метою забезпечення стабільного розвитку підприємства та зростання його власного капіталу в поточній і стратегічній перспективах [107, с. 24].

Узагальнення і систематизація поглядів учених дає змогу стверджувати про доцільність виокремлення двох найбільш поширених підходів до тлумачення фінансової безпеки суб'єктів підприємництва:

– це фінансовий стан, який дає змогу забезпечити захист фінансових інтересів від загроз;

– це сукупність умов та чинників, які дають змогу протистояти негативним впливам.

Також ми виявили, що фінансову безпеку суб'єктів підприємництва здебільшого характеризують через такі основні аспекти:

- рівень забезпеченості фінансовими ресурсами;
- стійкість фінансового стану;
- здатність протидіяти загрозам.

Варто врахувати й те, що фінансова безпека є системним поняттям, яке характеризується складністю взаємозв'язків з усіма іншими складовими макро- та мікрорівнів. Така складність та багатоаспектність даного поняття потребує виокремлення його основних функціональних характеристик, які подано на рис. 1. 2.

Фінансова безпека посідає вагоме місце в структурі економічної безпеки суб'єктів підприємництва, адже у ній відображається результат функціонування за усіма сферами діяльності (операційної, інформаційної, правової, кадрової, екологічної тощо) й одночасно вона є важливою складовою фінансової безпеки держави. Операційна складова економічної безпеки дає змогу забезпечити безперервність виробничого процесу, виконання робіт чи надання послуг. В операційній сфері необхідно застосовувати інноваційно-інвестиційний підхід, щоб протидіяти загрозам стратегічного характеру в матеріально-сировинній сфері та здійснювати постійний моніторинг поточного становища з метою протидії різноманітним ускладненням й труднощам у виробничому циклі. Кадрова безпека суб'єктів підприємництва відображає використання фахового персоналу на всіх ділянках функціонування ділових одиниць та запобігає можливим

помилкам і фінансовим злочинам зі сторони працівників. Інформаційна складова економічної безпеки суб'єкта підприємництва передбачає захист його інформаційного середовища та інформаційних потоків від кіберзлочинів, захист комерційної таємниці й конфіденційної фінансової інформації від несанкціонованого доступу, витоку й спотворення, а також проведення ділового шпигунства недобросовісними конкурентами чи потенційними рейдерами. Екологічна складова економічної безпеки ділових одиниць полягає в дотриманні чинних екологічних норм та мінімізації втрат від забруднення довкілля. Зокрема, з 2020 року внаслідок пандемії Covid-19 зросла увага до екологічних правопорушень, Європейський суд вніс екологічні злочини до ключових злочинів відповідно до 6-ї Директиви ЄС про боротьбу з відмиванням коштів (6AMLD) [65]. Правова складова економічної безпеки ділових одиниць відображає законодавче регулювання їхнього функціонування та належний внутрішній юридичний супровід фінансово-господарської діяльності (формування статуту та договірної документації тощо).

ОСНОВНІ ФУНКЦІОНАЛЬНІ ХАРАКТЕРИСТИКИ ФІНАНСОВОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА	<ul style="list-style-type: none"> ⇨ забезпечує стійкість фінансового стану суб'єкта підприємництва, стабільність фінансових параметрів його розвитку ⇨ створює підґрунтя стійкого зростання в перспективному періоді ⇨ забезпечує гнучкість у разі ухвалення управлінських рішень фінансовими менеджерами суб'єкта підприємництва ⇨ дає можливість протидіяти наявним і потенційним загрозам, які можуть завдати фінансових і репутаційних збитків суб'єкту підприємництва, змінити структуру його капіталу або призвести до банкрутства ⇨ нейтралізує негативний вплив фінансових криз локального та глобального характеру, недобросовісних дій конкурентів чи інших зловмисників на розвиток суб'єкта підприємництва ⇨ дає змогу запобігти фінансовим помилкам та шахрайству ⇨ запобігає та протидіє рейдерським атакам ⇨ сприяє узгодженню фінансових інтересів власників, менеджерів і суб'єктів зовнішнього економічного середовища ділових одиниць та мінімізує рівень фінансових конфліктів між ними
---	--

Рис. 1.2. Основні функціональні характеристики фінансової безпеки суб'єктів підприємництва

Джерело: розробила автор

Взаємозв'язки макро- та мікрорівневих складових фінансової безпеки подано на рис. 1.3.



Рис. 1.3. Взаємозв'язки мікро- та макрорівневих складових фінансової безпеки

Джерело: [136, с. 23]

Як видно з рис. 1.3, усі макрорівневі складові фінансової безпеки пов'язані між собою і також впливають на фінансову безпеку суб'єктів підприємництва шляхом:

- функціонування усіх секторів фінансової системи країни: бюджетного, грошово-кредитного, валютного, банківського, інвестиційного, фондового, страхового;
- реалізації грошово-кредитної, бюджетної, податкової, валютної, боргової, інвестиційної та інших видів державної політики;
- збалансування національних економічних інтересів та фінансових інтересів суб'єктів підприємництва;
- реалізації національної стратегії забезпечення фінансової безпеки держави;
- законодавчого регулювання функціонування усіх секторів фінансової системи країни;

– реалізації контрольної функції держави, зокрема за допомогою ключових державних органів – Державною фіскальною службою України, Рахунковою палатою України, Національним банком України, Державною казначейською службою України, Державною аудиторською службою України, Державною митною службою України тощо.

Водночас, суб'єкти підприємництва також впливають на стан фінансової безпеки держави за такими основними напрямками:

– у сфері бюджетної безпеки держави – шляхом взаємовідносин з державною фіскальною службою України при розрахунках за податковими зобов'язаннями;

– у сфері валютної безпеки держави – при здійсненні експортно-імпортних операцій (купівля і продаж валюти, кредити в іноземних валютах, розрахунки з іноземними споживачами і постачальниками продукції і послуг у валюті);

– у сфері грошово-кредитної безпеки держави – шляхом взаємовідносин з інститутами фінансово-кредитної системи при здійсненні розрахункового обслуговування, кредитуванні, депозитному обслуговуванні тощо;

– у сфері фінансової безпеки банківської системи – шляхом взаємовідносин з банківськими установами при кредитних, депозитних операціях;

– у сфері інвестиційної безпеки держави – шляхом взаємовідносин підприємств з вітчизняними, іноземними інвесторами, а також державою, як одним із суб'єктів фінансування капітальних вкладень у розвиток перспективних підприємств;

– у сфері безпеки фондового та страхового ринків – при здійсненні страхування майна або результатів діяльності суб'єктів підприємництва, безпечної праці і збереження здоров'я працівників, при здійсненні випуску підприємствами власних акцій і купівля акцій інших ділових одиниць тощо.

Предметом діяльності органів державної влади у сфері забезпечення фінансової безпеки суб'єктів підприємництва є:

– виявлення і моніторинг чинників, які впливають на їхнє функціонування, поточний та перспективний розвиток;

– надання консультативної і методичної допомоги у формуванні діловими одиницями власної фінансової політики в контексті реалізації загальнодержавної фінансової політики;

- недопущення недобросовісної конкуренції шляхом формування ефективного антимонопольного законодавства та відповідної роботи Антимонопольного комітету України;

- забезпечення прозорості механізму реалізації національних (державних) програм щодо розвитку фінансової бази підприємств й недопущення проявів дискримінації з боку державних органів виконавчої влади стосовно участі суб'єктів господарювання у відповідних конкурсних відборах;

- формування ефективного законодавства в сфері захисту прав власності та відповідних державних інституцій, які забезпечують реалізацію функцій протидії рейдерству в Україні;

- розроблення та реалізація антикорупційної політики в Україні;

- протидія нелегальним фінансовим операціям тощо.

Аналіз поглядів науковців на тлумачення сутності поняття “фінансова безпека” як на державному рівні, так і на рівні суб'єктів підприємництва, а також дослідження вченими [11, 24; 40; 61; 125; 134; 135; 294; 302] взаємозв'язків її мікро- та макрорівневих складових засвідчили чимало відмінностей. Водночас необхідно зауважити, що фінансова безпека держави є вихідною умовою фінансової безпеки суб'єктів підприємництва, і, навпаки, фінансова безпека ефективно функціонуючих у країні ділових одиниць створює передумови для стійкості фінансової системи країни, а отже забезпечення її фінансової безпеки. Відтак, фінансова безпека держави передбачає необхідні економічні, політичні й правові умови для зміцнення фінансової безпеки суб'єктів підприємництва. Водночас фінансова безпека суб'єктів підприємництва передбачає необхідні економічні основи для забезпечення стійкості фінансової системи країни та належного рівня її фінансової безпеки. Окрім того, важливим у випадку здійснення суб'єктами підприємництва зовнішньо-економічної діяльності, є врахування впливу ризиків інших країн, оскільки прояви економічних і політичних ризиків можуть становити суттєву загрозу як фінансовій безпеці держави, так і фінансовій безпеці окремих суб'єктів підприємництва.

Попри те, що фінансова безпека ділових одиниць значною мірою залежить від фінансової безпеки держави, на мікроекономічному рівні є можливість здійснювати управління фінансовою безпекою, адаптуватися до змін у функціонуванні фінансової системи країни та протидіяти

деструктивному впливу інших загроз зовнішнього середовища. Однак у практиці функціонування суб'єктів підприємництва впродовж багатьох років спостерігалася значна частка таких, власники й керівництво яких не приділяє належної уваги питанням забезпечення фінансової безпеки. Водночас недостатність уваги до вирішення проблем фінансової безпеки може призвести до критично негативних наслідків для ділових одиниць. Це стосується як тих суб'єктів підприємництва, що перебувають у стадії фінансової кризи, так і фінансово успішних суб'єктів підприємництва. Адже господарюючі суб'єкти, що характеризуються високою результативністю фінансово-господарської діяльності й стрімкими темпами розвитку в умовах зростання економічної злочинності, зокрема недобросовісної конкуренції, ділового шпигунства, рейдерства, можуть стати об'єктом агресивних дій третіх сторін.

Значна частина причин неналежного забезпечення фінансової безпеки пояснюються наявністю багатолітніх стагнаційних процесів в економіці та державному управлінні, що неможливо подолати одномоментно та потребує системних трансформацій, які своєю чергою ускладнилися виникненням нетипових умов господарювання, пов'язаних із появою нових викликів, інструментів протидії яким ще не напрацьовано – пандемії Covid-19 та гібридної війни росії, яка 24 лютого 2022 року перейшла в стадію повномасштабного вторгнення. Серед проявів гібридної війни, які вплинули на фінансову безпеку макро- й мікроекономічного рівнів варто виокремити такі, як: розпалювання конфліктів у бізнес-середовищі, отримання контролю агресором над багатьма стратегічними об'єктами національної економіки, хаотизація політичних процесів, підвищення рівня кримінальної й економічної злочинності, толерування корупції, кіберзлочинність.

Нові виклики значною мірою ускладнили економічну ситуацію в державі й спричинили кризові явища у функціонуванні більшості вітчизняних ділових одиниць. Попри те, можемо констатувати, що деструктивні наслідки пандемії та війни, зумовили позитивний ефект для розуміння власниками й керівництвом ділових одиниць важливості й необхідності приділення уваги безпековій складовій управління, зокрема фінансовій, підвищили рівень значущості розроблення антикризових заходів, досвід використання яких у майбутньому може бути корисним у міжнародній практиці нейтралізації гібридних загроз.

1.3. Загрози фінансовій безпеці суб'єктів підприємництва

Систему забезпечення фінансової безпеки неможливо розглядати без врахування в її понятійно-категоріальному апараті таких ключових безпекових понять, як “виклик”, “загроза”, “ризик”, “небезпека”. Варто зауважити, що серед науковців, які вивчають проблематику безпекознавства й фінансової безпеки зокрема, тривають дискусії не лише щодо тлумачення цих взаємопов'язаних між собою категорій, але й щодо первинності їх виникнення.

Виклик з англ. – “challenge” автори Оксфордського словника тлумачать як завдання або ситуація, яка перевіряє навички та здібності [365]. Дослідники фінансової безпеки здебільшого розуміють під викликами такі обставини, які потребують реагування з огляду на можливість їхнього негативного впливу:

- сукупність обставин, не обов'язково негативного впливу, на які необхідно відреагувати, при цьому їх ігнорування може спричинити позитивні чи негативні наслідки для підприємства [121, с. 6];

- сукупність обставин не обов'язково дестабілізуючого характеру, але безумовно таких, що потребують реагування на них [33].

Відтак, виклики необхідно сприймати як сукупність нейтральних за своїм впливом на фінансову безпеку чинників та обставин, а також оприлюднених або виявлених намірів певних суб'єктів щодо реалізації сукупності дій, що потенційно можуть негативно вплинути на фінансово-господарську діяльність суб'єктів підприємництва. Особливістю викликів є їх дуальність. Вони містять як потенціал позитивного розвитку події, так і можуть бути джерелом загрози безпечному функціонуванню ділових одиниць. З огляду на це, керівництву суб'єктів підприємництва необхідно постійно відстежувати усі виклики з метою протидії їхнього переходу в стадію, яку вже можна ідентифікувати як загрозу фінансовій безпеці. Потрібно враховувати, що джерелом загрози є не самі виклики, а їх деструктивна дія на можливість реалізації конкретних фінансових інтересів суб'єктів підприємництва. Окрім того, виклики можуть зумовити негативний вплив на фінансову безпеку як поодиночі, так і певною їхньою сукупністю. Негативна дія викликів має ймовірнісний характер. Тобто одночасно із викликами з'являється ризик, під яким необхідно розуміти ймовірність настання певної несприятливої (небажаної, критичної) події,

що може завдати шкоди та викликати низку втрат у різних формах, зокрема втрати доходу, капіталу, упущеної вигоди, зниження ділової репутації господарюючих суб'єктів тощо. Ризик є чинником невизначеності, випадковості розвитку події, який зі змінним рівнем ймовірності може зумовити виникнення загроз, що своєю чергою може спричинити небезпеку, а це, як варіант, може призвести до катастрофи – надзвичайної ситуації із незворотніми негативними наслідками. Крім того, один вид ризику може генерувати декілька видів загроз.

Серед найпоширеніших підходів до трактування поняття “загрози” зустрічаються такі:

– загроза – найбільш конкретна і безпосередня форма небезпеки або сукупність умов і чинників, що створюють небезпеку інтересам різних суб'єктів [193, с. 23];

– загрози – це потенційні чи реальні умови, чинники або дії фізичних та юридичних осіб, що порушують нормальний фінансово-економічний стан суб'єктів підприємницької діяльності і здатні заподіяти великої шкоди аж до припинення їхньої діяльності [103, с. 41];

– це можливість випадкового виникнення небажаних фінансових наслідків [16, с. 22–23].

Як видно із розглянутих визначень, в усіх тлумаченнях йдеться про потенційну можливість завдання шкоди суб'єкту підприємництва, водночас вони різняться між собою ступенем деталізації негативних чинників і умов, що можуть її завдати. Водночас, на нашу думку, у розглянутих підходах авторів не конкретизовано деструктивні чинники за їх приналежністю до суб'єкта підприємництва – чи це фактори негативного впливу, генеровані внутрішнім чи зовнішнім середовищем.

Узагальнивши підходи вчених щодо розуміння сутності досліджуваного поняття пропонуємо під загрозою розуміти ендогенний або екзогенний чинник негативної дії або розвиток подій, що пов'язаний зі змінами в зовнішньому або внутрішньому середовищі ділових одиниць, унаслідок яких з'являється вірогідність порушення їхнього нормального функціонування та завдання шкоди, яка призводить до небажаних змін параметрів безпеки.

Щодо розуміння загроз безпосередньо для економічної, в тому числі, фінансової безпеки ділових одиниць, відзначимо, що спектр наукових поглядів у цьому випадку також різниться. На думку Д. Зеркалова, під

поняттям “загрози економічній безпеці підприємства” варто розуміти дію дестабілізуючих природних і/або суб’єктивних чинників, пов’язаних із недобросовісною конкуренцією та порушенням законів і норм, що може спричинити потенційні або реальні втрати для організації [95, с. 272].

Зокрема, Т. Васильців вважає, що можливість появи економічних загроз і небезпек для суб’єктів підприємництва виникає насамперед через конфлікт інтересів усіх учасників підприємницького середовища (а також засобів їхнього досягнення) і дії чинників зовнішнього та внутрішнього середовища їхнього функціонування [34, с. 26].

Щодо розуміння сутності загроз фінансовій безпеці суб’єктів підприємництва, то В. Корнєєв визначає їх як сукупність деструктивних чинників та явищ, а також потенційних або реальних дій фізичних і юридичних осіб, що порушують стан захищеності суб’єктів підприємницької діяльності, спричиняють матеріальні та репутаційні втрати й здатні призвести до припинення діяльності (банкрутства) [122, с. 74]. Погоджуємося з думкою вченого, водночас вважаємо доцільним уточнити зміст цього поняття в контексті можливості забезпечення фінансових інтересів ділових одиниць та пропонуємо розуміти під загрозами фінансовій безпеці суб’єктів підприємництва потенційно можливі або реальні дії зловмисників, а також сукупність чинників та умов об’єктивного характеру, здатних завдати матеріальну або моральну шкоду й спричинити негативні фінансові наслідки для їхньої діяльності, унеможлививши захист головних і пріоритетних фінансових інтересів.

Загрози своєю чергою зумовлюють конкретні форми небезпеки, що мають характер деструктивної і руйнівної дії в сфері функціонування ділових одиниць. Зокрема, на думку М. Єрмошенка [76, с. 39] небезпекою є об’єктивно існуюча можливість негативного впливу на явисьце, систему, механізм, соціальний організм, завдяки чому йому може бути заподіяно шкоду, занепад, потрапляння в кризовий стан тощо.

Під небезпекою Н. Магас розуміє будь-які явища і процеси, які можуть негативно вплинути на функціонування суб’єктів господарювання і таким способом призвести до кризового стану та неможливості подальшого розвитку [145, с. 80]. Погоджуємося з думкою вчених, що коли йдеться про небезпеки, то необхідно розуміти, що ця сукупність явищ, процесів і

дій негативного впливу може з великою ймовірністю зумовити кризовий стан у функціонуванні суб'єктів підприємництва.

Досліджуючи понятійно-категоріальний апарат забезпечення фінансової безпеки ділових одиниць важливим є встановлення взаємозв'язку між поняттями ризику, загроз та небезпек. Нам імпонує наукове бачення цього взаємозв'язку, яке запропонував Н. Носань, у контексті забезпечення фінансової безпеки зазначивши, що ризик існує постійно, може мати як позитивні, так і негативні наслідки, тому є первинною щодо інших категорією. Наявність ризиків є об'єктивною умовою функціонування кожної економічної системи незалежно від рівня складності її організації. Тоді як під загрозами, на думку науковця, необхідно розуміти можливість прояву негативних наслідків дії ризику, а небезпекою потрібно вважати нездатність уникнути загрози. Відтак, небезпеки можна уникнути, але нею не можна управляти, як ризиком [171, с. 37].

Розглядаючи категорію “ризик”, О. Ляшенко акцентує увагу на дуалізмі цього поняття, адже воно розглянуте науковцем і як усвідомлена частина небезпеки (пасивний бік), і як активна дія, спрямована або на усунення небезпеки чи загрози, або, навпаки, на свідоме (але вірогідне) отримання шкоди, збитку тощо [144]. Отже, вчений розглядає ризик як усвідомлену частину загрози і як свідому дію, що може мати негативні наслідки та стати загрозою.

Г. Пазєєва [190] тлумачить ризик як відхилення від певної поставленої мети залежно від ситуації, що настала в певний час, тоді як під небезпекою автор розуміє послідовність дій у системі, внаслідок чого руйнується економічний потенціал, що призводить до занепаду, кризового стану тощо. Загроза згідно з розглянутим науковим підходом є однією із форм небезпеки, що з'являється і розвивається на основі невизначеності.

На думку О. Підхомного, поняття “загрози” та “небезпеки” близькі за змістом до категорії “ризик”. Однак автор акцентує, що існує безліч визначень ризику, що вживаються у різних ситуаціях і в найбільш загальному розумінні ризик є випадковою можливістю отримати відмінний від очікуваного результат. Тоді як загроза, зумовлює не ймовірність виникнення позитивного чи негативного відхилення від очікуваного результату, а чітко виражену можливість настання виключно несприятливих наслідків [196, с. 15].

На наш погляд, у процесі функціонування суб'єкти підприємництва постійно маневрують в умовах численних викликів та ризиків, що своєю чергою генерують загрози та небезпеки й знаходяться в так званій “зоні переходу (маневрування)”, прагнучи досягти зони “безпеки” та уникнути зони “катастрофа” (див. рис. 1.4).

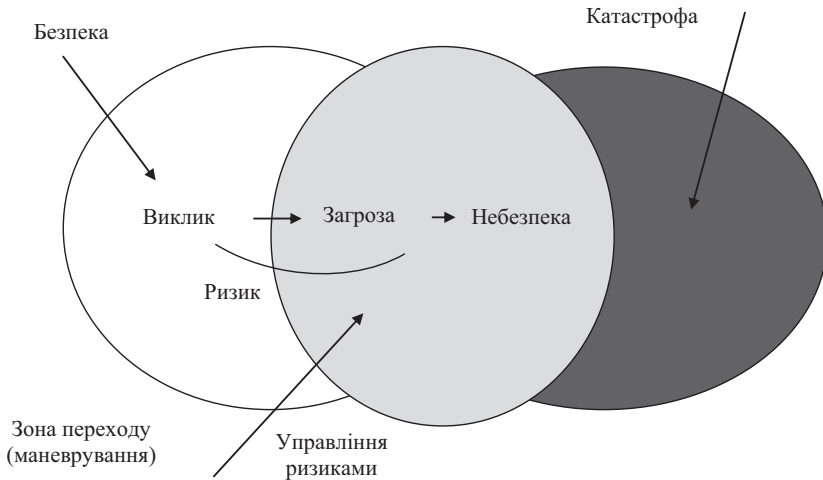


Рис. 1.4. Зони функціонування суб'єктів підприємництва відповідно до критерію безпечності

Джерело: розробила автор

Зона “безпека”, на наш погляд, як поняття “досконалість” є відносним і умовним. Це може бути сформульовано як ціль для власників та керівництва ділової одиниці, до якої необхідно прагнути максимально наблизитись, але усвідомлюючи, що середовища, в якому відсутні виклики, загрози й небезпеки, не існує. Зона “безпека” – це відносно безпечне функціонування суб'єктів підприємництва в обставинах численних викликів та ризиків.

Зона переходу (маневрування) – стан балансування, при якому спостерігаються загрози, що здатні призвести до кількісного зростання ризику, яке спричинить до їх трансформації у небезпеку, а за ефективної протидії – до уникнення такої видозміни.

В зоні переходу (маневрування) необхідно здійснити усі можливі заходи щодо нейтралізації ідентифікованих загроз. У цьому контексті використання інструментів ризик-менеджменту дає можливість значно

підвищити ефективність управління фінансовою безпекою суб'єктів підприємництва, зокрема шляхом виявлення й оцінювання ризиків та передбачення можливих критичних фінансових ситуацій з метою попередження, мінімізації їх наслідків. Водночас, варто зауважити, що навіть за умови ефективного управління ризиками можливі непередбачувані наслідки. Нам імпонує інноваційний підхід Н. Талеба, який у своїй книзі “Чорний лебідь: про неймовірне у реальному житті” [281], проілюструвавши на численних випадках, аргументував, що в житті, в тому числі, фінансовому, існують непередбачувані, надзвичайні події – “чорні лебеді”, які нівелюють усі розрахунки, прогнози і можуть докорінно змінити хід подій. Не дивно, адже термін ризик у давніх варіантах сучасних мов означає близькі поняття: в італійській “risicare” – лавірувати між скелями, у французькій “risquer” – оминати стрімчак, скелю. Зв'язок зі словом “скеля” є не випадковим, що пояснюється тим, що в часи первісного мореплавства зіткнення зі скелею означало катастрофу судна.

Щодо зони “катастрофа”, то вона є протилежною зоні “безпека”, оскільки характеризується радикальною зміною параметрів функціонування ділових одиниць, що може призвести до критично негативних наслідків для їхньої діяльності.

Катастрофа передбачає суттєву негативну зміну фінансових показників діяльності суб'єктів підприємництва, що може спричинити банкрутство, поглинання іншим підприємством тощо.

Функціонування ділових одиниць в Україні відбувається в умовах невизначеності та наявності великої кількості загроз, притаманних ринковій економіці, ускладнене недосконалістю законодавства, криміналізацією суспільства, нестабільністю політичної і соціально-економічної ситуації в країні внаслідок пандемії Covid-19 і війни. Для зміцнення фінансової безпеки суб'єктів підприємництва необхідно використовувати ефективні інструменти ідентифікації загроз, які генерують безпосередню небезпеку для їхнього функціонування. Моніторинг основних загроз фінансовій безпеці ділових одиниць дає змогу своєчасно розробляти і впроваджувати заходи запобігання їм, нейтралізації негативного впливу на результативність діяльності чи їхнього повного усунення. З метою розроблення таких заходів, необхідно визначити їх основні види.

Т. Васильців, В. Волошин, О. Бойкевич та В. Каркавчук [293, с. 34] поділяють загрози фінансовій безпеці підприємств за: суб'єктами, місцем виникнення; ставленням до загроз; ступенем важкості наслідків; об'єктом посягань; можливістю здійснення; формою збитків; тривалістю й частотою дії; рівнем прогнозованості; можливістю попередження.

Учений І. А. Бланк [18, с. 77–79] виділяє такі класифікаційні ознаки загроз фінансовій безпеці ділових одиниць: об'єктна спрямованість; характер прояву; джерела виникнення; характер походження; часовий період; рівень ймовірності реалізації; розмір можливого збитку; можливість передбачення. Х. Цвайг, Н. Галайко пропонують групувати загрози фінансовій безпеці суб'єктів підприємництва за місцем виникнення, сферою походження, джерелами виникнення, можливістю реалізації, тривалістю дії, ступенем важкості наслідків, суб'єктами загроз [296, с. 183].

На думку О. Підхормого, Н. Микитюка та І. Вознюка [198, с. 121–122], загрози фінансовій безпеці суб'єктів підприємницької діяльності необхідно поділяти за джерелом виникнення; рівнем тяжкості наслідків; рівнем вірогідності; стадіями підприємницької діяльності; об'єктами посягань; суб'єктами загроз; формою збитку.

О. Орлик [175, с. 110–111] запропонувала класифікацію загроз фінансово-економічній безпеці ділових одиниць здійснювати за джерелом виникнення; об'єктом посягань, суб'єктами загроз; можливістю здійснення; характером впливу; часовим періодом; характером причинно-наслідкового зв'язку; характером виникнення; тривалістю дії; рівнем ймовірності реалізації, розмірами ймовірних збитків; тяжкістю наслідків; рівнем небезпеки; формою збитку; можливістю передбачення; ступенем прогнозованості; можливістю попередження; стадіями підприємницької діяльності; масштабами можливого впливу; видами діяльності; сферами прояву; характером загроз тощо.

Систематизація та узагальнення поглядів науковців щодо класифікації загроз фінансовій безпеці суб'єктів підприємництва дали нам можливість виокремити такі критерії їх групування (рис. 1.5).

1. За рівнем фінансової діяльності:

- загрози фінансовим інтересам загалом;
- загрози фінансовим інтересам структурних одиниць;
- загрози фінансовим інтересам окремих проектів.

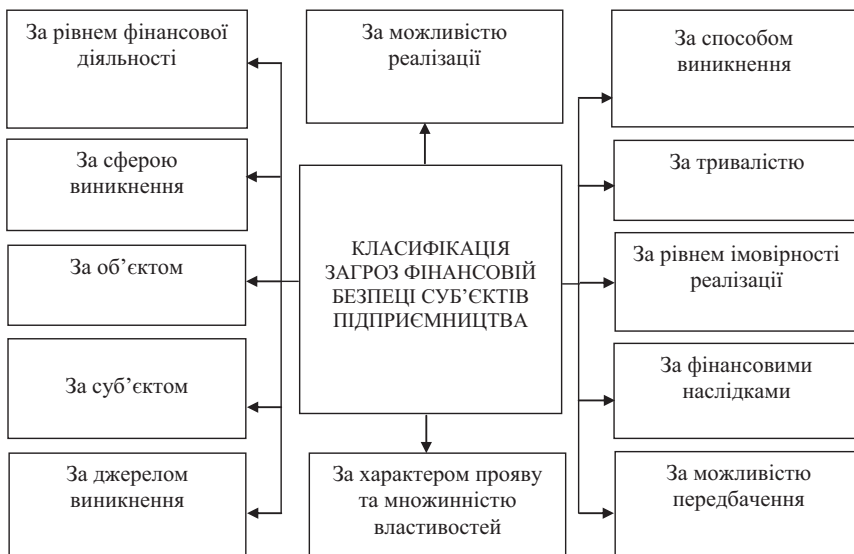


Рис. 1.5. Класифікація загроз фінансовій безпеці суб'єктів підприємництва

Джерело: розробила автор

2. За сферою виникнення:

- у сфері інвестиційної діяльності;
- у сфері кредитної діяльності;
- у сфері емісійної діяльності;
- у сфері інноваційної діяльності;
- в інших сферах фінансової діяльності.

3. За об'єктом:

- загрози фінансовим операціям;
- загрози активам;
- загрози фінансовій інформації;
- загрози фінансовим технологіям;
- загрози фінансовому персоналу.

4. За суб'єктом виділяють загрози, що можуть бути зумовлені діями:

- партнерів по бізнесу;
- конкурентів;
- кримінальних груп;
- державних інститутів;
- власників та персоналу.

5. За джерелом виникнення:

- загрози, генеровані чинниками зовнішнього середовища (зовнішні загрози);
- загрози, генеровані чинниками та умовами внутрішнього середовища (внутрішні загрози).

6. За можливістю реалізації:

- реальні загрози;
- потенційні загрози.

7. За способом виникнення:

- загрози, генеровані дією об'єктивних чинників та умов;
- загрози, генеровані дією суб'єктивних чинників фінансових відносин.

8. За тривалістю:

- короткотермінові;
- довготермінові.

9. За рівнем імовірності реалізації:

- з низьким рівнем імовірності;
- з середнім рівнем імовірності;
- з високим рівнем імовірності;
- імовірність реалізації яких визначити неможливо.

10. За фінансовими наслідками:

- з допустимим рівнем збитків;
- з критичним рівнем збитків;
- з катастрофічним рівнем збитків.

11. За можливістю передбачення:

- передбачувані;
- непередбачувані.

12. За характером прояву та множинністю властивостей:

- прості загрози;
- гібридні загрози.

Серед запропонованих критеріїв на особливу увагу заслуговує групування загроз фінансовій безпеці суб'єктів підприємництва за джерелом виникнення. Серед зовнішніх загроз варто виділити такі:

- глобальні та локальні фінансові кризи;
- гібридна агресія зі сторони інших країн;
- військові інтервенції інших країн;

- несприятливі макроекономічні умови в країні;
- тінізація та криміналізація економіки;
- високий рівень корупції;
- неефективність державної фінансової політики, зокрема, її фіскальної, грошово-кредитної, валютної, інвестиційної та інших складових;
- неефективність державного регулювання фінансової безпеки суб'єктів підприємництва;
- дії зловмисників щодо зниження рівня ділової репутації суб'єкта підприємництва;
- недосконалість нормативно-правової бази, що регламентує фінансову діяльність суб'єктів підприємництва;
- значна залежність ділових одиниць від зовнішніх джерел фінансування.

Серед внутрішніх загроз фінансовій безпеці суб'єктів підприємництва необхідно виділити такі:

- недосконалість організації фінансового менеджменту;
- часті зміни керівництва та працівників;
- помилки в стратегічному плануванні фінансової діяльності;
- низький рівень фінансового аналізу та контролю діяльності;
- недостовірна оцінка прибутковості, незбалансованість грошових потоків;
- конфлікт інтересів між власниками, власниками й топ-менеджментом та інші прояви конфліктів;
- низький рівень кадрової безпеки, що виявляється в непрофесійному доборі працівників, і, як наслідок, – помилках та шахрайстві у фінансовій сфері;
- витік конфіденційної фінансової інформації, її спотворення, дезінформація;
- низький рівень моніторингу дебіторської та кредиторської заборгованості;
- відсутність або неефективність організаційної структури служби фінансової безпеки;
- неналежне юридичне забезпечення фінансово-господарської діяльності;
- низький рівень корпоративної культури.

Значна кількість зовнішніх загроз фінансовій безпеці суб'єктів підприємництва пов'язана з недосконалістю законодавчого регламентування різних аспектів їхньої діяльності, а також з відсутністю або неефективністю державних органів у сфері забезпечення їхньої фінансової безпеки. Ті ж проблеми екстраполуються і на рівень ділових одиниць – відсутність ефективної служби фінансової безпеки й відповідної внутрішньої концептуальної та інструктивної документації, які б визначали всі аспекти забезпечення їхньої фінансової безпеки.

Окрім того, багатолітня гібридна агресія рф в Україні актуалізувала нові виклики. Відтак, пропонуємо новий класифікаційний критерій поділу загроз фінансовій безпеці суб'єктів підприємництва – за характером прояву та множинністю властивостей й відповідно виокремлювати прості та гібридні їх види. Під гібридними загрозами розуміємо явища, що виникають унаслідок еволюції та взаємозв'язку різних елементів, які своєю чергою можуть становити комбінацію різноманітних властивостей і характеристик, що разом утворюють більш складну багатоаспектну загрозу.

Недостатність знань про джерела гібридних загроз зумовлює хибне сприйняття безпеки у ключових сферах функціонування суб'єктів підприємництва, а інституційна слабкість забезпечення розпізнавання, оцінювання та реагування на загрози нового типу знижує можливості забезпечення належного рівня їх фінансової безпеки. Водночас, розроблення відповідних механізмів реагування на такі загрози, на нашу думку, має бути пріоритетним, оскільки на сьогодні підприємницькі структури в своїй діяльності вкрай рідко стикаються з чітко ідентифікованим одним видом загроз фінансовій безпеці, здебільшого на їхнє фінансове становище впливає певна комбінація загроз і більшість із них є гібридними.

1.4. Гібридні фінансові конфлікти суб'єктів підприємництва як дестабілізуючий чинник фінансової безпеки

Фінансові інтереси суб'єктів підприємництва тісно пов'язані з інтересами інших учасників мінливого конкурентного ринкового середовища. Вони можуть бути суперечливими та важко узгоджуваними. Суттєвість розбалансованості фінансових інтересів ділових одиниць із

фінансовими інтересами дотичних до їх діяльності структур, а також із власним персоналом породжує конфлікти й проблеми фінансової безпеки. Тож, можемо констатувати, що значна кількість загроз фінансовій безпеці суб'єктів підприємництва є формою виразу суперечностей між їхніми фінансовими інтересами та інтересами інших учасників ринку й внутрішнього середовища. Адже кожен суб'єкт підприємництва, здійснюючи фінансово-господарську діяльність взаємодіє з чималою кількістю інших учасників економічного оточення, що потребує збалансування його фінансових інтересів з фінансовими інтересами контрагентів на кожному етапі взаємодії. Окрім того, працівники суб'єктів підприємництва також можуть бути джерелом різноманітних суперечностей та протистоянь.

Також протистояння у фінансовій сфері серед низки учасників підприємницького середовища значно загострились в умовах фінансової кризи внаслідок пандемії Covid-19, що набула значних масштабів як в Україні, так і в світовому вимірі.

Конфлікти у фінансовій сфері можуть зумовлювати втрату господарських зв'язків із контрагентами, погіршення відносин з органами державної влади, формування негативної ділової репутації на ринку, що призводить до втрати інвестиційної привабливості.

Наслідками застосування недієвих інструментів протидії таким конфліктам, зволікання з їхнім вирішенням, непрофесійні дії керівництва щодо нейтралізації їхнього деструктивного впливу на фінансову діяльність, а також недосконалість законодавчої бази щодо їхнього регулювання, співучасть корумпованих працівників органів державної влади з одним із учасників конфлікту, є зниження рівня фінансової безпеки суб'єктів підприємництва.

Дослідженню умов, причин і чинників виникнення конфліктів, а також послідовності етапів їх розвитку присвячено праці як вітчизняних, так зарубіжних учених. На основі них розроблено чимало теорій конфліктів. Серед різноманіття наукових підходів, що набули поширення в теорії конфліктології варто виділити соціологічний підхід (Г. Зіммель, Л. Козер, Р. Дарендорф, К. Боулдінг, Г. Лебон та ін.), що передбачає розуміння конфлікту як зіткнення об'єктивних і суб'єктивних суперечностей.

Так, Л. Козер зазначає, що конфлікт виникає, коли одна зі сторін прагне зберегти певний визначений стан справ, наприклад, соціальний

статус чи набуті привілеї, а інша прагне до його зміни; або тоді, коли обидві сторони прагнуть змінити певну ситуацію, але цілі та способи зміни вони розуміють по-різному [357].

Зокрема, Р. Дарендорф (теорія “конфліктної моделі суспільства”) стверджує, що всі відносини між групами індивідів зі взаємно несумісними цілями, які в своїй більш загальній формі є бажанням обох конкурентів отримати те, що можливе лише для одного – в цьому розумінні є відносинами соціального конфлікту [359, с. 135].

Згідно з мотиваційним підходом (М. Дойч, Г. Макклінтон) конфлікт визначають як усвідомлену несумісність індивідуальних намірів та інтересів протидіючих сторін. За цього підходу значну увагу приділяють суб’єктивним, мотиваційним чинникам у розвитку конфліктної взаємодії. М. Дойч зауважує, що конфлікт існує, коли з’являються суперечливі прагнення або дії. Ці суперечності можуть проявлятися у вигляді внутрішньої напруги (боротьби мотивів) або ж у формі ворожих дій між особами чи групами осіб за обмежені цінності або ресурси [360, с. 7].

У перекладі з латинської конфлікт (*conflictus*) означає “зіткнення”. Щодо тлумачення поняття “конфлікт” через призму правового регулювання, то його визначено як зіткнення поглядів, інтересів, позицій та ін., що супроводжується конфронтацією, суперництвом, конкуренцією чи протиборством його учасників [304, с. 335].

У психологічному ракурсі конфлікт можна розуміти як крайнє загострення суперечностей і протистояння декількох сторін соціальної взаємодії, який супроводжується негативними діями. Це може бути відкрита або прихована форма боротьби конфліктуючих сторін унаслідок відстоювання ними взаємовиключних інтересів.

Відтак, можемо зробити висновок, що конфлікт є природнім, невід’ємним компонентом розвитку суспільства в цілому, окремих суб’єктів господарювання та індивідів, оскільки еволюція завжди передбачає наявність вибору різних думок і поглядів, відтак – суперечностей, дискусій, протистоянь.

Незважаючи на різні тлумачення конфлікту, викладені вище визначення не суперечать, а доповнюють одне одного, розкриваючи різні аспекти й умови виникнення та розвитку конфліктів, водночас в усіх наукових підходах йдеться про наявність суперечності, яка виникає в процесі певних взаємовідносин.

Близьким за значенням до поняття “конфлікт” є термін “конфліктна ситуація”, однак, попри існування між ними тісної спорідненості, їх потрібно розмежовувати. Конфліктна ситуація передбачає виникнення розбіжностей при дискусії, спорі, тоді як конфлікт – це взаємне негативне відношення, яке виникає при зіткненні бажань, думок. Конфліктна ситуація – це об’єктивна основа конфлікту, що фіксує виникнення реальної суперечності в інтересах і потребах сторін. Відтак, це ще не конфлікт, оскільки існуюча об’єктивна суперечність може деякий час не усвідомлюватися учасниками взаємодії [72, с. 49].

Окрім того, на наш погляд, необхідно виокремлювати також поняття “конфлікт інтересів” та розуміти під ним ситуацію вибору рішення, коли є суперечності між власним інтересом та інтересом іншої сторони. Зокрема, якщо йдеться про взаємодію учасників у площині “бізнес–влада”, то конфлікт інтересів може існувати, коли в державного службовця є особисті інтереси у фінансовій сфері, що можуть призвести до ухвалення ним рішення, що порушують інтереси держави. Зокрема Закон України “Про запобігання корупції” від 14.10.2014 1700-VII визначає такі види конфлікту інтересів [225]:

- потенційний конфлікт інтересів – наявність у особи приватного інтересу у сфері, в якій вона виконує свої службові чи представницькі повноваження, що може вплинути на об’єктивність чи неупередженість прийняття нею рішень, або на вчинення чи невчинення дій під час виконання зазначених повноважень;

- реальний конфлікт інтересів – суперечність між приватним інтересом особи та її службовими чи представницькими повноваженнями, що впливає на об’єктивність або неупередженість прийняття рішень, або на вчинення чи невчинення дій під час виконання зазначених повноважень.

Отже поняття “конфлікт інтересів” означає ситуацію розбалансованості інтересів її учасників, спричинену різними очікуваннями від взаємодії.

Якщо йдеться про корпоративні відносини, то проведений нами аналіз наукових підходів у цій сфері дав можливість виявити вживання у цьому випадку терміну “корпоративний конфлікт”, під яким розуміють конфлікт інтересів між суб’єктами корпоративних відносин, що мають прямий вплив на бізнес, та зацікавленими особами, які мають опосередкований вплив на бізнес, за матеріальні та

нематеріальні ресурси підприємства, що спричинено різними групами корпоративних інтересів, які в результаті призводять до змін у його діяльності [141, с.173]. Водночас, на нашу думку, це визначення не відображає сутність поняття повною мірою, адже в ньому не враховано наявність суттєвих концептуальних розбіжностей, що можуть виникнути між акціонерами АТ, а також між акціонерами й самим товариством в особі його органів управління та посадових осіб. Для більш повного розуміння конфлікту цього типу пропонуємо виокремити такі його сутнісні характеристики:

1. Суб'єкти корпоративних конфліктів – учасники корпоративних відносин як носії корпоративних інтересів в особі товариства, його засновників, учасників/акціонерів, органів управління, посадових осіб.

2. Типові причини корпоративних конфліктів: розбіжності в поглядах на управління товариством (виникають між акціонерами, акціонерами й менеджерами товариства щодо питань здійснення діяльності, стратегії розвитку); порушення норм чинного законодавства, статуту чи внутрішніх документів товариства, прав акціонерів чи групи акціонерів.

3. Наслідки корпоративних конфліктів: порушення прав акціонерів, позови щодо товариства або керівників з приводу ухвалених ними рішень, дострокове припинення повноважень органів управління, суттєві зміни в складі акціонерів.

Водночас зауважимо, що першопричиною корпоративних конфліктів є організаційно-правова й економічна природа акціонерних товариств, яка характеризується взаємодією різних груп учасників – акціонерів, менеджерів, персоналу, що мають різні інтереси й бачення способів їхнього досягнення. Ми виокремили основні причини корпоративних конфліктів, пов'язані з особливостями організації товариств акціонерної форми власності (рис. 1.6.).

Відтак, розбіжності інтересів між окремими учасниками товариства пояснюються властивою природою взаємовідносин такого типу організаційно-правової форми. Окрім того, до чинників, що можуть поглиблювати конфліктні ситуації в акціонерних товариствах, належать: низький рівень корпоративної культури акціонерів і керівництва товариства, дублювання повноважень окремих працівників й недотримання ними службової й організаційної дисципліни; відсутність чи недостатнє використання моральних і матеріальних важелів впливу на

стимулювання продуктивності праці працівників; недосконалість законодавчої бази, що регламентує питання захисту інтересів власників; високий рівень корупції в органах державної влади; недосконалість судової системи тощо.

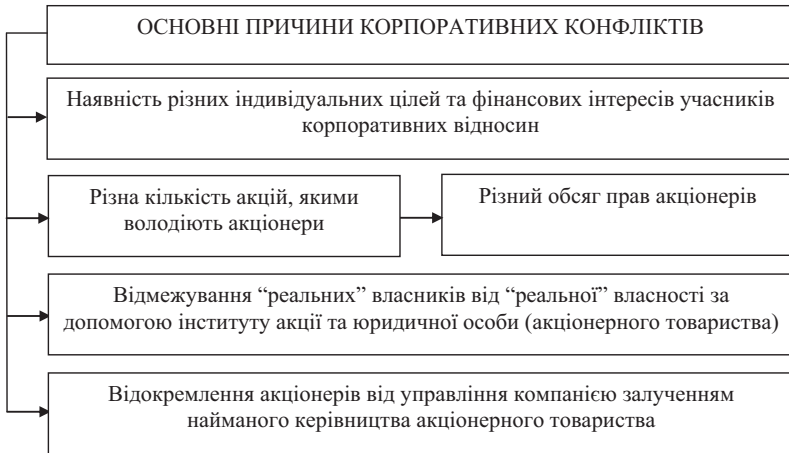


Рис. 1.6. Систематизація причин корпоративних конфліктів

Джерело: розробила автор

Основні конфліктні взаємозв'язки в акціонерних відносинах подано на рис. 1.7.

Якщо йдеться, про можливі розбіжності в поглядах на організацію управління товариством, що можуть виникати між учасниками корпоративних відносин, варто виокремити також такі проблемні аспекти: обрання членів правління та їхнє призначення; визначення розміру винагород/премій, які виплачують членам правління; звільнення членів правління, провідних виконавчих посадових осіб компанії; оцінка вартості акцій, питання емісії нових акцій; умови ймовірного злиття або поглинання; придбання активів компанії або розпорядження ними тощо.

Корпоративні конфлікти завдають власникам і державі значних матеріальних та моральних збитків, зумовлюючи загострення фінансових криз в діяльності суб'єктів підприємництва та провокуючи загрозу банкрутства, знижуючи позиції України в міжнародних рейтингах, скорочуючи обсяги інвестування, зменшуючи обсяги виробництва.

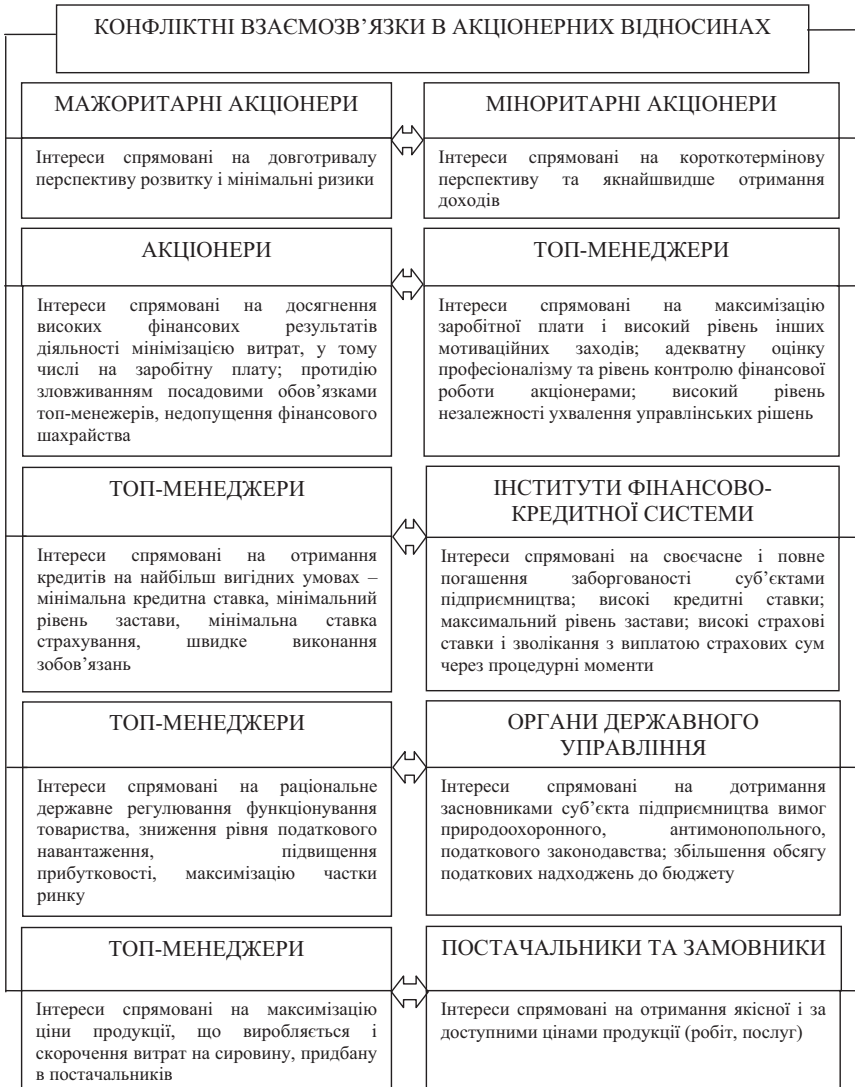


Рис. 1.7. Структурно-логічна схема конфліктних взаємозв'язків в акціонерних відносинах

Джерело: розробила автор

Зміна одних теорій іншими забезпечувала постійне концептуальне оновлення конфліктології та підходів до визначення поняття “конфлікт”, й суміжних категорій, таких як “конфліктна ситуація”, “конфлікт інтересів”, “корпоративний конфлікт”. Водночас, підсумовуючи ключові ідеї основних концепцій конфліктології і поглядів вчених у цій сфері [101; 126; 137; 141; 164; 279] вважаємо доцільним виокремлення таких характеристик конфлікту:

- конфлікт є природнім соціальним явищем, оскільки кожному індивіду притаманна сукупність різноманітних фізичних, соціальних, психологічних, економічних чинників, що за певних обставин можуть зумовити розбалансування інтересів;

- конфлікти здатні генерувати позитивний ефект у процесі суспільного розвитку, стимулюючи прогресивний рух суспільного життя і сприяючи збереженню єдності соціальних утворень;

- конфліктні стани розвитку суспільства загалом, суб’єктів господарювання та окремих індивідів є взаємопов’язаними;

- конфлікти зумовлюються наявністю незворотних та постійних суспільних явищ з наявністю керівної меншості й керованої більшості, що уможливорює виникнення різних соціальних конфліктів.

Водночас вважаємо, що в умовах нових викликів й загроз існує потреба дослідження конфліктів, яке б охоплювало ширший перелік аспектів, зокрема не лише вивчення конфлікту як соціально-психологічного явища, а й розкриття природи фінансового конфлікту як особливого суспільного явища, складових та причин виникнення таких конфліктів, а також виокремлення й характеристика їх основних видів з метою впливу на них і можливості управління.

Наукові погляди щодо розуміння фінансових конфліктів хоча й наявні у фаховій літературі, однак, не всі аспекти їх розвитку на сьогодні достатньо досліджені. Зокрема, О. Підхонний конкретизує лише, що важливим чинником фінансового конфлікту є певна фінансова угода, й зазначає, що такий конфлікт має свою власну логіку, що підпорядковує собі сторони, які вступили у протиборство [196, с. 58].

З метою більш повного розуміння цього поняття пропонуємо визначати фінансовий конфлікт як протистояння суб’єктів фінансових відносин, що виникає в процесі здійснення ними фінансово-господарської діяльності внаслідок несумісності інтересів та ціннісних орієнтирів.

До основних елементів та ознак фінансових конфліктів, на нашу думку, варто виділити такі (рис. 1.8):



Рис. 1.8. Систематизація елементів та ознак фінансових конфліктів

Джерело: розробила автор

- сторони конфлікту – суб'єкти фінансових відносин, інтереси яких порушено безпосередньо, або суб'єкти, що явно чи/або приховано підтримують конфліктерів;

- предмет конфлікту – те, через що виникає конфлікт між його учасниками, на що претендує кожний із них. Предметом конфлікту можуть бути як фінансові ресурси, матеріальні й інтелектуальні цінності, так і в цілому опосередковано практично будь-який предмет, процес або явище соціально-економічної дійсності (авторитет, влада, престиж, ідея проекту тощо);

- умови конфлікту – зовнішній контекст, у якому виникає і розвивається конфлікт;

- мотиви конфлікту – внутрішні спонукальні сили, що підштовхують суб'єктів фінансових відносин до конфлікту і виявляються у формі потреб, інтересів, цілей, переконань;

- уявлення учасників про конфлікт – це індивідуальне розуміння обставин конфлікту кожним із його учасників;

- способи поведінки в конфлікті – конкретні дії учасників у процесі вирішення конфлікту (відхід від конфлікту, боротьба, поступливість, компроміс, співпраця).

Реалізація того чи іншого способу поведінки у фінансовому конфлікті в кожній конкретній ситуації залежить від її особливостей, а також індивідуально-психологічних характеристик учасників конфлікту та їхніх поведінкових упереджень. Водночас, нашу думку, цікавими й корисними для врахування при розробленні теоретико-практичного інструментарію для протидії конфліктам й забезпечення фінансової безпеки є результати дослідження, яке провели П. Коулман, Р. Фергюсон за участю 149 професійних конфліктних медіаторів [129].

Учені виявили ключові чинники конфлікту, які впливають на вибір стратегій й на результати виходу з кризи, ним спричиненої:

- інтенсивність конфлікту. Під інтенсивністю розуміють енергію, яку потрібно використати, щоб вирішити конфлікт. У цьому контексті конфлікти необхідно поділяти на такі, що легко подолати, так і такі, які складно врегулювати;

- структура конфлікту. Йдеться про природу виникнення конфлікту – реальні та об'єктивні підстави чи наявність суб'єктивних цілей конфлікту. Відтак, конфлікти можуть бути як такими, що мають кооперативні, взаємовигідні цілі, де учасники суперечки мають спільні базові погляди на проблему й прагнуть конструктивного вирішення, або ж такими, що базуються на ідеї неконструктивного суперництва;

- прозорість конфлікту. Цей чинник визначає рівень відкритості учасників конфлікту до його вирішення та легальність їхніх дій.

Результати дослідження впливу цих чинників на конфлікт показали, що інтенсивність конфлікту була однією із важливих ранніх ознак поведінки конкуруючих сторін: що вищою вона була, то агресивнішим було їхнє відношення між собою.

Також учені виявили, що наявність або відсутність спільної мети у конфліктуючих сторін є показником того, наскільки швидко буде вирішено конфлікт. Окрім того, акцентовано на важливості чіткого окреслення проблеми конфлікту – що чіткіше були виражені проблеми

конфлікту, то більш охоче конфліктуючі сторони розглядали процес медіації та були більш схильними до виходу з кризи.

Розглянуті чинники, зокрема прозорість конфлікту, є важливими не лише з метою їхнього врахування при розробленні рекомендацій щодо вирішення конфлікту в частині його фінансової складової, але й також у сфері забезпечення безпеки. Оскільки тіньові мотиви й приховані дії учасників фінансових конфліктів суб'єктів підприємництва можуть становити вагому загрозу їхній фінансовій безпеці.

Окремо ми виявили, що одним із різновидів фінансового конфлікту, який виділяється у працях науковців є податковий конфлікт. Зокрема, природу податкових конфліктів досліджували у своїх працях такі практики і теоретики, як І. Ващенко у монографії “Конфлікти: сучасний стан, проблеми та напрямки їх вирішення в органах внутрішніх справ” [35], А. Єзеров у монографії “Конституційний конфлікт як феномен та процес в Україні” [74] та інші фахівці у сфері державного регулювання сфери оподаткування, які вивчали правові основи застосування податкового законодавства і захисту прав і законних інтересів платників податків в адміністративному порядку.

Окрім того, період глобалізації та інформатизації фінансових процесів супроводжується появою низки фінансових протистоянь, характерною ознакою яких є перехід до використання гібридних важелів впливу на досягнення бажаних результатів фінансового конфлікту. В Україні дослідження цієї проблематики в теоретичній та прикладній площині актуалізувалося внаслідок багаторічного ведення гібридної війни російської федерації. Доктрина гібридної війни була представлена ще в 2013 р. на засіданні Академії військових наук росії генералом В. Герасимовим. У представленій доповіді “Про війни майбутнього” йшлося про так звані “асиметричні дії”, що передбачають використання як воєнних, так і невоєнних, першочергово, інформаційних методів дестабілізації супротивника. “Гібридність” такої війни полягає у тому, що для досягнення поставлених вищим політичним керівництвом держави цілей використовуються не тільки військові методи, а й дипломатичні, фінансово-економічні, енергетичні, розвідувальні засоби, а також важелі інформаційно-психологічного впливу. Технологічне бачення реалізації концепції гібридної війни рф в Україні належить В. Суркову,

який апелює до базового 4-тактного алгоритму нелінійних процесів, детально описаного в аналітичній публікації “Війни XXI: Полігібресія росії” Центру глобалістики “Стратегія XXI”, що використовуються для гібридних технологій ведення війни [39]:

- хибноцільове програмування супротивника через “коопераційну модель”, під прикриттям якої реалізується програма його крипто-деструкції;

- трансформація визначеностей і станів у сукупність невизначеностей, хаотизація причинно-наслідкових ланцюжків;

- управління хаосом через швидкі рішення й ініціативні дії;

- впорядкування хаосу, реінжиніринг простору, отримання нової реальності через синергетику.

Відтак, гібридні засоби передбачають не лише порушення правових норм, а й зловживання цими нормами, не лише застосування сили, але й засоби психологічного тиску на супротивника. Як зазначають учені, що займаються проблемами вивчення особливостей гібридної війни, головним об’єктом російської стратегії була не фізична реальність, а сфера її інтерпретації [289, С. 7]. Можна констатувати, що на підготовчому етапі російської гібридної агресії боротьба велася не за територію країни, а за світогляд її населення, перейшовши в 2014 році в нову форму – військового втручання, яке своєю чергою набуло нового гібридного формату, оскільки тлумачилось агресором міжнародній спільноті внутрішнім громадянським конфліктом в Україні й це тривалий час її дезінформувало.

Значна частина науковців, істориків та політиків вважають, що одними з ідеологів виникнення концепції гібридної війни були А. Гітлер та П. Й. Геббельс, оскільки вже тоді в політичних цілях активно використовувалася пропаганда за допомогою спеціальних інформаційних випусків по радіо та в кіно-хроніці, що стало ідеологічним підґрунтям для початку та ескалації бойових дій.

На сьогодні серед науковців і практиків ще не вироблено єдиного підходу до тлумачення терміна “гібридна війна” чи “гібридний конфлікт”. Адже йдеться про формування нового виду глобального протистояння на міжнародній арені та абсолютно нового формату міжнародного безпекового середовища. Водночас це поняття теоретично й практично є найбільш придатним для визначення специфіки дій рф, яка, поєднуючи

історико-ідеологічні, інформаційні, фінансово-економічні та мілітарні й квазімілітарні засоби, терористичі акції та ядерний шантаж, намагається досягти в Україні та в геополітичній площині своїх політичних цілей. Проблематику розвитку конфліктів гібридного типу досить широко досліджували західні науковці й практики. Зокрема, ще в 2014 р. Ф. М. Брідлав зазначав: “Те, що ми бачимо в росії зараз, це гібридний підхід до війни, що полягає в тому, щоб використовувати всі важелі впливу, щоб створити проблеми, які можна буде згодом використовувати за допомогою військового потенціалу” [394].

Зокрема, Р. Бернсбі та Ш. Рівз зазначали, що сучасні конфлікти складно правильно ідентифікувати, оскільки часто вони є поєднанням характеристик традиційно не пов’язаних між собою форм війни. Відтак, окремі державні суб’єкти регулярно використовують непрямую тактику асиметричної війни, здійснюючи кібератаки, терористичні акти, щоб отримати стратегічну перевагу над своїми супротивниками. Подібним способом недержавні збройні угруповання та повстанці застосовують засоби традиційної війни, включаючи використання зброї у вирішенні конфліктів [385].

Відмінності між розумінням сутності гібридної війни, що використовується в західній практиці, – конфлікту, що охоплює багатомодальність, – і російським підходом, де “гібридність” розглядається як наступальне глибоке вторгнення і рефлекторний контроль, описав К. Касапоглу [375].

Г. Лассвелл, Г. Ласконьяріас характеризують гібридний конфлікт як такий, у якому використовуються всі засоби впливу на об’єкт агресії державними чи недержавними виконавцями задля досягнення політичної мети – кіберзасоби, ядерні, стратегічні комунікації та навіть найбільш неоднозначні й антигуманні [377].

Зокрема, П. Піндяк стверджує, що гібридний конфлікт охоплює багаторівневі зусилля, спрямовані на дестабілізацію функціонування держави та поляризацію її суспільства. Отже, супротивник має на меті вплинути на політичне керівництво країни, здійснюючи приховані дії [383].

Варто також зазначити, що чимало дослідників схиляються до використання альтернативного визначення поняттю “гібридний конфлікт”, терміна “війни сірої зони” або “сурогатна війна”, зокрема Е. Фолі, К. Каунерт зазначають, що сурогатна війна характеризує

стратегічні й оперативно-тактичні засоби війни, які часто використовують людські та/або технологічні замітники з метою мінімізації витрат на війну. Вони можуть варіюватися від озброєних повстанських груп до використання озброєних дронів і до кіберпропаганди [367].

В Україні, з огляду на активне використання росією інформаційно-пропагандистських інструментів, економічних й енергетичних важелів впливу, втручання у внутрішньополітичне життя, стимулювання мовних, міжетнічних і міжконфесійних конфліктів, історичних та культурних маніпуляцій та інших засобів тиску на вразливості держави, від 2014 року першочерговим завданням практиків і науковців стало дослідження інструментів гібридної війни з метою розроблення стійкої й ефективної суспільно орієнтованої системи державного управління. В теоретичній площині впродовж цього періоду було опубліковано низку наукових праць: колективну монографію Інституту стратегічних досліджень “Світова гібридна війна: український фронт” за редакцією В. Горбуліна [269], монографію О. Базалука “Теорія війни і миру. Геофілософія Європи” [8], працю Р. Додонова “Конфлікт на Сході України у дзеркалі соціально-філософської рефлексії” [68] тощо. Зокрема, Р. Додонов визначає гібридну війну як комбінацію конвенційних, іррегулярних та асиметричних засобів, що включають постійну маніпуляцію політичним та ідеологічним конфліктом, а також залучення сил спеціальних операцій та конвенційних збройних сил, агентів розвідки, політичних провокаторів, представників медіа, економічний шантаж; кібератаки; проксі-сервери і сурогати, паравійськові, терористичні і кримінальні елементи. У гібридному протистоянні використовують такі форми послаблення супротивника, як контрабанда, торгівля наркотиками, незаконна передача зброї і військової техніки у руки криміналітету [47].

Що стосується розвитку поняття “гібридна війна” в міжнародних політичних відносинах, то значним проривом у цьому дискурсі стало застосування цього терміна військовими США та НАТО з 2006 року щодо дій Хезболли в ході лівансько-ізраїльського конфлікту [384]. Представники Альянсу акцентували увагу на тому, що новою формою ведення війни стала “гібридна війна” [370] та запропонували вважати “гібридними засобами” широкий перелік високоінтегрованих відкритих та прихованих мілітарних, парамілітарних і цивільних засобів” [395].

Відтак у 2016 році на саміті у Варшаві було вирішено поширити дію статті 5 Вашингтонського договору на атаки проти одного із союзників з використанням гібридних методів: “Альянс та його члени будуть готові протидіяти гібридній війні в рамках колективної оборони. Північноатлантична рада може прийняти рішення про приведення у дію статті 5 Вашингтонського договору” (п. 72). Тоді ж було затверджено і стратегію протидії гібридній війні [396].

У Спільному рамковому документі ЄС [374] гібридні загрози було визначено як “поєднання примусової та підривної діяльності, традиційних і нетрадиційних методів (тобто дипломатичних, військових, економічних, технологічних), які можуть бути скоординовано використані державними чи недержавними суб’єктами для досягнення конкретних цілей, залишаючись на рівні нижче межі формально оголошеної війни”. Актуальність розроблення інструментів протидії гібридним загрозам зумовила необхідність створення Центру аналізу гібридних загроз ЄС (EU Hybrid Fusion Cell) у межах Розвідувального і ситуативного центру ЄС (EU Intelligence and Situation Centre, EU INTCEN) Європейської служби зовнішньої дії. Одночасно було створено Центр передового досвіду з протидії гібридним загрозам, який зосереджується на дослідженні загроз гібридного типу та механізмів протидії їм.

У виданні “Military Balance” за 2015 рік Лондонського Міжнародного інституту стратегічних досліджень (англ. – International Institute for Strategic Studies of London) гібридну війну визначено як використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на досягнення ефекту неочікуваності, захоплення ініціативи та отримання психологічних переваг за допомогою використання дипломатичних можливостей, масштабних і раптових інформаційних засобів, прикриття і приховування військових і розвідувальних дій, у поєднанні з економічним тиском [392].

Відтак, конфлікти нового типу є симбіозом руйнації військово-політичної системи супротивника шляхом шантажу, підкупу, диверсій, дискредитації, інформаційного тиску, маніпуляцій масовою свідомістю. Такий тип конфлікту поєднує фрагментарне і ситуативне сполучення різних методів і теорій війни, імплементацію їх у різні сфери, особливо в інформаційну, ідеологічну, світоглядну і морально-етичну.

Особливістю розвитку гібридних конфліктів на підготовчому етапі є також те, що вони здійснюються приховано з використанням переважно

нелінійних тактик і спрямовані не на захоплення усєї території країни, хоча не виключається взяття під контроль окремих територій, а на отримання контролю над державою, який досягається через вплив на населення, політикум, бізнес, силові структури. Тому до протидії гібридним загрозам повинні залучатися не тільки силові структури держави, але й майже усі міністерства та відомства, недержавні організації, бізнес, громадянське суспільство.

24 лютого 2022 року на території України розпочалася “гаряча”, військова фаза гібридної війни росії. Свідченням її “гібридності” є не лише попередня багаторічна активація інформаційної складової, а й також неможливість кваліфікуватись як класична конвенційна війна, в якій збройні сили однієї держави у відкритій конфронтації за нормами міжнародного права протистоять військовим силам іншої через масові воєнні злочини щодо мирного населення, а також заперечення війни агресором та інтерпретації відкритого повномасштабного воєнного нападу як “спецоперації” з метою “демлітаризації і денацифікації України”.

Серед інструментів гібридних конфліктів важливе значення відводиться фінансово-економічним, зокрема росією використовувались такі:

- агентурне проникнення агресором у державні органи управління з метою регулювання економіки України та управління її міжнародними економічними відносинами;
- концентрація контролю над банківським сектором України;
- здійснення агресором торговельної війни, зокрема блокування портів, міжнародного транзиту українських товарів, впровадження дискримінаційних умов торгівлі тощо;
- маніпулювання цінами на значущі для економіки України товари;
- проникнення російського капіталу у стратегічно важливі об’єкти України та встановлення реального чи прихованого контролю над ними, в тому числі штучне блокування/припинення діяльності рентабельних українських підприємств;
- посилення залежності України від постачання стратегічної сировини (енергоресурсів, ядерного палива та ін.);
- використання бізнесу в Україні з російським капіталом для деструктивної чи протиправної діяльності, зокрема фінансування тероризму, підконтрольних політичних проєктів, виведення/відмивання коштів тощо.

Використані агресором фінансово-економічні інструменти гібридної війни суттєво знижували рівень фінансової безпеки України впродовж десятиліть, створюючи підґрунтя для початку бойових дій у 2014 році, їх подальшої ескалації та повномасштабного військового вторгнення. Аналіз особливостей розвитку міждержавних гібридних конфліктів, інструментів, які в них застосовуються, та впливу на фінансову безпеку країни, яка стала об'єктом агресії, функціонуючих у ній суб'єктів господарювання, а також змін, спричинених ними в глобальному економічному, політичному й безпековому середовищі, доводить, що фінансова безпека – це системне поняття, що інтегрує в собі як фінансові інтереси світової спільноти, міждержавних утворень, держави, так і фінансові інтереси окремих громадян, домашніх господарств, населення, суб'єктів підприємництва. На різних рівнях управління фінансова безпека має своє специфічне наповнення, водночас, основні сутнісні характеристики та закономірності ведення гібридних конфліктів на міждержавному рівні, можна, на наш погляд, екстраполювати на рівень суб'єктів підприємництва. Адже на мікрорівні відбуваються протистояння фінансових інтересів, які також мають гібридний характер. Підтвердження нашої аргументації знаходимо ще в працях Платона, який наголошував на схожості характеристик міждержавних та внутрішніх конфліктів. Відповідно до подій того історичного періоду він поділяв війни на внутрішні (між грецькими полісами) та зовнішні (боротьба греків з іншими державами) й попри наявності відмінних причин їх розвитку, акцентував, що базова мотивація в обох випадках є однаковою. Зовнішні війни Платон вважав природним явищем, що виникають з відмінності Греції від варварів, необхідності забезпечення її безпеки [207]. Джерелом внутрішніх війн, на його думку, були несправедливість, відсутність згоди і гармонії та “ненаситна жага” тощо, тобто приватні і публічні “джерела нещастя”. Такої ж думки дотримувався й Жан-Жак Руссо, зокрема у своїх теоріях він пояснював причини війни в бажанні людей мати приватну власність і в матеріальній нерівності в суспільстві [47, с. 17]. Відтак, можемо констатувати, що на якому б рівні не розвивалися конфлікти, в тому числі гібридного типу (міждержавному чи на рівні функціонуючих у державі суб'єктів підприємництва), їм притаманні схожі важелі впливу на досягнення цілей.

Наявність різновидів конфліктів, зокрема фінансових та значне різноманіття термінів у сфері конфліктології й підходів до їхнього

тлумачення створює плутанину в понятійно-категоріальному апараті і зумовлює необхідність систематизації фінансових конфліктів із урахуванням виявлених під час дослідження нових аспектів їхнього гібридного розвитку. У контексті забезпечення фінансової безпеки ділових одиниць пропонуємо групувати їх за низкою ознак з виділенням нових критеріїв – наслідками, результативністю й множинністю важелів впливу на їх фінансову безпеку (рис. 1.9):

1. За суб'єктами необхідно виділяти фінансові конфлікти:

- між власниками;
- між власниками та топ-менеджерами;
- між топ-менеджерами й інститутами фінансово-кредитної системи;
- між топ-менеджерами та державними органами;
- між топ-менеджерами й іншими діловими одиницями;
- між працівниками.

1. За сферою виникнення фінансових конфліктів:

- в інвестиційно-інноваційній сфері;
- у кредитній сфері;
- у сфері оподаткування;
- в інших сферах.

2. За відношенням до суб'єкта підприємництва:

- внутрішні конфлікти (зумовлені діями безпосередніх учасників суб'єктів підприємництва та, зазвичай, регульовані з використанням внутрішніх важелів, що передбачені установчими документами);

- зовнішні конфлікти (виникають між безпосередніми учасниками суб'єктів підприємництва та іншими учасниками його економічного оточення, і регульовані, здебільшого, за участю відповідного уповноваженого державного органу).

3. За рівнем впливу на фінансову безпеку:

- конфлікти з високим рівнем впливу;
- конфлікти з низьким рівнем впливу;
- конфлікти, що не впливають.

4. За природою виникнення:

- об'єктивно зумовлені конфлікти (породжені складними ситуаціями, в яких опинилися суб'єкти конфлікту через вплив певних чинників, зокрема, неоптимальний розподіл функцій і відповідальності);



Рис. 1.9. Систематизація фінансових конфліктів у діяльності суб'єктів підприємництва

Джерело: розробила автор

- суб'єктивно зумовлені конфлікти (виникають унаслідок особистісних характеристик сторін конфлікту).

5. За рівнем взаємодії учасників:

- вертикальні конфлікти (виникають між працівниками суб'єктів підприємництва та їхніми керівниками);

- горизонтальні конфлікти (виникають між рядовими працівниками суб'єктів підприємництва).

6. За тривалістю:

- короткотермінові конфлікти (здебільшого є наслідком взаємного непорозуміння учасників конфлікту та помилок й прорахунків, які швидко усувають);

- довготермінові конфлікти (пов'язані зі суттєвими розбіжностями бачення стратегії й тактики фінансового управління, об'єктивними труднощами щодо їхньої реалізації тощо).

7. За організаційно-правовою формою:

- конфлікти в акціонерних відносинах (корпоративні конфлікти);

- конфлікти в діяльності підприємств інших форм власності.

8. За наслідками впливу на фінансову безпеку:

- конфлікти з допустимим рівнем фінансових і репутаційних втрат;

- конфлікти з критичним рівнем фінансових і репутаційних втрат;

- конфлікти з катастрофічним рівнем фінансових і репутаційних втрат;

9. За результативністю впливу на фінансову безпеку:

- конструктивні конфлікти (здатні генерувати позитивний ефект для суб'єкта підприємництва, оскільки вони пов'язані зі суперечностями та розбіжностями щодо принципово значущих проблем його функціонування й можуть сприяти розвитку шляхом виявлення й усунення джерела розбіжностей);

- деструктивні конфлікти (гальмують розвиток суб'єкта підприємництва, зумовлюють зниження фінансових результатів діяльності, зменшують мотивацію й працездатність працівників).

10. За множинністю важелів впливу на фінансову безпеку:

- простий фінансовий конфлікт;

- гібридний фінансовий конфлікт.

Оскільки на сьогодні глобальна ситуація у сфері безпеки зазнала суттєвих, незворотних та радикальних змін, пов'язаних із появою нового

типу загроз безпеці міжнародного середовища, окремих країн та ділових одиниць, вважаємо, що сучасні конфлікти й конфлікти у майбутньому матимуть переважно гібридний характер. Відтак, доцільним, на нашу думку, є одночасно з використанням запропонованої нової класифікаційної ознаки фінансових конфліктів (множинність важелів впливу на фінансову безпеку суб'єктів підприємництва) виокремлення гібридних фінансових конфліктів у самостійну галузь наукового пізнання з метою подальшого дослідження їх видів, особливостей розвитку й розроблення інструментів ідентифікації й протидії їм.

З огляду на це, цілком виправданим у сучасних реаліях є введення в термінологічний апарат забезпечення фінансової безпеки суб'єктів підприємництва поняття “гібридний фінансовий конфлікт”, під яким пропонуємо розуміємо конфлікт, що виникає у фінансових відносинах, має переважно прихований характер і передбачає скоординоване застосування множинності методів впливу з метою реалізації тіньових фінансових інтересів його учасників.

Серед найпоширеніших на сьогодні гібридних фінансових конфліктів вважаємо за доцільне виокремити конфлікти суб'єктів підприємництва із такими учасниками його ринкового середовища (див. рис. 1.10).

Окрім того, гібридність цих протистоянь значною мірою виявляється в тому, що здебільшого в них бере участь кілька учасників, й одночасно може розвиватися декілька конфліктних взаємозв'язків. Пов'язаність досліджуваних гібридних фінансових конфліктів між собою пояснюється тим, що взаємозв'язки між ними часто генеруються під впливом сукупності спільних мотиваційних чинників та опосередковуються використанням схожих важелів впливу на досягнення тіньових фінансових інтересів. Для прикладу, за наявності гібридного фінансового конфлікту суб'єкта підприємництва із недобросовісними конкурентами часто використовуються шахрайські схеми за участю нечесних працівників. Недобросовісна конкуренція може реалізуватися також усуненням конкурента з ринку шляхом його незаконного поглинання.

Серед поданих на рис. 1.10 гібридних фінансових конфліктів вагоме місце посідає рейдерство, що видозмінюється разом з економічними та політичними процесами в країні. Сучасне рейдерство є багатограним

процесом, у якому використовуються різноманітні методи протиправного захоплення бізнесу, зокрема корупційні технології взаємодії з державними органами, витік конфіденційної фінансової інформації, економічне шпигунство, кримінальні схеми тощо.

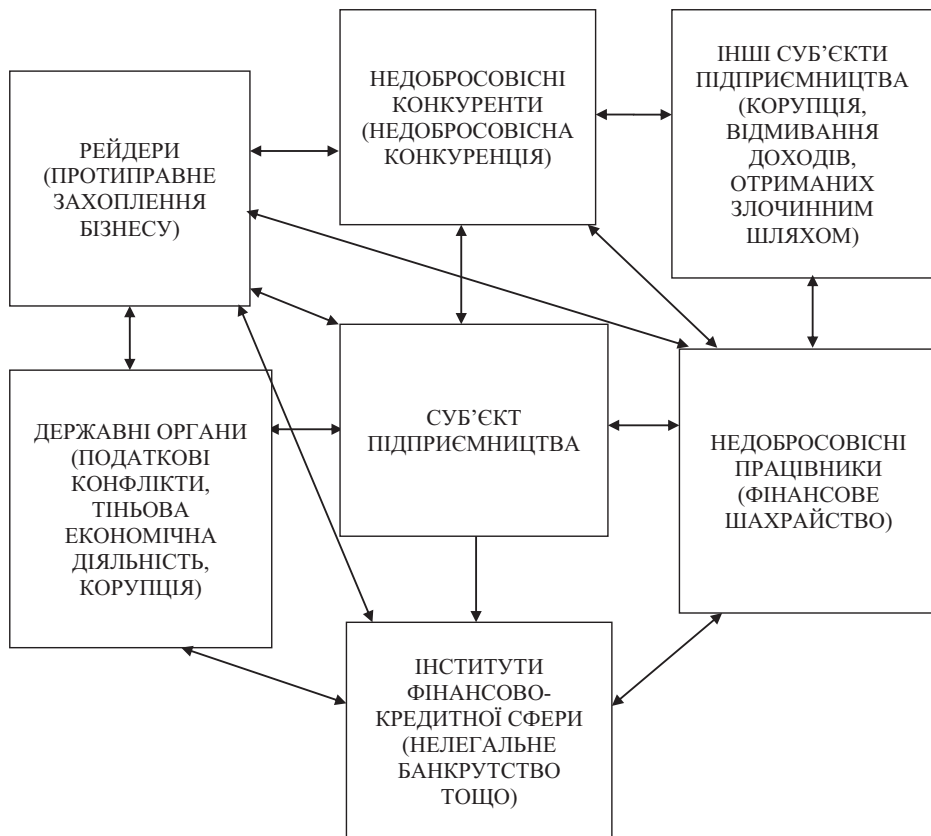


Рис. 1.10. Гібридні фінансові конфлікти: концептуалізація взаємозв'язків

Джерело: розробила автор

Ще одним гібридним конфліктом, який на сьогодні поширений у підприємницькій діяльності є фінансове шахрайство, що передбачає зумисні протиправні дії працівників ділових одиниць, що безпосередньо пов'язані з їх службовими обов'язками, з метою отримання власної вигоди та задоволення особистих фінансових інтересів. За такого гібридного фінансового конфлікту використовують

сукупність незаконних та антиморальних методів, таких як корупція, викрадення активів, несанкціоноване використання конфіденційної інформації тощо.

Окрім того, в мінливому й невизначеному ринковому середовищі важко забезпечити баланс фінансових інтересів між суб'єктами підприємництва, що конкурують в одній галузі, особливо ускладнилось це під час впровадження карантинних заходів, спричинених пандемією Covid-19. У таких умовах окремі суб'єкти підприємництва можуть застосовувати нелегальні або умовно легальні методи конкурентної боротьби, які характерні для гібридного фінансового конфлікту. Використання множинності методів недобросовісної конкуренції дає можливість одному з учасників ринку одержати комерційної вигоди і забезпечити краще становище на ринку часто обманом споживачів, партнерів, державних органів.

Структурні перетворення, що відбуваються в Україні, зокрема у фінансній сфері, ускладнені політичною нестабільністю та фінансовою кризою внаслідок пандемії Covid-19 і війни, призводять до обтяжливих для суб'єктів господарювання наслідків та зумовлюють існування конфліктів між підприємствами і державою в особі фінансних органів. Однак необхідно врахувати, що взаємовідносини у сфері оподаткування є конфліктними за своєю природою в цілому, оскільки є відображенням зіткнення індивідуальних і суспільних інтересів. Водночас завдяки імперативному методу правового регулювання індивідуальні інтереси підпорядковуються суспільним.

Для вирішення податкових конфліктів є законодавчо окреслені відповідні нормативно-правові акти та організаційно сформовані механізми їхнього регулювання (спеціальні інститути захисту прав та інтересів підприємств-платників податків). Водночас існує низка чинників, які зумовлюють виникнення гібридного фінансового конфлікту між підприємствами та фінансними органами. Це прихована форма конфлікту інтересів, яка є відображенням неприйняття державної політики в сфері оподаткування, діяльності фінансних органів та має свій вияв у переході окремих ділових одиниць у тіньовий сектор ведення бізнесу.

Поширення та зростання рівня тіньової економічної діяльності значною мірою пов'язано з неврахуванням у податковій політиці

негативних наслідків надмірного податкового навантаження на платників податків. Адже оподаткування – це не лише метод мобілізації доходів держави, а й один із вагомих чинників державного впливу на сферу функціонування суб'єктів підприємництва. Зі зростанням рівня податкового тягара потенційні вигоди завдяки ухиленню від оподаткування стають привабливими для їхніх платників і мотивують їх до переходу в тіньовий сектор підприємницької діяльності. Відтак, формуючи податкову політику, необхідно забезпечувати оптимальне співвідношення інтересів учасників податкових відносин, розробляючи найбільш ефективні конструкції взаємодії платників та фіскальних органів.

Погоджуємось із думкою З. Варналія, що тіньова економіка є однією із основних форм вияву інституціональної деформації фінансової безпеки будь-якої країни [27, с. 13]. Як найбільш вагому загрозу економічній безпеці розглядає тіньову економіку також В. Предборський [212].

Здійснення тіньової економічної діяльності є на сьогодні одним із найбільш поширених гібридних фінансових конфліктів. Гібридність у цьому випадку виражена сукупністю неконтрольованих і нерегульованих протиправних та умовно законних (законних, однак антиморальних) економічних відносин між економічними суб'єктами з метою отримання прибутку внаслідок приховування доходів і ухилення від сплати податків.

Зокрема, для цього виду економічної діяльності характерні такі ознаки [197, с. 12]:

- діяльність у сфері неформального, неврахованого, прихованого й нелегального виробництва легальної продукції, виконання легальних робіт, надання легальних послуг;

- сукупність легальних, а також неформальних, неврахованих, прихованих і нелегальних відносин між покупцями і продавцями нелегальних товарів, робіт і послуг (виробництво та збут наркотичних засобів, нелегальне виробництво та збут зброї, викрадення й збут автотранспортних засобів, нелегальна торгівля культурними цінностями й антикваріатом, нелегальні операції на ринку фінансових послуг, нелегальна торгівля трансплантатами, торгівля людьми, організована проституція, нелегальний гральний бізнес, шахрайство, рекет,

розкрадання майна з подальшою його реалізацією, контрабанда, надання послуг із відмивання нелегальних доходів тощо).

Також тіньова економічна діяльність характеризується більшою гнучкістю та динамічністю порівняно з легальним здійсненням фінансово-господарської діяльності.

Значні масштаби тіньової економіки негативно впливають на усі економічні процеси в країні та інвестиційну привабливість вітчизняних суб'єктів господарювання, що загалом знижує рівень фінансової безпеки як держави, так і її ділових одиниць. Окрім того, наявність значних обсягів тіньової економічної діяльності призводить до дезінформації суспільства про реальні економічні показники, що унеможлиблює здійснення ефективного економічного аналізу на макро- і мікрорівнях, ухвалення раціональних управлінських та законодавчих рішень. Погоджуємось із думкою З. Варналія, що ігнорування такого суперечливого та полісистемного явища, як тіньова економіка, призводить до серйозних помилок у визначенні макроекономічних показників та неадекватної оцінки найважливіших процесів і тенденцій, тактичних і стратегічних прорахунків щодо забезпечення конкурентоспроможності економіки [28, с. 48].

Суб'єкти тіньової економічної діяльності використовують різноманітні незаконні схеми, еволюціонуючи в застосовуваних методах. Від початку здобуття Незалежності України ми виявили такі схеми тіньової економічної діяльності (рис. 1.11):

Основними причинами використання офшорних схем були такі: мінливість політичної та економічної ситуації в країні, відсутність віри в ефективність державної політики, прорахунки у фінансовій політиці, недосконалість податкового й валютного регулювання в країні, високий рівень оподаткування й криміналізації суспільства і економічних процесів тощо.

Наявність офшорного підприємництва властива країнам з високим рівнем корупції, нестабільності національної валюти, низького рівня захисту інтересів власників. Відтак, це ще раз підтверджує факт існування тісного взаємозв'язку між гібридними фінансовими конфліктами не лише у схемах, які використовуються, але й у причинах їх розвитку.

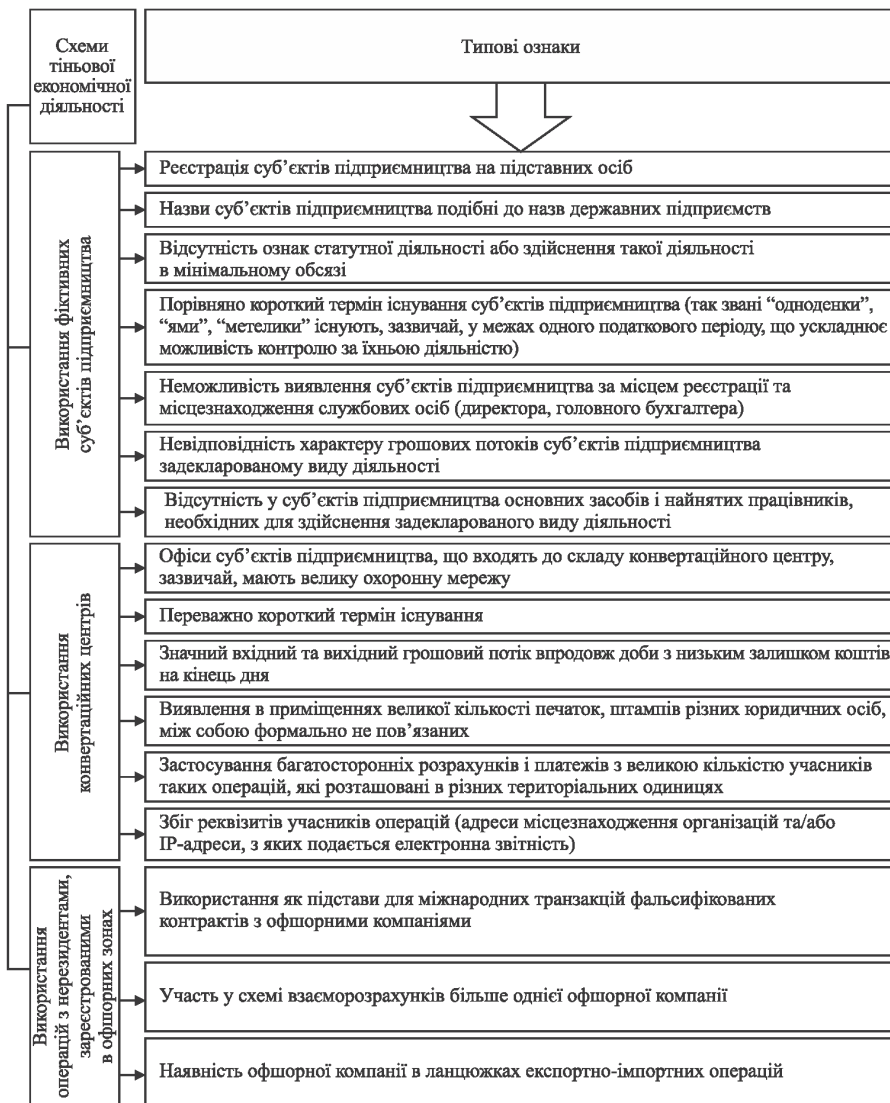


Рис. 1.11. Схеми тіньової економічної діяльності

Джерело: розробила автор

Серед причин поширення тіньової економіки в Україні в цілому, на наш погляд, доцільно виділити такі групи чинників (рис. 1.12):

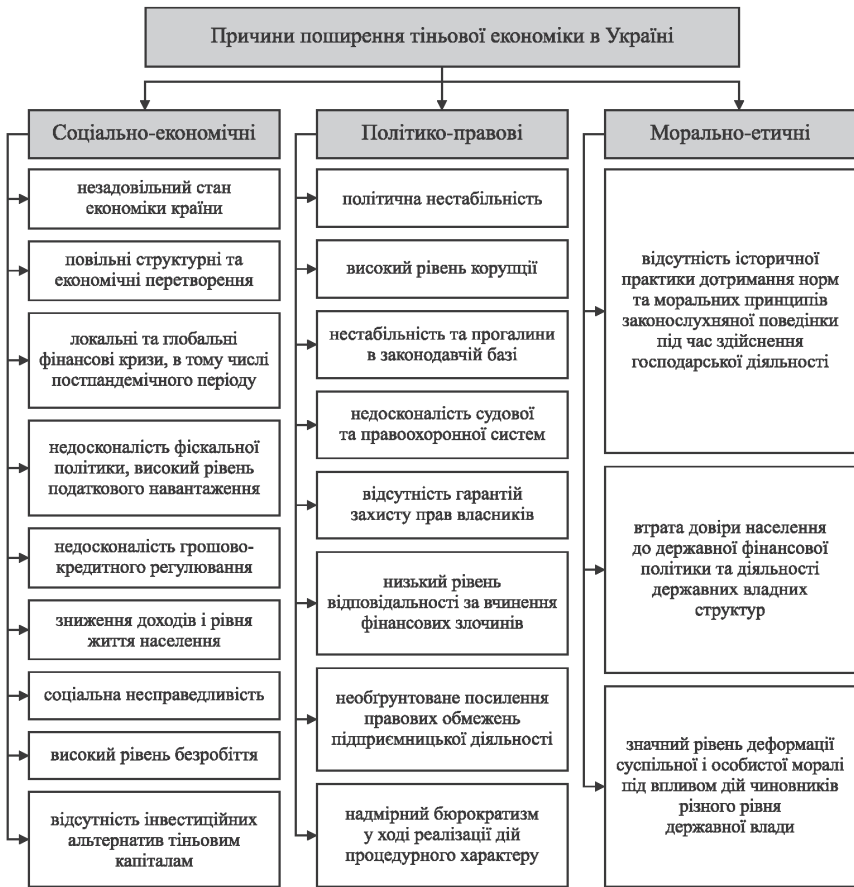


Рис. 1.12. Систематизація причин поширення тіньової економіки

Джерело: розробила автор

Наслідки поширення тіньової економічної діяльності є однією із загроз розвитку національної економіки та суттєво впливають на фінансову безпеку суб'єктів підприємництва. Аналіз підходів вчених [7; 49; 120; 123; 124 173; 286; 287; 356; 393], які досліджували цю проблематику та виявлені тіньові схеми діяльності суб'єктів підприємництва дали нам змогу виокремити чинники, які ускладнюють виявлення фактів здійснення тіньової діяльності:

- створення суб'єктами підприємництва уявлення про законний характер їхньої діяльності і приховування реального змісту виконаних операцій;

ухвалення законодавчих актів, що посилюють захист комерційної та банківської таємниці;

- застосування корупційної взаємодії зі співробітниками державних органів для прикриття злочинної діяльності;

- використання фальсифікованих документів та підставних осіб, що ускладнює виявлення виконавців у злочинній діяльності;

- складність розкриття реальних осіб, які здійснюють управління діяльністю фіктивних ділових одиниць, причетних до реалізації тіньових економічних схем;

- використання в злочинних схемах ведення бізнесу сучасних інформаційних технологій щодо управління грошовими потоками на банківських рахунках без відвідування банківських установ і можливість розпоряджатися коштами з використанням віддаленого доступу до банківських рахунків;

- використання новітніх банківських продуктів, які дають змогу отримувати готівку за межами банківських установ (банківські платіжні картки тощо);

- нераціональна організація взаємодії між органами державної влади в сфері виявлення схем тіньової економічної діяльності й обміну інформацією між ними.

У функціонуванні суб'єктів підприємництва можуть виникати також гібридні фінансові конфлікти з інститутами фінансово-кредитної системи. Зокрема, ще в давні часи, одночасно з виникненням відносин власності, сформувались основні економічні й політико-правові засади регулювання фінансової неспроможності учасників таких відносин. Для прикладу, у Давньому Римі неповернення боргів загрожувало життю й здоров'ю боржника та уможлиблювало захоплення його майна. В українській історії особливості регулювання інституту фінансової неспроможності знаходимо у першій редакції "Руської Правди" (початок XI – кінець XIII ст.), де йдеться про злісне банкрутство як різновид шахрайських дій з метою заволодіння чужим майном [300, с. 283–284].

У сучасній світовій практиці вирішення конфлікту фінансових інтересів боржника та його кредиторів відбувається за допомогою інституту банкрутства. Відтак, з одного боку, задовольняють інтереси кредиторів, надаючи їм шанс повернути вкладені кошти або внаслідок продажу (придбання кредиторами) майна боржника, або завдяки

різноманітним реорганізаційним й іншим процедурам у діяльності суб'єкта підприємництва. З іншого боку, реорганізаційні процедури дають змогу зберегти функціонування суб'єкта господарювання.

На сьогодні основним нормативно-правовим актом, який регламентує процедуру банкрутства в Україні, є Кодекс України з процедур банкрутства від 18.10.2018 року № 2597-VIII [113], відповідно до якого, банкрутство – визнана господарським судом неспроможність боржника відновити свою платоспроможність за допомогою процедури санації та реструктуризації і погасити встановлені грошові вимоги кредиторів інакше, ніж через застосування ліквідаційної процедури. Водночас, характеризуючи банкрутство, можна виділяти такі його види (рис. 1.13).

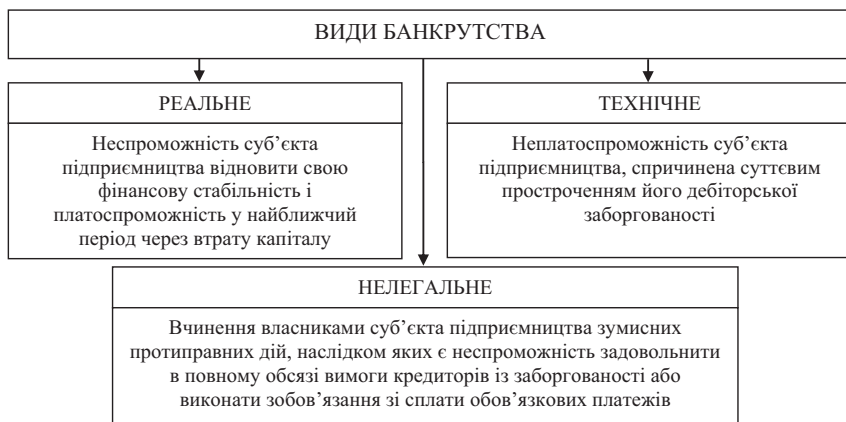


Рис. 1.13. Види банкрутства

Джерело: розробила автор

Щодо причин банкрутства, то їх можна згрупувати за такими ознаками:

- за сферою виникнення (зовнішні й внутрішні);
- за природою виникнення (об'єктивні (не залежать від намірів і дій окремих осіб, компаній і урядів – стихійні лиха, інші несприятливі природні явища, а також такі закономірності економічного розвитку, як циклічність і кризи) і суб'єктивні (дії власників, керівництва та працівників));
- за суб'єктами, що генерують загрозу банкрутства (боржник, ділові партнери, треті особи);
- за можливістю впливу на них (усувні, неусувні, важко усувні);

– за можливістю передбачення (передбачувані, непередбачувані, частково передбачувані).

Найбільшу загрозу фінансовій безпеці суб'єктів підприємництва становлять зовнішні причини банкрутства, оскільки вплив на них мінімальний, а наслідки їхньої реалізації можуть бути катастрофічними. До них відносимо:

- економічні (темп інфляції, ставки податків і банківських кредитів, курси валют, рівень доходів населення тощо);
- політичні (державна політика, здійснена з урахуванням інтересів різних груп впливу в органах державного управління та глобальних політичних процесів);
- ринкові (демографічні тенденції, життєві цикли виробів, рівень конкуренції тощо);
- технологічні (вплив на економіку науково-технологічного прогресу);
- соціокультурні (звичаї, традиції, менталітет населення, рівень добробуту, рівень його освіти, культурного розвитку тощо);
- міжнародні (глобалізація економіки, діяльність транснаціональних компаній, економічних і військово-політичних об'єднань тощо).

До внутрішніх причин банкрутства, зумовлених, здебільшого, неефективністю менеджменту, належать: відсутність довготермінової концепції розвитку; неефективність організаційної структури; низький рівень фінансової компетентності управлінського персоналу; недобросовісність та наявність зловмисних намірів у працівників; незначна частка власного капіталу; низький рівень інвестиційної активності; неефективне використання ресурсів; нераціональний розподіл прибутку.

Банкрутство суб'єктів підприємництва становить вагомий деструктивний наслідок для інших учасників їх ринкового оточення (економічні збитки бізнес-партнерів через невиконання фінансово неспроможним суб'єктом підприємства зобов'язань) та погіршує економічну ситуацію (скорочення надходження до бюджетів різних рівнів у зв'язку зі збільшенням кількості фінансово неспроможних ділових одиниць) й соціальний клімат у державі (підвищення рівня безробіття через зменшення кількості робочих місць внаслідок закриття виробничих об'єктів).

Щоб скоротити кількість фінансово неспроможних ділових одиниць на мікроекономічному рівні та на рівні держави необхідно впроваджувати організаційно-економічні заходи попередження банкрутства, передусім

важливо здійснювати діагностику фінансового стану підприємств. З цією метою використовують сукупність ознак та чинників, що генерують загрозу фінансової неспроможності ділових одиниць та методів фінансового аналізу для своєчасного розпізнавання фінансової кризи й реагування на неї з метою попередження її критичних наслідків. На основі синтезу наукових поглядів вчених [102; 105; 133; 276] та аналізу практики нами виділено такі основні ознаки загрози банкрутства: скорочення попиту на продукцію суб'єктів підприємництва та відповідне зниження обсягів її виробництва; наявність значної частки позикового капіталу в структурі капіталу; дефіцит власного оборотного капіталу; негативні тенденції фінансових параметрів розвитку; несприятливі зміни в портфелі замовлень і втрата основних контрагентів; зниження ринкової вартості акцій (в акціонерних товариствах); відсутність диверсифікації діяльності та ринків збуту; наявність простроченої дебіторської і кредиторської заборгованості; втрата досвідчених менеджерів; конфліктів між різними учасниками суб'єктів підприємництва.

Функціонування інституту банкрутства характерне для практики більшості країн і покликане шляхом реалізації спеціальних процедур господарського права вирішувати тимчасові фінансові проблеми учасників ринку або ж усувати з нього неконкурентоспроможні ділові одиниці. Водночас у певних випадках цей інститут може ставати знаряддям для реалізації тінювих інтересів окремих учасників. Використовуючи процедуру банкрутства, ці особи можуть ухилитися від своїх майнових зобов'язань.

Незаконне банкрутство пропонуємо поділяти за способом і часом вчинення злочину (рис. 1.14).

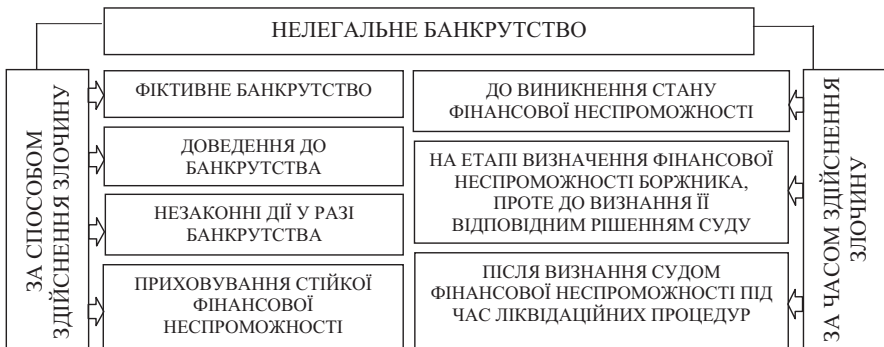


Рис. 1.14. Систематизація видів нелегального банкрутства в Україні за способом і часом вчинення

Джерело: розробила автор

Відтак, згідно з чинним вітчизняним законодавством поняття “нелегальне банкрутство” за способом вчинення злочину об’єднує такі делікти: фіктивне банкрутство, доведення до банкрутства, незаконні дії у разі банкрутства та приховування стійкої фінансової неспроможності підприємства.

Аналізуючи підходи до розуміння фіктивного банкрутства, ми виявили таке його тлумачення в нормативно-правових актах України (табл. 1.3.).

Таблиця 1.3

**Визначення поняття “фіктивне банкрутство”
в нормативно-правових актах України**

Вид нелегального банкрутства	Кодекс про адміністративні правопорушення (ст. 166-17)	Господарський кодекс України (ст. 215)	Методичні рекомендації щодо виявлення ознак неплатоспроможності підприємства та ознак дій з приховування банкрутства, фіктивного банкрутства чи доведення до банкрутства
Фіктивне банкрутство	Завідомо неправдива офіційна заява громадянина-засновника (учасника) або службової особи суб’єкта господарської діяльності, а так само громадянина-суб’єкта підприємницької діяльності про фінансову неспроможність виконання вимог з боку кредиторів і зобов’язань перед бюджетом, якщо такі дії завдали великої матеріальної шкоди кредиторам або державі	Завідомо неправдива заява суб’єкта підприємництва до суду про нездатність виконати зобов’язання перед кредиторами та державою	Завідомо неправдива офіційна заява громадянина-засновника (учасника) або службової особи суб’єкта господарської діяльності, а так само громадянина-підприємця про фінансову неспроможність виконання вимог з боку кредиторів і зобов’язань перед бюджетом, якщо такі дії завдали великої матеріальної шкоди кредиторам або державі

Джерело: сформовано на основі [112; 53; 154]

Злочин, пов’язаний із доведенням до банкрутства, визначено у Кримінальному кодексі України (ст. 219) як умисне, з корисливих мотивів, іншої особистої зацікавленості або в інтересах третіх осіб вчинення власником або службовою особою суб’єкта господарської діяльності дій, що призвели до стійкої фінансової неспроможності суб’єкта господарської діяльності, якщо це завдало великої матеріальної шкоди державі чи кредитору [132]. У цьому випадку йдеться про цілеспрямовані дії, що погіршують фінансове становище суб’єкта

підприємництва, вчинені його власниками або службовими особами (укладання свідомо невігідних контрактів, нездійснених угод із значним розміром штрафних санкцій тощо).

Відповідно до ст.166-16 Кодексу України про адміністративні правопорушення, приховування стійкої фінансової неспроможності є умисним приховуванням громадянином-засновником (учасником) або службовою особою суб'єкта господарської діяльності своєї стійкої фінансової неспроможності шляхом подання недостовірних відомостей, якщо це завдало великої матеріальної шкоди кредиторів [112].

Згідно зі ст.166-16 Кодексу України про адміністративні правопорушення, незаконні дії в разі банкрутства – це умисне приховування майна, відомостей про майно, передання майна в інше володіння або його відчуження чи знищення, а також фальсифікація, приховування або знищення документів, які відображають господарську чи фінансову діяльність, якщо ці дії вчинені громадянином-засновником (учасником) або службовою особою суб'єкта господарської діяльності в період провадження у справі про банкрутство і завдали великої матеріальної шкоди [112].

В умовах сучасних тенденцій мотивами зловживань боржниками у разі банкрутства можуть бути такі:

- намір приховання іншого злочину;
- уникнення оподаткування;
- реструктуризація боргів списанням коштів на фіктивну санацію;
- позбавлення заборгованості перед кредиторами.

Мотивами зловживань з боку кредиторів можуть бути наміри перерозподілу власності, зокрема використання банкрутства як інструменту недобросовісної конкурентної боротьби з метою придбання майна за невиправдано низькою ціною.

Аналіз судово-слідчої практики свідчить про те, що від здобуття Незалежності України використовувалися схеми, які передбачали акумулювання всіх пасивів на підприємстві-боржнику для збільшення його неплатоспроможності та виведення його активів на новостворений суб'єкт підприємництва ще до початку процедури банкрутства такими способами:

- передавання майна підприємства-боржника в статутні капітали новостворених юридичних осіб в обмін на отримання неадекватної частки участі (акцій) у них;

- погашення заборгованості за будь-якими зобов'язаннями перед конкретним кредитором, де розмір вимог кредитора значно завищений порівняно з основним боргом. У цьому випадку заборгованість збільшується завдяки сплаті штрафних санкцій, відшкодування збитків;

- безоплатне передавання майна у вигляді надання допомоги, дарування;

- свідоме ухвалення управлінських рішень у сфері управління виробництвом, які негативно позначаються на фінансовому стані підприємства;

- приховування боржником реальної до стягнення дебіторської заборгованості, що дає змогу розраховатися з кредиторами, майна або інформації про майно суб'єкта підприємництва. Зловживання з боку кредиторів полягають у тому, що вони прагнуть не одержати борг, а незаконно перехопити управління бізнесом боржника чи незаконно довести його до банкрутства для того, щоб за невиправдано низькою ціною придбати його активи;

- прямий продаж майна підприємства-боржника за заниженою ціною чи його обмін на інше майно, що не становить інтересу для боржника, відповідно до специфіки діяльності боржника, а також обмін майна боржника на інше майно, вартість якого є завищеною;

- передавання майна за договорами про надання послуг нематеріального характеру (маркетингових, консалтингових, юридичних, консультативних тощо);

- зняття з розрахункового рахунку суб'єкта підприємництва коштів та їхнє привласнення;

- перерахування коштів контрагенту на підставі фіктивного договору;

- фактичне зменшення майна суб'єкта підприємництва, що полягає в таких діях:

- а) укладення явно не вигідних, збиткових угод, тобто угод, які розраховані на менший прибуток порівняно з витратами (наприклад, реалізації продукції підприємства за умисно зниженими цінами, придбання сировини й матеріалів за спеціально завищеними цінами, надання кредитів особам, які завідомо не збираються їх повертати);

- б) кредитування на велику суму, яке роблять незадовго до банкрутства (фінансової неспроможності) за незначного розміру дивіденду;

в) незаконні перекази коштів на рахунок інших підприємств, їхнє зняття та привласнення;

д) переказ коштів за кордон за фіктивними контрактами; використання коштів на купівлю особистих речей [288, с. 65–67].

Суб'єктами нелегального банкрутства можуть бути як власники, й керівники ділової одиниці, так і конкуренти, представники державних органів, які зацікавлені у її банкрутстві. У випадку, коли ініціатором нелегального банкрутства є власник, його мотивацією зазвичай є намір стати одноосібним власником, відсторонивши від управління інших учасників. Зовнішнього замовника нелегального банкрутства може цікавити придбання суб'єкта підприємництва на суму, значно нижчу від його реальної вартості, або для подальшої приватизації земельної ділянки, на якій розташований об'єкт власності. Інколи усуненням керівництва збанкрутілої ділової одиниці ініціатор банкрутства має намір усунути свого конкурента.

Серед причин поширення злочинів у сфері банкрутства виділяють низький рівень правової захищеності економічних відносин та значну латентність серед таких злочинів. За оцінками фахівців, латентність злочинів у сфері економіки становить від 60 до 95 %, вагому частку серед них займає нелегальне банкрутство [298];

Поширення нелегального банкрутства становить вагому загрозу фінансовій безпеці ділових одиниць та державі, оскільки порушується порядок господарської діяльності, регламентований чинним законодавством, завдається майнова шкода кредиторам, державі, іншим господарюючим суб'єктам.

Розглянувши прояви окремих гібридних фінансових конфліктів в практиці функціонування суб'єктів підприємництва, ми виявили, що вони поєднують сукупність принципово різних способів досягнення фінансових цілей. Типовими їх компонентами є використання методів, що сприяють виникненню та поглибленню в діяльності ділових одиниць протистоянь та створення агресором у їхньому внутрішньому середовищі певних фінансових протиріч та суперечок з подальшим їхнім використанням для досягнення фінансових цілей агресії. Також ці методи можуть включати здійснення шпигунської ділової діяльності, шантаж, кіберзлочини та інші види протиправної поведінки, що скоординовано застосовуються з метою реалізації фінансових інтересів та досягнення певних фінансових цілей однією із конфліктуючих сторін.

Попри застосування сукупності різних способів досягнення тіньових фінансових цілей, гібридним фінансовим конфліктам притаманні і спільні риси. В цьому контексті пропонуємо узагальнену їх характеристику за такими ознаками та деструктивними наслідками для фінансової безпеки (рис. 1.15).

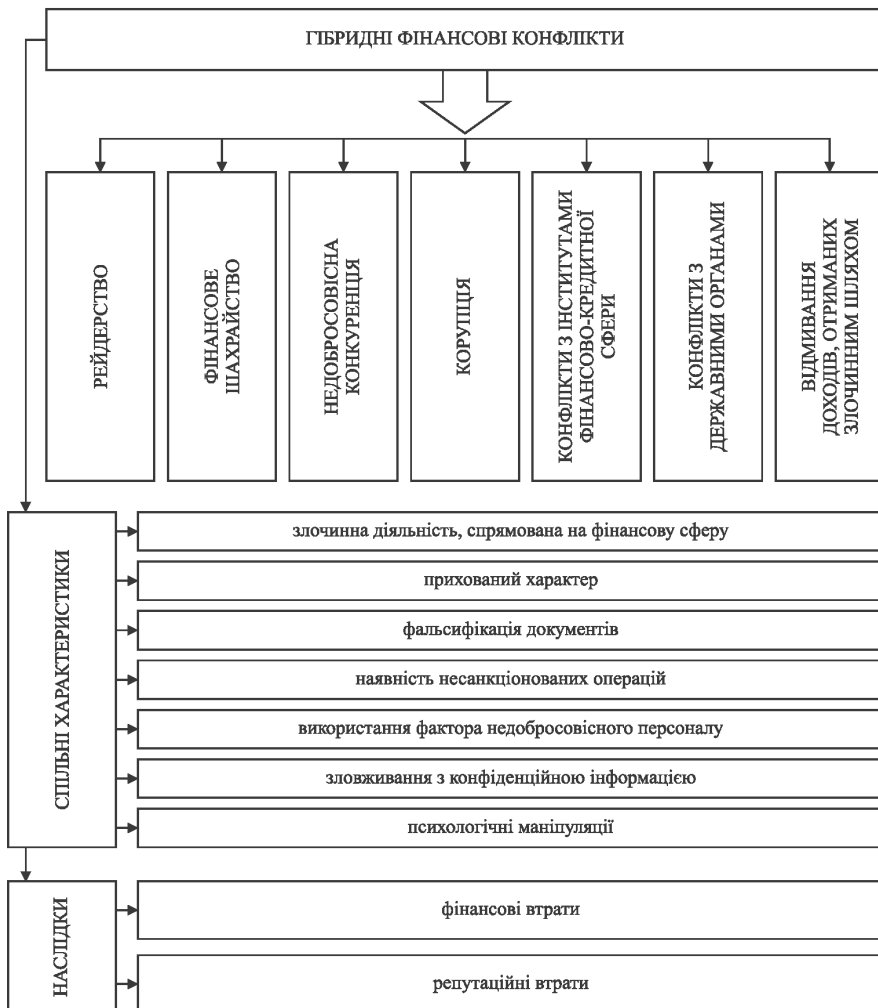


Рис. 1.15. Узагальнена характеристика гібридних фінансових конфліктів

Джерело: розробила автор

Гібридні фінансові конфлікти не лише спричиняють деструктивні наслідки для фінансової безпеки суб'єктів підприємництва, а й становлять суспільну небезпеку. Водночас необхідно констатувати, що виникнення й розвиток фінансових конфліктів у конкурентному ринковому середовищі є неминучим явищем й необхідно виокремити також і певне їхнє позитивне функціональне значення у майбутньому у випадку їх вирішення. Конфлікти еволюціонують разом з еволюцією суспільства, оскільки це природні закономірні процеси його розвитку. Зокрема, один із фундаторів соціологічної теорії конфлікту Г. Зіммель уважав конфлікт універсальним явищем, стверджуючи, що безконфліктне суспільство не має механізму саморозвитку. Саме конфліктність як форма суперечностей спонукає суб'єктів фінансової діяльності до розвитку та вдосконалення [268, с. 535]. Позитивний ефект конфліктів був обґрунтований також у працях Р. Дарендорфа, який уважав конфлікт джерелом розвитку та вдосконалення будь-якої соціальної системи [359, с. 135].

Згідно з концепцією позитивно-функціонального конфлікту Л. Козера, не може бути соціальних груп без конфліктних взаємовідносин, водночас вони відіграють вагомий роль у послабленні соціального напруження, мінімізації рівня суперечностей між людьми та соціальними групами і спроможні позитивно впливати на внутрішню консолідацію груп [357, с. 233]. Погоджуємось із думкою вченого, що конфлікт може бути важливим чинником підтримання динамічної рівноваги в соціально-економічних системах. Своєю чергою вважаємо, що спроможність суб'єктів підприємництва зберігати динамічну рівновагу в гібридних фінансових конфліктах є запорукою їх фінансової безпеки.

Відтак, гібридні фінансові конфлікти, з одного боку, можуть загальмувати розвиток ділових одиниць, призвести до їх протиправного захоплення або ліквідації, з іншого боку, будучи вчасно розпізнаними, можуть також стимулювати їх розвиток. Оскільки кризові умови зумовлюють виявлення вразливостей у системі фінансової безпеки, що може стати своєрідним фільтром для її очищення від деструктивних елементів й сприяти формуванню нової більш досконалої системи взаємодії зі суб'єктами економічного середовища. Тому виняткового значення у сфері безпекової політики набуває розроблення методологічних засад забезпечення фінансової безпеки суб'єктів підприємництва із урахуванням впливу гібридних фінансових конфліктів.

РОЗДІЛ 2.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ЧИННИКІВ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

2.1. Концептуальні підходи до вивчення чинників фінансової безпеки суб'єктів підприємництва в Україні

Розкриття особливостей забезпечення фінансової безпеки суб'єктів підприємництва потребує застосування сучасного, відповідного кризовим умовам постпандемічного періоду й гібридних агресій, методологічного інструментарію дослідження. З огляду на необхідність виокремлення гібридних фінансових конфліктів у самостійну галузь наукового пізнання, що відповідає потребам нової глобальної ситуації у сфері безпеки, можна констатувати, що забезпечення фінансової безпеки суб'єктів підприємництва на сьогодні вимагає утримання їх динамічної фінансової рівноваги та постійного пошуку балансу інтересів з інтересами інших учасників економічного середовища. Відтак, уважаємо, що методологія наукового дослідження чинників фінансової безпеки ділових одиниць повинна реалізовуватись із врахуванням двох ключових концептуальних підходів – фінансового – при розкритті проблем забезпечення динамічної фінансової рівноваги та соціально-психологічного – у процесі вивчення гібридних фінансових конфліктів.

Під методологією розуміємо концептуалізацію мети, об'єкта, предмета, методів й принципів дослідження, які забезпечують отримання достовірної, максимально об'єктивної, систематизованої інформації про процеси та явища. Об'єктом дослідження є те, на що спрямована пізнавальна діяльність, зокрема процес або явище, що зумовлює проблемну ситуацію. Предметом дослідження є властивості, характерні для наукового пізнання, це визначення певного аспекту дослідження як припущення про найістотніші для вивчення вибраної проблеми характеристики об'єкта.

Відтак, визначивши мету наукового пізнання особливостей забезпечення фінансової безпеки суб'єктів підприємництва шляхом розкриття проблем забезпечення їх динамічної фінансової рівноваги та

вивчення гібридних фінансових конфліктів, методологію наукового дослідження із врахуванням цих двох підходів подано в структурно-логічній схемі (рис. 2.1).



Рис. 2.1. Структурно-логічна схема методології наукового дослідження чинників забезпечення фінансової безпеки суб'єктів підприємництва

Джерело: розробила автор

Відповідно до фінансового підходу об'єктом наукового пізнання ми визначили фінансові параметри суб'єктів підприємництва, предметом дослідження – динамічну фінансову рівновагу ділових одиниць. Відповідно до соціально-психологічного підходу об'єктом наукового пізнання є гібридні фінансові конфлікти суб'єктів підприємництва, предметом дослідження є динамічна рівновага в гібридних фінансових конфліктах.

У сучасних економічних дослідженнях висвітлюється багатовекторність вчення про рівновагу. Особливості рівноважного стану системи ідентифікують як специфіку її циклічного розвитку, зокрема, визначають іманентні характеристики кризи [42, с. 138]. Погоджуємось із думкою А. Гальчинського, що при цьому необхідно враховувати те, що рівновага будь-якого рівня економічної ієрархії має свої особливості з огляду на складність економічної системи та мету її розвитку, досягненню якої підпорядковується завдання забезпечення рівноважного стану; специфіку історичного часу та структуру економічного простору [43, с. 141].

Зокрема, І. Гонгарева зазначає, що рівновага передбачає такий стан, для підтримки якого потрібні мінімальні витрати трудових, сировинних, енергетичних та інформаційних ресурсів [51, с. 201]. Тобто під рівновагою учена розуміє незмінність показників системи з допустимими відхиленнями від їх заданих рівнів, що не потребують значних витрат різних ресурсів.

Водночас, вважаємо, що стан рівноваги властивий виключно системам, що не мають зв'язків із зовнішнім середовищем, тоді як для відкритих систем, до яких належить національна економіка і суб'єкт підприємництва, рівновага можлива лише як мить у процесі постійних змін. Відкриті соціально-економічні системи не можуть перебувати у стані спокою, адже вони постійно взаємодіють із мінливим зовнішнім середовищем. Окрім того, в умовах глобалізації усіх фінансових процесів, стрімкого розвитку інформаційних технологій, поширення гібридних агресій можна констатувати, що економіка перебуває в хаосі, суб'єкти підприємництва – у турбулентній нестійкості. Відтак, на сьогодні немає лінійних залежностей, вони нелінійні, тому є складно прогнозованими. Крім того, рух суб'єктів підприємництва в їхньому життєвому циклі завжди є конфліктним. Ділові одиниці, здійснюючи свою фінансово-господарську діяльність та перебуваючи в постійному русі, зіштовхуються з постійними змінами внутрішнього та зовнішнього середовища, гібридними фінансовими конфліктами, а отже – із втратою рівноваги та пошуком можливості їхнього повернення до рівноважного стану, який характеризується визначеними значеннями параметрів діяльності або ж знаходженням нового стану рівноваги. Отже, впродовж життєвого циклу відбувається постійний перехід господарюючих суб'єктів із одного

рівноважного стану в інший. Ця постійна зміна, динаміка станів відображає особливості їх функціонування в часі. Тому ми вважаємо, що доцільно вживати щодо діяльності суб'єктів підприємництва поняття “динамічна рівновага”, що дає змогу усунути будь-які аспекти сталості, статичності та заперечення змін. Водночас необхідно акцентувати, що період нестійкості ділових одиниць, коли стан вихідної рівноваги порушено, а нову рівновагу ще не сформовано, повинен бути короткостроковим, оскільки при довгостроковому порушенні рівноваги їхньому функціонуванню загрожують деструктивні наслідки, зокрема неспроможність протидіяти внутрішнім та зовнішнім загрозам фінансовій безпеці. Тобто рівновага і розвиток, як два несумісні стани, не можуть одночасно домінувати в діяльності суб'єктів підприємництва: вони можуть перебувати або в стані рівноваги, або в стані розвитку, а значить нерівноваги. Відтак, можемо визначити, що для того, щоб ділові одиниці були успішними та у стані фінансової безпеки, необхідні обидва стани, однак за умов злагодженої зміни їх у часі, що можливо за умов стійкості, як однієї із характеристик фінансової безпеки.

Спектр підходів до тлумачення поняття “стійкість” у лексикографічних джерелах є доволі широким, зокрема:

- стійкість – здатність довго зберігати і проявляти свої властивості, не піддаючись руйнуванню і псуванню [273, с. 710];

- стійкість – здатність об'єкта, системи, виведеної зі стійкого стану, самостійно повертатися у цей стан [38].

У контексті забезпечення фінансової безпеки будемо розуміти під стійкістю суб'єктів підприємництва їх спроможність протидіяти сукупності чинників, явищ і дій осіб, що здатні вивести їх із вихідного стану статичної або динамічної рівноваги та здатність самостійно повертатися у цей стан у випадку виведення із нього.

Кожен суб'єкт підприємництва для забезпечення ефективного функціонування в перспективі повинен розвиватися. З позицій теорії систем та концепцій самоорганізації розвиток ділової одиниці передбачає значні якісні зміни її структури, зв'язків й режиму функціонування. Тому вважаємо, що умовну сукупність точок у просторі, в яких суб'єкт підприємництва досягає стану динамічної рівноваги, можна розглядати як лінію бажаного (запланованого) розвитку, коли узгоджуються його потреби та ресурси, як траєкторію його еволюції. Відтак, стійкість

функціонування господарюючого суб'єкта передбачатиме стійкість з досягнення його цілей у конкретний період часу. Узагальнюючи та об'єднуючи розуміння таких станів суб'єкта підприємництва, як “рівновага”, “динамічна рівновага”, “періоди нерівноваги (розвитку)”, поняття “стійкість” у цьому контексті, на нашу думку, передбачає здатність суб'єкта підприємництва забезпечувати оптимальний у часі перехід із одного рівноважного стану в інший шляхом усунення впливу дестабілізуючих чинників чи адаптації до нових умов внутрішнього й зовнішнього середовища або відхилення від рівноваги з подальшим поверненням у вихідний рівноважний стан без втрати цілісності. Графічну ілюстрацію динамічної рівноваги суб'єктів підприємництва в траєкторії його еволюції подано на рис. 2.2.

Періоди нерівноваги – біфуркації передбачають процес якісного переходу ділових одиниць від стану рівноваги до хаосу або порядку, більш вищого рівня розвитку через певні збурення. У точці біфуркації відбувається “коливання” щодо вибору можливого напрямку розвитку.



Рис. 2.2. Динамічна рівновага суб'єктів підприємництва в процесі їх розвитку

Джерело: розробила автор

Тому в контексті забезпечення фінансової безпеки важливим є врахування того, що навіть незначний вплив окремого чинника чи їхньої сукупності визначає розвиток суб'єкта підприємництва у певному напрямі, у тому числі й небажаному. В широкому розумінні “точка біфуркації” є останньою зміною параметра, яка супроводжує настання небажаної ситуації. Тому забезпечення фінансової безпеки ділових одиниць потребує злагодженої роботи усіх їх суб'єктів управління щодо досягнення визначених фінансових параметрів розвитку та узгодження їх інтересів із інтересами учасників внутрішнього та

зовнішнього середовища в процесі ділової взаємодії. Оскільки суб'єкт підприємництва може характеризуватися високими фінансовими показниками розвитку, проте стати об'єктом гібридної агресії (фінансового шахрайства, недобросовісної конкуренції, рейдерства, корупції тощо). Тому фінансова безпека господарюючого суб'єкта відображає здатність забезпечення його динамічної рівноваги як з позиції забезпечення фінансової стійкості, тобто здатності забезпечувати перехід із одного рівноважного фінансового стану в інший, так і з позиції стійкості в протидії гібридним фінансовим конфліктам. Відтак, пропонуємо тлумачити фінансову безпеку суб'єктів підприємництва як спроможність зберігати динамічну фінансову рівновагу та рівновагу в гібридних фінансових конфліктах.

Проаналізувавши публікації, присвячені поняттю “фінансова рівновага” (табл. 2.1), узагальнивши й систематизувавши погляди вчених щодо його тлумачення, розуміємо під фінансовою рівновагою суб'єктів підприємництва такий стан, який характеризується високим рівнем їх фінансової стійкості і платоспроможності на всіх етапах розвитку, забезпечується формуванням оптимальної структури капіталу, авансуванням в необхідних обсягах у високоліквідні активи й спроможністю виконати зобов'язання перед усіма учасниками ділової взаємодії.

Таблиця 2.1

Підходи до тлумачення понять “фінансова рівновага”

Автор	Дефініція
Т. Гудзь [57, с.6]	Збалансування процесів формування фінансового стану підприємства залежно від інтенсивності їх протікання, напрямку зміни, характеру внутрішньої взаємодії та чутливості до впливу зовнішніх факторів
Л. Мельник [150, с. 24]	Збалансованість між власним та залученим капіталом
М. Білик [15]; І. Бланк [19]	Ситуація, коли є відповідність обсягів формування та використання (споживання) власних фінансових ресурсів
І. Кладченко [108, с. 371]	Певний стан підприємства, який відображує його спроможність забезпечення виконання власних фінансово-майнових зобов'язань перед іншими господарськими суб'єктами завдяки ефективно організованій роботі з власними засобами, за рахунок оптимальної структури активів підприємства та ефективності їх використання та правильно сформованих пасивів

Джерело: систематизувала автор на основі [15; 19; 57; 108; 150]

Гібридні фінансові конфлікти характеризуються складною системою взаємозв'язків учасників та множиною важелів впливу на досягнення

їхніх тіньових інтересів. Утримувати рівновагу в агресивному зовнішньому середовищі досить складно, водночас суб'єкти підприємництва, взаємодіючи з іншими учасниками ринку, постійно перебувають у пошуку певного балансу інтересів.

Визначені об'єкти та предмети дослідження чинників фінансової безпеки суб'єктів підприємництва передбачають встановлення методів та принципів наукового пізнання. Важливо визначити способи збору інформації щодо фінансово-господарської діяльності суб'єкта підприємництва та наявності гібридних фінансових конфліктів, окреслити методи аналізу отриманих даних й прогнозування ситуації на майбутнє.

Як ми зазначили раніше, окреслені цілі пропонуємо реалізувати зі застосуванням фінансового та соціально-психологічного підходів, а також з метою додаткової перевірки, підтвердження, пояснення висунутих гіпотез та обґрунтування висновків використовуватимемо метафоричний підхід, який на сьогодні набуває широкого застосування в цілях альтернативного висвітлення економічних явищ. Так, доцільними в контексті забезпечення фінансової безпеки суб'єктів господарювання в умовах гібридних фінансових конфліктів є, на наш погляд, такі теорії:

– теорія “розбитих вікон”, яку сформулювали американські соціологи Дж. Вілсон і Дж. Келлінг у 1982 році [376], ключовою тезою якої є те, що безкарність породжує всюдозволеність;

– теорія чорного лебедя – метафора, розроблена дослідником Н. Талебом [281], що описує виникнення раптових, неможливих для прогнозування ситуацій, які здатні повністю змінити наявні парадигми;

– теорія “сірого носорога” М. Вуккера [399], що описує ситуації з надзвичайно високим ризиком реалізації негативного сценарію розвитку подій, які є очевидними й можливими для управління ними, водночас залишаються поза увагою;

– теорія “королівського дракона” Д. Сорнетта [388], яка характеризує важкопрогнозовані події, що зумовлені діями особливих специфічних механізмів зі значними руйнівними наслідками, які, однак, можливо передбачати й навіть контролювати.

Застосування метафоричного підходу до пояснення чинників фінансової безпеки суб'єктів підприємництва дасть змогу підвищити рівень обґрунтування отриманих результативних даних та пояснити взаємозв'язки між ними за допомогою додаткової форми подання отриманих результатів.

Сукупність фінансового, соціально-економічного й метафоричного (додатковий) підходів забезпечить комплексний характер наукового пізнання чинників фінансової безпеки з метою отримання більш повних й достовірних результатів.

2.2. Використання сучасних методів виявлення закономірностей у забезпеченні фінансової безпеки суб'єктів підприємництва

Множинність та складність чинників формування фінансової безпеки суб'єктів підприємництва зумовлює необхідність врахування при науковому дослідженні цієї проблематики системного підходу (об'єкт дослідження розглядається як система, що об'єднує певну множину взаємодіючих елементів у єдине ціле; взаємозв'язок системи та її складових підпорядковується діалектиці цілого і частинного, загального й окремого). Системність у цьому випадку буде виявлятися передусім в об'єднанні двох підходів до вирішення проблем фінансової безпеки – фінансового та соціально-психологічного. Це своєю чергою допоможе забезпечити ефект синергії – зростання ефективності дослідження в результаті інтеграції окремих об'єктів наукового пізнання в єдину систему та виявлення внаслідок цього принципово нових закономірностей їх розвитку.

Методи наукового дослідження – це сукупність способів і прийомів, які використовуються в певній галузі знань для дослідження закономірностей, що становлять її об'єкт та предмет. Використання комбінації методів наукового пізнання дає можливість знайти оптимальний або альтернативний до наявних, шлях до наукової істини. Наукове пізнання передбачає два рівні дослідження – емпіричний і теоретичний. Емпіричний рівень пов'язаний із отриманням і обробленням початкового фактичного матеріалу, статистичних даних емпіричного об'єкта про тенденції його розвитку. Теоретичний рівень наукового дослідження передбачає перехід від конкретного до абстрактного задля того, щоб на основі наукових абстракцій вивчити конкретні аспекти проблематики, але на більш високому рівні. Візуальну інтерпретацію методів і принципів наукового дослідження чинників забезпечення фінансової безпеки суб'єктів підприємництва подано на рис. 2.3.

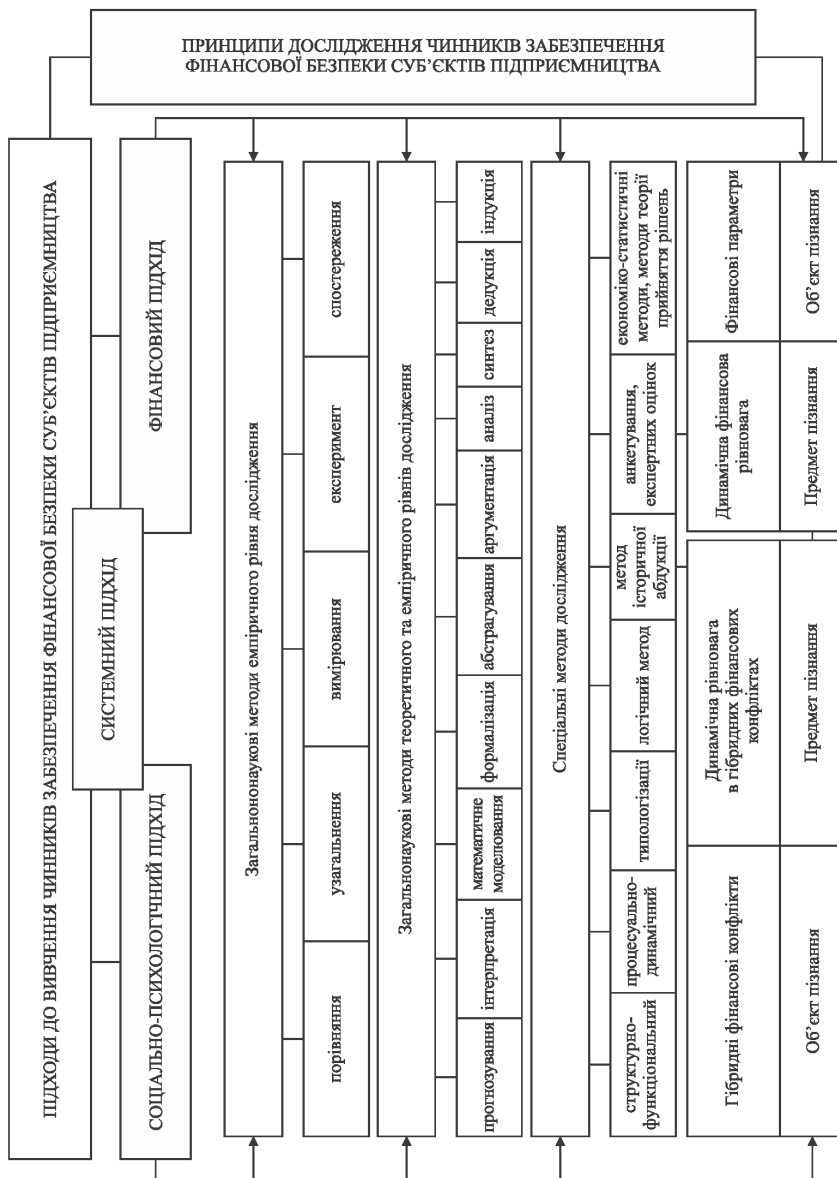


Рис. 2.3. Структурно-логічна схема використання методів та принципів наукового дослідження чинників забезпечення фінансової безпеки суб'єктів підприємництва

Джерело: розробила автор

Дослідження чинників фінансової безпеки суб'єктів підприємництва повинно ґрунтуватись як на загальнонаукових методах, які застосовують для різних наук, так і на спеціальних – при розв'язанні прикладних наукових завдань. Це пояснюється тим, що система методів вивчення засад забезпечення фінансової безпеки перебуває на стадії становлення, враховуючи відносно короткий період від початку її виокремлення в самостійну галузь знань й, водночас, вже потребує оновлення в зв'язку із появою нового типу загроз. Окрім того, проблематика розвитку гібридних фінансових конфліктів на сьогодні загалом є ще малодослідженою й методологічний інструментарій її пізнання потребує розроблення.

Враховуючи міждисциплінарний підхід розкриття усіх аспектів фінансової безпеки суб'єктів підприємництва, крім економічних методів, необхідно використовувати методи, що застосовують у дослідженнях таких наук, як право, політологія, соціологія, філософія, психологія, менеджмент, інформатика, математика тощо.

Дослідження фінансової безпеки суб'єктів підприємництва передбачає використання таких загальнонаукових методів наукового пізнання:

- методи, що використовують на теоретичному рівні дослідження (індукція, дедукція, системний підхід);
- методи, що використовуються як на теоретичному, так і на емпіричному рівнях дослідження (формалізація, абстрагування, аналіз і синтез, систематизація, узагальнення, моделювання);
- методи емпіричного дослідження (спостереження, експеримент, вимірювання, оцінювання, порівняння, візуально-графічні прийоми).

До методів теоретичного та емпіричного рівнів вивчення проблем забезпечення фінансової безпеки суб'єктів господарювання відносимо такі:

- індукція (логічний прийом дослідження, що пов'язаний із узагальненням результатів спостереження та експерименту і рухом мислення від одиничного до загального);
- дедукція (метод переходу від знання загальних закономірностей до окремого його прояву);
- аналіз (поділ предмета дослідження на складові з метою всебічного його вивчення);
- синтез (об'єднання раніше виділених частин предмета в єдине ціле);

- аргументація (раціональний спосіб переконання шляхом обґрунтування та оцінювання доводів на захист певної тези);
- абстрагування (відокремлення істотного від неістотного);
- формалізація (відображення об'єкта чи явища в знаковій формі);
- моделювання (заміна реального процесу певною конструкцією, яка відтворює основні, найістотніші риси процесу, абстрагуючись від другорядних, неістотних);
- інтерпретація (розкриття змісту явища, тексту чи знакової форми, що сприяє їх розумінню).

Серед методів емпіричного дослідження чинників фінансової безпеки суб'єктів підприємництва виділяємо такі:

- спостереження (збір даних про соціально-економічні явища та процеси шляхом фіксації фактів чи опитування респондентів);
- експеримент (науковий дослід у спеціально створених і контрольованих умовах, які дослідник може відтворювати неодноразово, визначати їх вплив на перебіг відповідних процесів);
- вимірювання (надання властивостям явища чи процесу певних значень);
- узагальнення (комплекс послідовних дій щодо зведення конкретних поодиноких фактів у єдине ціле з метою виявлення типових рис і закономірностей, притаманних досліджуваному явищу);
- порівняння (встановлення подібності або відмінностей різних об'єктів дослідження за певними ознаками).

До спеціальних методів дослідження чинників фінансової безпеки ділових одиниць зачисляємо економіко-статистичні методи, методи теорії прийняття рішень, анкетування, експертних оцінок тощо.

Дослідження проблем формування фінансової безпеки суб'єктів підприємства крізь призму забезпечення динамічної рівноваги в гібридних фінансових конфліктах передбачає використання сукупності конкретних методик і процедур. Методологічні основи конфліктології зорієнтовані на вивчення конфліктів і причин, що сприяють їх виникненню, на розкриття закономірностей їх розвитку, пошук шляхів розв'язання конфліктів. З метою наукового аналізу конфліктологія спирається на відомі закони і категорії філософської науки. Наприклад, закон єдності й боротьби протилежностей є методологічною основою вивчення конфліктуючих сторін та причин конкретного виду конфлікту.

Такі поняття, як необхідність і випадковість, причина й наслідок, загальне й одиничне, сутність і явище, сприяють розкриттю змісту базових понять у конфліктології. Це дає змогу встановити мотиви виникнення конфліктів, прогнозувати їх розвиток та вирішення.

Методологія дослідження конфліктів передбачає цілісну систему методів і засобів отримання наукових даних про конфліктні взаємозв'язки, серед яких своєю чергою розрізняють загальнонаукові та спеціальні методи таких досліджень. До спеціальних методів у цьому контексті відносимо:

- структурно-функціональний (виявлення ключових елементів конфліктних взаємозв'язків та визначення ролі кожного з них);
- процесуально-динамічний (вивчення конфлікту шляхом дослідження його основних етапів);
- метод типологізації (класифікація форм конфліктних взаємозв'язків, їх основних сутнісних характеристик).

Врахування соціально-психологічного підходу при вивченні конфліктів передбачає використання спеціальних методів з інших галузей знань – математики, соціології, психології. Найбільшого поширення у вивченні конфліктів набули методи опитування, зокрема шляхом формування опитувальника з необхідними для розкриття питаннями та здійснення анкетування. Одночасно з опитуванням доцільним є використання експертного методу для встановлення оцінки отриманих результатів анкетування.

Цікавим та корисним, на наш погляд, у контексті вивчення гібридних фінансових конфліктів є використання математичних прийомів. Підтвердженням цього є своєрідне поняття “математика конфлікту”, яке ввели американські математики Дж. Непман та О. Моргенштерн у 1944 році. Відтак, математичні моделі допомагають виявити приховані закономірності функціонування конфліктних взаємовідносин, а математичне опрацювання великого обсягу статистичного матеріалу сприяє формуванню чітких та достовірних результатів. Для моделювання узгодження інтересів конфліктуючих сторін використовують теорію ігор. Метою застосування цього інструменту математичного апарату є визначення інтересів учасників конфлікту, знаходження можливих варіантів узгодження їхніх інтересів і прогнозування розвитку подій відповідно до зробленого конфліктерами вибору.

Одночасно з методами наукового пізнання важливим є врахування принципів наукового дослідження. Ключовим із них є, на нашу думку, принцип системності, сутність якого виявляється у застосуванні комплексного підходу в характеристиці складних об'єктів і предметів наукового пізнання й орієнтує дослідження на розкриття їх цілісності та виявлення всіх типів взаємозв'язків між ними, інтеграція їх у єдину систему знань. Системний характер аналітичних досліджень фінансової безпеки суб'єктів підприємництва посилюється також в умовах зростаючої складності їх взаємодій з іншими учасниками ринку, гібридної природи виникаючих фінансових конфліктів, багатовекторності управлінських рішень.

Важливим принципом наукового пізнання проблем формування фінансової безпеки суб'єктів підприємництва є принцип усебічності, що забезпечує багатоаспектність дослідження і дає можливість охарактеризувати ключові категорії фінансової безпеки у взаємозв'язку з іншими поняттями, явищами та процесами.

Принцип обґрунтованості допомагає розкрити усі чинники об'єктивного та суб'єктивного характеру, що визначають динамічну фінансову рівновагу суб'єктів підприємництва та зумовлюють виникнення гібридних фінансових конфліктів.

Застосування комплексу методів наукового пізнання із врахуванням принципів системності, усебічності та обґрунтованості дасть змогу поглибити розуміння основних чинників фінансової безпеки суб'єктів підприємництва і сформулювати обґрунтовані висновки та рекомендації.

Водночас, зауважимо, що ми виділили найбільш універсальні принципи дослідження чинників фінансової безпеки, проте сукупність принципів, що будуть враховані при детальному розкритті кожного досліджуваного гібридного фінансового конфлікту (рейдерство, фінансове шахрайство, недобросовісна конкуренція та корупція), визначимо в процесі їхнього структурно-компонентного аналізу.

Окремі аспекти структурно-компонентного аналізу гібридних фінансових конфліктів у контексті забезпечення фінансової безпеки суб'єктів підприємництва пропонуємо здійснювати за допомогою опитування власників/керівників суб'єктів підприємництва. З цією метою ми розробили анкету, яка містить такі блоки питань:

1. Випадки фінансового шахрайства, вчиненого працівниками суб'єкта підприємництва впродовж 2017–2021 рр. у розрізі:

- 1.1. суб'єктів зловмисних дій з оцінкою впливу окремих чинників на вчинення фінансового шахрайства;
 - 1.2. видів фінансового шахрайства з оцінкою впливу окремих чинників на його вчинення;
 - 1.3. обсягів фінансових втрат, відвернених фінансових втрат та суми витрат на заходи із протидії фінансовому шахрайству;
 - 1.4. методів виявлення фінансового шахрайства та їхньої ефективності;
 - 1.5. суб'єктів, що повідомляли про випадки фінансового шахрайства;
 - 1.6. способів повідомлень про фінансове шахрайство.
2. Злочини у сфері інформаційної безпеки суб'єкта підприємництва впродовж 2017–2021 рр. у розрізі:
 - 2.1. їх видів з оцінкою впливу окремих чинників на їх вчинення;
 - 2.2. обсягів фінансових втрат, відвернених фінансових втрат та суми витрат на заходи із протидії злочинам у сфері інформаційної безпеки;
 - 2.3. методів виявлення злочинів та їхньої ефективності.
 3. Загроза протиправного захоплення суб'єкта підприємництва в розрізі:
 - 3.1. випадків рейдерства;
 - 3.2. схем протиправного захоплення;
 - 3.3. розміру втрат у % до річного доходу внаслідок дій рейдерів;
 - 3.4. важелів впливу, що використовувались рейдерами при спробі захопити підприємство;
 - 3.5. виявлених ранніх ознак загрози протиправного захоплення;
 - 3.6. методів протидії рейдерству та їхньої ефективності.
 4. Випадки недобросовісної конкуренції в економічному оточенні суб'єкта підприємництва впродовж 2017–2021 рр. в розрізі:
 - 4.1. інструментів недобросовісної конкуренції з оцінкою впливу окремих чинників на її прояви;
 - 4.2. обсягів фінансових втрат, відвернених фінансових втрат та суми витрат на заходи із протидії недобросовісній конкуренції;
 - 4.3. методів виявлення випадків недобросовісної конкуренції та їхньої ефективності.

5. Корупційні прояви в діяльності суб'єктів підприємництва впродовж 2017–2021 рр. в розрізі:

5.1. корупційних взаємозв'язків між працівниками суб'єкта підприємництва та його контрагентами;

5.2. обсягів фінансових втрат, відвернених фінансових втрат та суми витрат на заходи із протидії недобросовісній конкуренції;

5.3. методів виявлення випадків корупції та їхньої ефективності.

Пропонований підхід до структурно-компонентного аналізу ми застосували шляхом опитування власників/керівників 20-ти суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні (перелік підприємств подано в додатку А). Водночас окремі з досліджуваних суб'єктів підприємництва (ТОВ “Поділлянафтозбут”, АТ “Концерн Галнафтогаз”, ТОВ “Західнафтозбут”, ТОВ “ОККО-Бізнес Партнер”, ТОВ “Вест Ойл Трейдінг”, МПП “Ірена”) було досліджено на предмет ширшого переліку гібридних фінансових конфліктів (протидія корупції; запобігання недобросовісній конкуренції; попередження та ліквідація фінансового шахрайства працівників; запобігання відмиванню доходів, одержаних злочинним шляхом; протидія конфліктам з державними органами; запобігання конфліктам з інститутами фінансово-кредитної сфери; нейтралізація інформаційних загроз) з метою подальшої експертної оцінки отриманих результатів анкетування.

Запропонований підхід до структурно-компонентного аналізу дає змогу ідентифікувати ознаки, виявити типові схеми, що використовуються у гібридних фінансових конфліктах, оцінити вплив на них різних внутрішніх і зовнішніх чинників, оцінити значущість деструктивних наслідків для фінансової безпеки. Це сприятиме більш повному вивченню ключових тенденцій розвитку гібридних фінансових конфліктів й розробленню на цій основі напрямів протидії їм та нейтралізації негативного впливу на фінансову безпеку.

2.3. Метод історичної абдукції в дослідженні гібридних фінансових конфліктів

Значущим у дослідженні чинників фінансової безпеки суб'єктів підприємництва є історичний метод, заснований на вивченні виникнення, формування та розвитку об'єктів у хронологічній послідовності, а також

логічний метод, що передбачає відтворення, реконструювання в мисленні складного об'єкта. При використанні логічного методу в дослідженні проблем фінансової безпеки відбувається абстрагування від усіх історичних випадків до виокремлення тих, що є найбільш вагомими, визначальними та істотними.

Водночас, погоджуємося з А. Грабченко, В. Федорович, Я. Гаращенко, що історичний і логічний методи наукового пізнання використовуються тільки там, де так чи інакше предметом дослідження стає історія об'єкта [54, с. 30]. Відтак, у випадку дослідження розвитку гібридних фінансових конфліктів у контексті забезпечення фінансової безпеки ділових одиниць цей метод становитиме вагоме значення для формування, перевірки гіпотез й формування відповідних висновків.

Серед методів дослідження поряд з індукцією й дедукцією використовують також абдукцію. Вперше абдукцію як метод дослідження виділив Ч. Пірс, який уважав, що відбираючи з величезної кількості гіпотез найсуттєвіші, дослідники реалізують “абдукційний інстинкт”, без якого розвиток науки неможливий. Згідно з таким баченням методологія науки має розумітися як взаємодія абдукції (прийняття правдоподібних гіпотез, які можна пояснити); індукції (реалізації емпіричного тестування висунутих гіпотез) і дедукції (методу, шляхом якого з прийнятих гіпотез виводять нові твердження). На думку вченого, всі ідеї наукового пізнання виникають шляхом абдукції, яка складається з вивчення фактів, встановлення взаємозв'язку між ними й висловлення гіпотези, що їх пояснює. Учений створив ідейний ескіз теорії міркування, яка пізніше була розвинута в дослідженнях зі штучного інтелекту, де абдуктивний висновок є видом автоматизованого правдоподібного міркування [85].

На перший погляд може здатися, що абдукція не відрізняється від індукції, у якій висновок роблять на основі узагальнених фактів і тому також має характер гіпотези. Водночас індукція визначає факти, що мають певну загальну ознаку, але не пояснює їх. Відтак, абдуктивне міркування широко використовується як у повсякденному мисленні, так і у всіх випадках, коли доводиться звертатися до гіпотез. Для прикладу, коли медики встановлюють діагноз на основі низки симптомів захворювання, вони роблять абдуктивний висновок, тобто, розглядаючи симптоми як взаємозалежну систему фактів, намагаються знайти їм

пояснення за допомогою діагнозу передбачуваної хвороби. В такий же спосіб, коли в діяльності суб'єктів підприємництва починає з'являтися низка ознак агресивної поведінки третіх осіб, то внаслідок встановлення такої системи пов'язаних фактів служба фінансової безпеки ділової одиниці висуває гіпотезу ймовірної рейдерської атаки. Ознаки (симптоми) виступають як безпосередньо спостережувані факти, наслідки, а рейдерство (хвороба) – як їхня причина. Тобто абдукція є логічною схемою пошуку пояснювальних гіпотез і головною відмінністю абдукції від індукції й дедукції є її орієнтація на пояснення досліджуваних фактів.

Застосування методу абдукції характеризується такими особливостями:

- пошук правдоподібних пояснювальних гіпотез відбувається в процесі розмірковування.
- у якості підстави для висновку можуть виступати як емпіричні факти, так і засновані на них узагальнення й емпіричні гіпотези;
- рівень пояснення фактів зростає в міру переходу від емпіричних гіпотез до теоретичних;
- в абдуктивному висновку використовується поєднання дедукції й індукції, зокрема дедукція служить для встановлення наслідків з гіпотези, запропонованої для пояснення нових фактів, а індукція – підтверджує або спростовує цю гіпотезу й відповідно коректує її. Тобто внаслідок абдукції відбувається модифікація й корекція гіпотез.

Враховуючи те, що забезпечення фінансової безпеки характеризується складністю та багатогранністю чинників впливу, а гібридні фінансові конфлікти мають переважно прихований характер їхнього розвитку впродовж тривалого часу і їм властива зміна інструментів агресії впродовж низки історичних періодів, пропонуємо в дослідженні цієї складної проблематики використовувати метод історичної абдукції (рис. 2.4).

Рекомендований нами метод передбачає інтегрування двох складових:

- історичного методу (вивчення виникнення, формування та розвитку чинників фінансової безпеки суб'єктів підприємництва в історичній хронології);
- абдукції (спосіб міркування від наявних даних до гіпотези, що пояснює або оцінює їх краще, ніж альтернативні гіпотези [54, с. 27–29]).

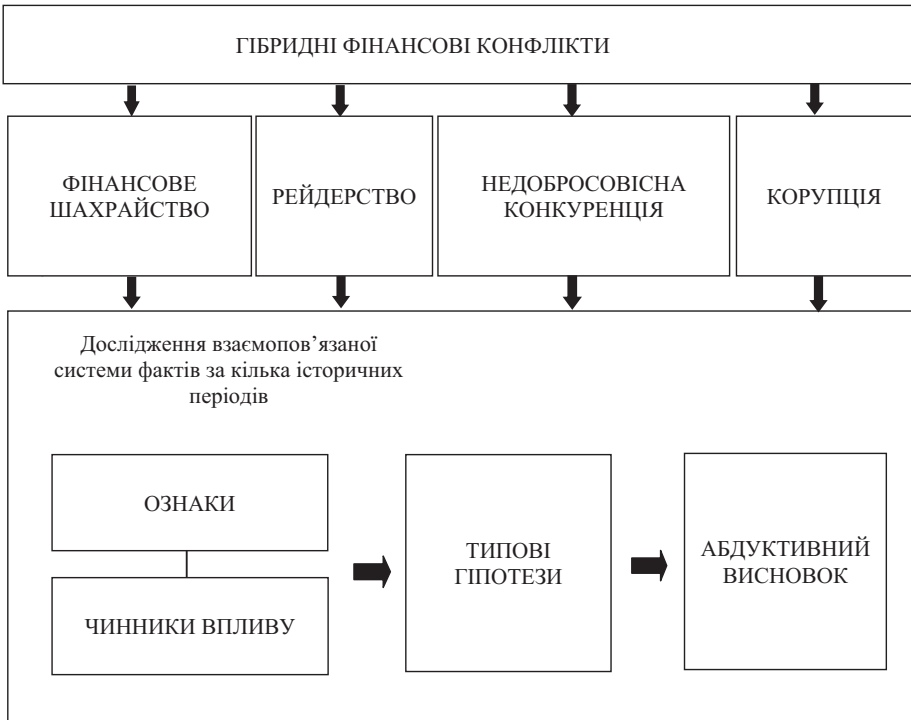


Рис. 2.4. Концептуальна схема використання методу історичної абдукції в дослідженні гібридних фінансових конфліктів

Джерело: розробила автор

Використання методу історичної абдукції можна простежити на прикладі гібридних агресій на міждержавному рівні (гібридна війна росії проти України) та на рівні ділових одиниць (рейдерство) (рис. 2.5). Наукові дослідження істориків на основі значної сукупності історичних даних й оцінювання значної кількості фактів протягом ХХ століття та 2014–2022 рр., дають змогу провести паралелі у використанні росією гібридних важелів впливу на Україну. Більшість інструментів гібридного конфлікту (спроба закріплення свого впливу на українських теренах через підтримку лояльних українських політичних середовищ, внутрішньополітичний розкол українського суспільства засобами пропаганди, відкрите військове втручання, намагання пояснити агресію внутрішнім громадянським конфліктом) російська влада використовувала ще з XVII–XVIII ст.

ГІБРИДНИЙ КОНФЛІКТ НА МІЖДЕРЖАВНОМУ РІВНІ (НА ПРИКЛАДІ РОСІЙСЬКОЇ ГІБРИДНОЇ ВІЙНИ В УКРАЇНІ)	
ЧАСОВІ ПЕРІОДИ	
XX століття (на прикладі української революції 1917–1921 рр.)	XXI століття (на прикладі 2014–2022 рр.)
Підтримка більшовицькою росією лояльних українських політичних груп	Намагання росії закріпити свій вплив в Україні через підтримку лояльних українських політичних еліт
Військове втручання росії в Україну	Військове втручання росії в Україну, починаючи з 2014 р.
Створення більшовиками маріонеткової УНР та “місцевих радянських республік” на захоплених територіях та маскування з їхньою допомогою агресії	Створення росією маріонеткових “ДНР” та “ЛНР” і тлумачення агресії в Україні внутрішнім громадянським конфліктом
Фінансування упроваджених росією в дипломатичні та консульські канали емісарів з метою здійснення розвідувально-підривної роботи проти Української держави	Фінансування росією агентури, впроваджені в стратегічні об’єкти, державні органи України, дипломатичні представництва й консульські установи з метою розвідувально-підривної діяльності
Провокування внутрішньополітичного розколу українського суспільства використанням пропаганди та поширенням гасел класової боротьби	Провокування росією соціальних, політичних, національно-етнічних і релігійних зіткнень, пропаганда й поширення проросійських інформаційних ресурсів з метою створення в Україні соціально-політичної напруги
ГІБРИДНИЙ ФІНАНСОВИЙ КОНФЛІКТ У ПІДПРИЄМНИЦЬКІЙ ДІЯЛЬНОСТІ (НА ПРИКЛАДІ РЕЙДЕРСТВА)	
ЧАСОВІ ПЕРІОДИ	
1991–2000 рр. (відверто кримінальне рейдерство, часто із застосуванням фізичного насильства)	2000 р. – дотепер (рейдерство з використанням напівлегальних інструментів боротьби)
Захоплення майнових комплексів державних підприємств у процесі приватизації	Фінансування колишніх партнерів, недобросовісного персоналу, кредиторів, представників державних органів, ЗМІ з метою впливу на підприємство-об’єкт агресії
Фізичне захоплення суб’єктів підприємництва	Порушення інформаційної безпеки суб’єкта підприємництва з метою розвідувально-підривної діяльності
Психологічний тиск, залякування, шантаж власників та керівників суб’єкта підприємництва	Розпалювання впровадженими агентами внутрішньокорпоративних конфліктів
Використання корупційної взаємодії з партнерами, конкурентами, персоналом, кредиторами, представниками державних органів, ЗМІ з метою впливу на підприємство-об’єкт агресії	Захоплення підприємств шляхом доведення до банкрутства, зупинки роботи, фізичного насильства внаслідок початку бойових дій в Україні в 2014 р.

Рис. 2.5. Використання методу історичної абдукції в дослідженні гібридних конфліктів на міждержавному рівні та в підприємницькій діяльності

Джерело: розробила автор

Найкраще ілюструє гібридний сценарій російської агресії період Української революції 1917–1921 рр., коли більшовики проти Української Народної Республіки застосовували приблизно ті ж гібридні інструменти впливу, що й росія в XXI столітті використовує в Україні. Зокрема, під час Української революції в Україну було надіслано тисячі більшовицьких агітаторів, які вільно поширювали гасла більшовизму на території України в добу Центральної Ради, а подеколи і в добу Директорії Української Народної Республіки. Вдале використання більшовиками інформаційної пропаганди, поширення класової боротьби з метою розпалювання конфліктів між різними прошарками населення, а також організація масових заворушень є характерними ознаками гібридної війни [282, с. 36–39].

Як у сучасних умовах, так і 100 років тому росія використовувала також і політичні та фінансово-економічні інструменти гібридної агресії. Основними каналами ведення у 1918 році підривних дій проти Української держави були дипломатичні й консульські можливості. Через ці канали легальним і нелегальним шляхом упроваджували емісарів з метою розгортання антиурядового підпілля. Нехтуючи нормами міжнародного права, радянська росія активно використовувала участь своєї делегації у мирних переговорах з Україною. До її складу залучали осіб з досвідом ведення розвідувально-підривної роботи у царській армії, а під виглядом дипломатів і консульських працівників було надіслано близько тисячі агентів та агітаторів, яким поставили завдання з підготовки антигетьманського повстання. Для цього керівникові російської так званої Мирової делегації Х. Раковському було виділено близько 40 мільйонів карбованців [147].

Кошти нелегальним формуванням надходили тоді з росії здебільшого дипломатичною поштою. Одного з радянських дипломатичних кур'єрів було затримано з трьома мільйонами карбованців, які призначалися для підривної діяльності. Для прикладу, влітку 1918 року затримали радянського консула М. Бека разом з його підлеглими. Під час обшуку в приміщенні консульства знайшли велику кількість агітаційної літератури, циркуляри для підготовки збройних виступів, а також картки з фотографіями і біографічними даними членів бойових підпільних організацій [147].

Сучасні інформаційні інструменти гібридної агресії росії в Україні спрямовані на дестабілізацію та руйнування інформаційно-

комунікативного простору та суспільної свідомості українського суспільства шляхом поширення дезінформації. Пропагандистські операції росії характеризуються застосуванням великої кількості джерел дезінформування власного населення та світової спільноти з метою дискредитації та спростування правдивих повідомлень. Прикладом агресивних інформаційних кампаній є створення та розповсюдження пропагандистських наративів, зокрема таких, як так звана доктрина “ДНР” “Русский Донбас” та інших. За допомогою таких інформаційних диверсій російські агресори намагалися змінити свідомість як українських, так і російських громадян, спотворити розуміння реальності та використати їх як людський ресурс у 2014 році та продовжують застосовувати політику поширення дезінформації та пропагандистських потоків інформації у світі, фінансуючи широку мережу каналів передачі такої інформації.

Одночасно з інформаційними інструментами в гібридній війні росією використано також соціально-політичні інструменти, зокрема відбувалося фінансування соціальних, політичних, національно-етнічних і релігійних зіткнень з метою створення в Україні соціально-політичної напруги.

Фінансово-економічні інструменти гібридної війни росії охоплюють здійснення агресором систематичних торговельних війн з метою пригнічення зовнішнь-торговельного потенціалу України та блокування диверсифікації зовнішньоторговельних зв'язків. Суттєвої шкоди національним інтересам України завдано проникненням агентів агресора в економіку України з метою її ослаблення та встановлення реального чи прихованого контролю над стратегічними підприємствами. Наслідком таких дій стало здійснення актів економічного тероризму (організація широко спектру економічних заходів на економічних об'єктах України, які призвели до зупинки їх фінансово-господарської діяльності, доведення до банкрутства, розмивання частки акцій, істотного підвищення соціальної напруги внаслідок скорочення працівників, отримання конфіденційної інформації про акціонерів тощо). Для прикладу, Запорізький алюмінієвий комбінат із 2006 року цілеспрямовано знищували на користь російських виробників металу, Дніпропетровську паперову фабрику – з метою російського імпорту паперу та готової друкованої продукції. Бізнес росії заволодів значною нішею у паливно-енергетичному комплексі України, зокрема під його контролем

опинилася значна частка алюмінієвої і титанової промисловості, що дало можливість росії використовувати її виключно для забезпечення стратегічною сировиною власного оборонно-промислового комплексу (насамперед у виробництві бойових літаків та гелікоптерів). Навіть після повернення у державну власність низки титанових потужностей з 2014 року росія через підставні західні компанії налагодила імпорт титанової сировини з України. Небезпечних для захисту національних інтересів масштабів зазнала присутність російського бізнесу у галузі зв'язку і телекомунікацій, а також присутність у банківському секторі дочірніх банків російських банків, таких як “Промінвестбанк”, “ВТБ Банк”, “Сбербанк”.

Проникнення російського капіталу в український бізнес призвело також до деструктивної та протиправної діяльності, такої як організація нелегальної економічної діяльності (розширення потоків контрабанди, відмивання грошей, організація на території України інноваційних децентралізованих фінансових мереж для фінансування тероризму, підконтрольних політичних проектів та сепаратистських рухів, які здійснюють підривну діяльність тощо).

Фінансово-економічні інструменти гібридної війни росії передбачали також агентурне проникнення в державні органи управління з метою впливу на регулювання економіки України та міжнародні економічні відносини.

Значної шкоди економіці України було завдано шляхом вчинення російськими агентами впливу рейдерства, шпигунства (промислового, технологічного, патентного тощо), укладання економічно недоцільних, екологічно- та технологічно шкідливих контрактів, використовуючи хабарництво та системну корупцію. Військово-терористичні інструменти гібридної війни на її підготовчому етапі передбачали агентурний вплив на управлінські рішення в економічній сфері з метою стримування воєнного та інноваційно-технологічного розвитку, а також намаганнями руйнування морального духу українського населення з метою зниження обороноздатності та бойового потенціалу країни.

Метод історичної абдукції дає змогу ідентифікувати гібридний конфлікт за допомогою дослідження взаємозалежної системи фактів за кілька історичних періодів. З його допомогою ми виявили не лише схожість використання гібридних конфліктів на міждержавному рівні, але

й підтвердили також застосування подібного інструментарію на рівні суб'єктів підприємництва. Зокрема, схожими до інструментів російської агресії є важелі впливу рейдерів на захоплювані суб'єкти підприємництва – порушення інформаційної безпеки ділових одиниць з метою розвідувально-підривної діяльності; фінансування партнерів, недобросовісного персоналу, кредиторів, представників державних органів, ЗМІ з метою впливу на підприємство-об'єкт агресії; розпалювання впровадженими агентами фінансових конфліктів; захоплення підприємств шляхом доведення до банкрутства, зупинки роботи, фізичного насильства; використання корупційної взаємодії з різними учасниками бізнес-середовища підприємства-об'єкта агресії з метою впливу на нього.

Відтак, метод історичної абдукції дає змогу зробити відбір найсуттєвіших гіпотез, які можна пояснити на основі врахування часової послідовності реалізованих подій у сфері фінансової безпеки суб'єктів підприємництва. Завдяки використанню цього методу досягається поглиблене розуміння суті проблеми забезпечення фінансової безпеки суб'єктів підприємництва і з'являється можливість формулювати більш обґрунтовані висновки.

2.4. Вибір інструментів аналізу та прогнозування стану фінансової безпеки суб'єктів підприємництва в умовах гібридних загроз

Методологія наукового дослідження проблем фінансової безпеки суб'єктів підприємництва в умовах гібридних фінансових конфліктів передбачає розроблення концептуально-методологічного інструментарію аналізу та прогнозування рівня їх фінансової безпеки. Це дасть змогу не лише визначити поточний стан фінансової безпеки, але й своєчасно виявити реальні та потенційні загрози та вжити відповідні заходи нівелювання їх деструктивного впливу. Водночас методологія оцінювання фінансової безпеки ділових одиниць є складною та комплексною, залежить від мети і завдань оцінювання, оскільки в ній зацікавлені як внутрішні, так і зовнішні користувачі. Порівняльну характеристику зовнішнього та внутрішнього аналізу фінансової безпеки суб'єктів підприємництва подано в табл. 2.2.

**Порівняльна характеристика зовнішнього та внутрішнього аналізу
фінансової безпеки суб'єктів підприємництва**

КРИТЕРІЙ ПОРІВНЯННЯ	ВИД АНАЛІЗУ	
	ЗОВНІШНІЙ	ВНУТРІШНІЙ
Суб'єкти аналізу	Інвестори, кредитори, державні органи	Власники, управлінський персонал (керівники, служба фінансової безпеки, фінансові аналітики тощо)
Мета аналізу	Оцінка фінансової стійкості	Виявлення і протидія деструктивним чинникам впливу на фінансову безпеку
Інформаційна база аналізу	Фінансова звітність, зовнішні додаткові джерела інформації	Уся інформація про діяльність суб'єкта підприємництва
Методи аналізу	Кількісні та якісні методи аналізу	Кількісні та якісні методи аналізу
Періодичність виконання	Ретроспективний та перспективний	Оперативний, ретроспективний та перспективний

Джерело: склала автор

Інвестиційні та кредитні рішення ухвалюють на підставі інформації про фінансовий стан і рівень фінансової безпеки ділових одиниць. Відтак, саме інтересами внутрішніх і зовнішніх користувачів зумовлені завдання та масштаб, у якому оцінюватимуть фінансову безпеку – чи загалом, за структурними підрозділами, чи окремим проектом.

Об'єктивність оцінки фінансової безпеки суб'єктів підприємництва необхідно забезпечити з урахуванням таких принципів, як системність, об'єктивність, адекватність, комплексність, взаємоузгодженість, універсальність, однозначність, результативність тощо.

У теорії та практиці фінансового менеджменту є значна кількість підходів до оцінювання рівня фінансової безпеки суб'єктів підприємництва [18; 31; 32; 149; 156; 159]. Усю їх сукупність можна розділити на такі групи (рис. 2.6).

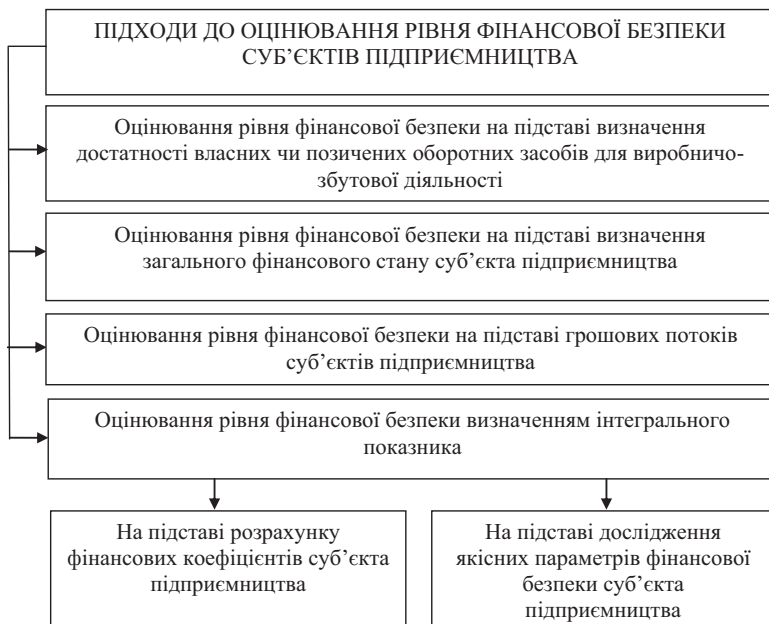


Рис. 2.6. Систематизація підходів до оцінювання рівня фінансової безпеки суб'єктів підприємництва

Джерело: розробила автор

- абсолютна фінансова стійкість та абсолютна безпека (суб'єкту підприємництва повністю достатньо власних оборотних коштів для функціонування);
- нормальна фінансова стійкість та нормальний рівень безпеки (суб'єкт підприємництва використовує практично лише власні оборотні кошти для формування запасів і забезпечення витрат);
- нестійке фінансове становище та нестабільний рівень безпеки (суб'єкту підприємництва недостатньо власних оборотних коштів і воно має потребу у використанні середньо- та довготермінових позикових коштів);
- критичний фінансовий стан та критичний рівень безпеки (суб'єкт підприємництва для фінансування діяльності використовує, крім середньо- та довготермінових кредитів, ще й короткострокові позики);
- кризовий фінансовий стан та кризовий рівень безпеки (суб'єкт підприємництва не в змозі забезпечити фінансування діяльності ані власними, ані позиченими коштами, тобто підприємство перебуває на межі банкрутства).

Ця методика оцінювання фінансової безпеки ділових одиниць не дає повного уявлення про її рівень, оскільки поза увагою є такі важливі показники фінансово-господарської діяльності, як основний капітал, прибуток, інвестиції.

Оцінювання рівня фінансової безпеки суб'єктів підприємництва здійснюють також шляхом аналізу їх грошових потоків, а саме – показника чистого грошового потоку в розрізі видів діяльності.

Серед науковців поширеним є підхід до оцінювання рівня фінансової безпеки на підставі аналізу фінансового стану суб'єктів підприємництва, що передбачає обчислення фінансових показників за такими напрямками (рис. 2.7).



Рис. 2.7. Показники для визначення рівня фінансової безпеки суб'єктів підприємництва на підставі аналізу фінансового стану

Джерело: склала автор

Водночас оцінювання рівня фінансової безпеки суб'єктів підприємства не можна здійснювати лише на основі дослідження параметрів фінансового стану, адже фінансові показники дають можливість лише частково оцінити рівень фінансової безпеки суб'єкта підприємництва.

Окрім того, використання значної кількості коефіцієнтів, з одного боку, дає змогу максимально різнобічно проаналізувати діяльність ділової одиниці, однак, з іншого, – значна кількість фінансових показників може зумовити формування неоднозначних підсумкових висновків унаслідок суперечливих результативних значень різних показників.

Окремі науковці пропонують оцінювати рівень фінансової безпеки суб'єктів підприємництва шляхом визначення інтегрального показника фінансової безпеки. Проте є розбіжності стосовно алгоритму його розрахунку. Зокрема, більшість учених схиляється до визначення інтегрального показника лише на підставі фінансових коефіцієнтів, що не повністю ідентифікує стан фінансової безпеки суб'єкта підприємництва. Згідно з розрахованими фінансовими коефіцієнтами, ділові одиниці можуть відповідати високому рівню фінансової безпеки, і водночас унаслідок фінансового шахрайства, зловживань з конфіденційною фінансовою інформацією можуть стати об'єктом рейдерського захоплення, що повністю спростує присвоєний високий рівень безпечності. Тому аналіз рівня фінансової безпеки ділових одиниць повинен охоплювати не лише фінансові індикатори, а й також і якісні параметри розвитку.

Враховуючи обґрунтовану нами необхідність одночасного досягнення двох незалежних цілей – динамічної фінансової рівноваги (бажані параметри фінансового стану) і рівноваги в гібридних фінансових конфліктах (баланс сил у гібридних фінансових конфліктах) пропонуємо використовувати концептуальну модель діагностування стану фінансової безпеки суб'єктів підприємництва – “Колесо рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах”. Поєднання соціально-психологічного й метафоричного підходів у цьому випадку дасть змогу виявити гібридні фінансові конфлікти в діяльності ділових одиниць, оцінити результативність протидії їм і проілюструвати позицію їх фінансової безпеки шляхом графічної інтерпретації – колеса, яке впродовж різних історичних періодів та у різноманітних культурах є символом балансу і руху, а отже в нашому випадку – розвитку суб'єкта підприємництва, окрім того, так зване “колесо колісниці” асоціюється з управлінням та владою (в умовах гібридних фінансових конфліктів розумітимемо спроможність ефективно протидіяти їм).

Застосовуючи такий підхід до забезпечення фінансової безпеки суб'єктів підприємництва, ми ґрунтуємося також на сучасних наукових дослідженнях коучингу [354; 389; 398], в яких обґрунтовано використання

техніки “Колесо життєвого балансу” для діагностування життєвого стану особистості. Коло згідно з цією методикою поділене на визначену кількість секторів, зазвичай їх 8 (кар’єра, гроші, здоров’я, друзі, сім’я, розвиток, відпочинок, умови життя). Метою побудови “Колеса життєвого балансу” є виявлення найбільш проблемних сфер життя особистості, стабілізування яких призведе до досягнення рівноваги в цілому. Отримані оцінки за кожним життєвим показником відображають графічно точками на діаграмі, з’єднаних по колу. Це дає можливість виявити результат – колесо правильної форми, що свідчить про рівновагу і можливість розвитку чи іншу геометричну фігуру, яка попри те, що на момент оцінки не забезпечує рівноважний стан й ускладнює розвиток (“нездатність рухатись”), проте, не унеможливує його в майбутньому, оскільки допомагає виявити проблемні аспекти й таким способом стабілізувати стан.

Запропонована нами модель побудована на основі найбільш поширених на сьогодні гібридних фінансових конфліктів у діяльності суб’єктів підприємництва (рис. 2.8).

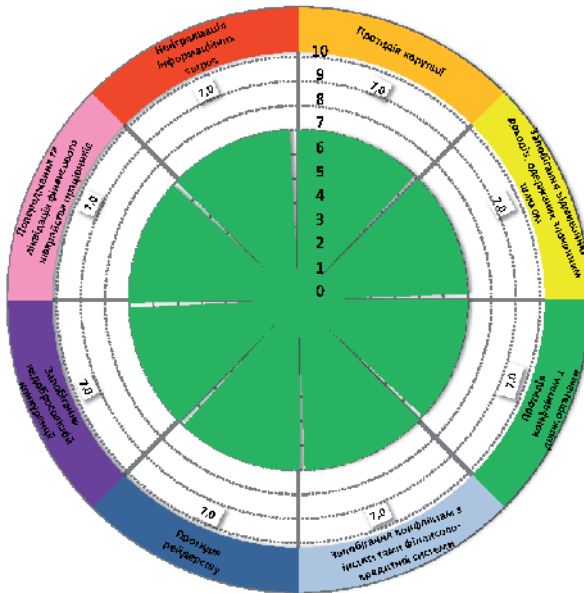


Рис. 2.8. Концептуальна модель “Колесо рівноваги суб’єктів підприємництва в гібридних фінансових конфліктах”

Джерело: розробила автор

Досягнуте значення по шкалі за кожним чинником, який визначає рівновагу в гібридних фінансових конфліктах дає можливість з'ясувати рівень досягнення поставлених цілей у протидії кожному із поданих у моделі конфліктів. Також досягнуті значення чинників рівноважного стану суб'єкта підприємництва в цих аспектах фінансової безпеки в динаміці дають змогу ідентифікувати специфіку його циклічного розвитку, зокрема, можуть визначати ранні ознаки кризи. Оскільки криза розпочинається із суперечностей рівноваги.

З метою забезпечення об'єктивності отриманих результатів шляхом експертного оцінювання гібридних фінансових конфліктів й показників ефективності протидії їм залучено фахівців із різних сфер, дотичних до діяльності досліджуваних суб'єктів підприємництва (склад експертної групи подано в додатку Б).

Окрім того, запропонований діагностичний інструмент уможлиблює порівняння досягнутих значень показників динамічної фінансової рівноваги й рівноваги в гібридних фінансових конфліктах, що допомагає з'ясувати й усунути причини виявлених відхилень. Водночас необхідно зауважити, що забезпечення фінансової безпеки суб'єктів підприємництва, що спрямовано на досягнення фінансової рівноваги лише у виняткових випадках одночасно призводить і до рівноваги у гібридних фінансових конфліктах. Зазвичай вигляд “Колеса рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах” в реальних обставинах відповідно до встановлених досягнутих значень чинників на підприємстві має спотворений вигляд. Водночас це дає змогу виявити проблемні сектори забезпечення фінансової безпеки ділових одиниць та вжити відповідні корегуючі заходи, що відобразяться в наближенні колеса до правильної форми.

Залежно від якості управління фінансовою безпекою можна спостерігати як позитивний, так і негативний вектор рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах. Так, коли управлінські дії породжують подальші зміни у напрямі зростання досягнутих значень чинників фінансової безпеки та посилюються з плином часу, йдеться про позитивний вектор динамічної рівноваги фінансової безпеки суб'єктів підприємництва (див. рис. 2.9). Якщо ж показники змінюються в напрямку спадання досягнутих значень, спостерігаємо негативний вектор динамічної рівноваги фінансової безпеки суб'єктів підприємництва (див. рис. 2.10).



Рис. 2.9. Позитивний вектор динамічної рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах

Джерело: розробила автор

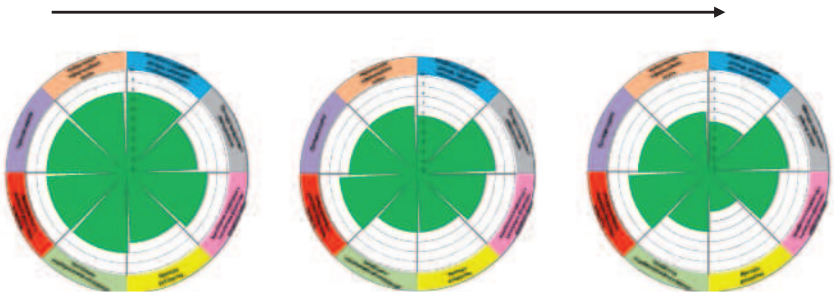


Рис. 2.10. Негативний вектор динамічної рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах

Джерело: розробила автор

Перехід суб'єкта підприємництва від однієї траєкторії функціонування до іншої становить зміну динамічної рівноваги, встановлення її на іншому рівні, фактично відображає перехід до нового етапу розвитку. В цьому контексті фінансова безпека ділових одиниць відображає їх здатність не лише зберігати ключові чинники фінансової безпеки незмінними або утримувати відхилення значень цих чинників від вектора динамічної рівноваги у допустимих межах в умовах несприятливого внутрішнього та зовнішнього середовища, а й потенційні можливості забезпечувати позитивну динаміку зростання досягнутих значень чинників фінансової безпеки. Бажаний стан колеса рівноваги виражений через множину максимального рівня досягнутих значень.

Враховуючи нестійкість рівноваги, складність еволюції суб'єктів підприємництва, а також можливість впливу спонтанних змін і кризових ситуацій у діяльності, множинність внутрішніх і зовнішніх чинників фінансової безпеки, необхідно розробити та використовувати математичний інструментарій прогнозування вектора динамічної рівноваги чинників фінансової безпеки суб'єктів підприємництва. При вирішенні завдань оцінювання необхідно встановити критерії знаходження суб'єкта підприємництва в стані рівноваги:

– необхідна умова: досягнуте значення в балах кожного із чинників моделі “Колеса рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах”, на наш погляд, має перевищувати поріг 7 балів. Значення і вагомість кожного із чинників фінансової безпеки ділових одиниць визначатиметься експертним шляхом.

– достатня умова: середня сума відсотків відхилення досягнутого бального значення сусідніх чинників у пропонованій моделі не повинна перевищувати певного порогу – 10 %.

Якщо суб'єкт підприємництва відповідає цим умовам, можна класифікувати такий стан фінансової безпеки як рівноважний. Якщо підприємство перебуває в зазначених критеріях рівноваги в динаміці, то можна зробити висновок, що воно знаходиться в динамічній рівновазі.

Попри те, що концептуальна модель “Колесо рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах” як інструмент діагностики допомагає виявити рівноважний стан суб'єкта підприємництва, важливо передбачити позитивний або негативний вектор динамічної рівноваги в майбутньому. Прогнозування чинників фінансової безпеки суб'єктів підприємництва на майбутні етапи життєвого циклу можна реалізувати із врахуванням таких підходів:

1. Шляхом екстраполяції значення балів кожного з чинників фінансової безпеки суб'єктів підприємництва за допомогою таких моделей:

– лінійна модель (за умови розвитку ситуації, що передбачає рівномірну зміну значень чинників);

– експоненціальна модель (за умови агресивного розвитку ситуації, що передбачає різку зміну значень чинників);

– логарифмічна модель (за умови плавної зміни ситуації, що передбачає уповільнення зміни чинників);

– синусоїдальна (перехідна) модель, побудова моделі екстраполяції Жозефа Фур'є (за умови накопичення достатньої бази статистичних даних у майбутньому).

2.3 використанням методу рухливих середніх (Moving Average) (передбачає прогнозування бальних значень чинників фінансової безпеки суб'єктів підприємництва за допомогою елементів технічного аналізу, а саме рухливих середніх з оптимальним підбором вагомості чинників).

3. Екстраполяція моделі чинників фінансової безпеки суб'єктів підприємництва як рух точки в десятивимірному фазовому просторі (векторному просторі).

Використання для діагностування стану фінансової безпеки суб'єктів підприємництва концептуальної моделі “Колесо рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах” та прогнозування вектора динамічної рівноваги чинників фінансової безпеки в майбутньому із врахуванням запропонованих підходів дасть змогу більш ефективно збалансувати їх інтереси з інтересами суб'єктів економічного оточення.

Ми провели анкетування та експертне оцінювання наявності, особливостей розвитку гібридних фінансових конфліктів та методів протидії їм у діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні – ТОВ “Поділлянафтозбут”, АТ “Концерн Галнафтогаз”, ТОВ “Західнафтозбут”, ТОВ “ОККО-Бізнес Партнер”, ТОВ “Вест Ойл Трейдинг” МПП “Ірена”. Отримані результати (додатки В, Г) дали змогу побудувати для кожного із досліджуваних підприємств “Колесо рівноваги у гібридних фінансових конфліктах” та виявити стан їхньої фінансової безпеки (рис. 2.11–2.16).

Аналіз протидії гібридним фінансовим конфліктам у діяльності ТОВ “Вест Ойл Трейдинг” (рис. 2.11) засвідчив досягнення порогового значення 7 балів за 5-ма показниками – у сфері протидії рейдерству, корупції, запобігання конфліктам з інститутами фінансово-кредитної сфери, попередження та ліквідації фінансового шахрайства, запобігання відмиванню доходів, одержаних злочинним шляхом. За іншими 3-ма параметрами моделі підприємство не відповідає встановленому необхідному мінімальному значенню. Відтак, попри те, що середня сума відсотків відхилення досягнутого бального значення сусідніх чинників у пропонованій моделі не перевищує порогу (10 %), не можна констатувати стан його фінансової безпеки як рівноважний.

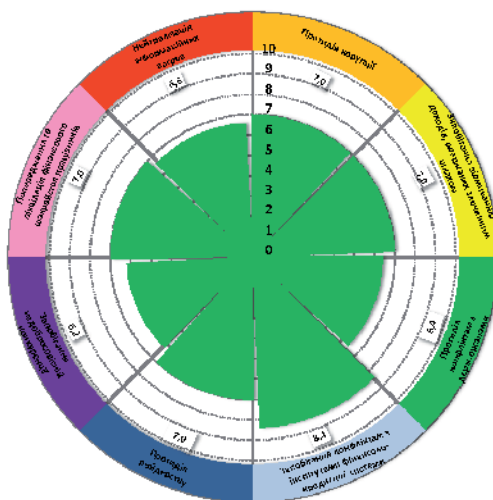


Рис. 2.11. Позиція ТОВ “Вест Ойл Трейдінг”

Джерело: побудувала автор на основі експертних оцінок

У діяльності АТ “Концерн Галнафтогаз” (рис 2.12) виявлено результативні значення показників протидії гібридним фінансовим конфліктам, що не відповідають необхідній вимозі пропорційності сусідніх чинників (понад 10 %) хоча їхні досягнуті значення є високими і відповідають необхідному пороговому значенню – 7 балів.

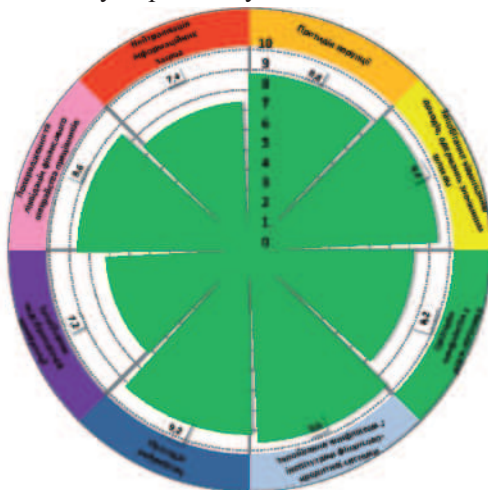


Рис. 2.12. Позиція АТ “Концерн Галнафтогаз”

Джерело: побудувала автор на основі експертних оцінок

Відтак, позицію цього підприємства в пропонованій концептуальній моделі також не може бути ідентифіковано як рівноважний стан його фінансової безпеки.

Функціонування ТОВ “Західнафтозбут” (рис. 2.13) характеризується невідповідністю оцінюваних параметрів моделі вимозі пропорційності сусідніх чинників (понад 10 %) й характеризується низьким рівнем протидії недобросовісній конкуренції та рейдерству. Тому, попри інші задовільні показники, позицію підприємства в концептуальній моделі визначено як нерівноважний стан його фінансової безпеки.

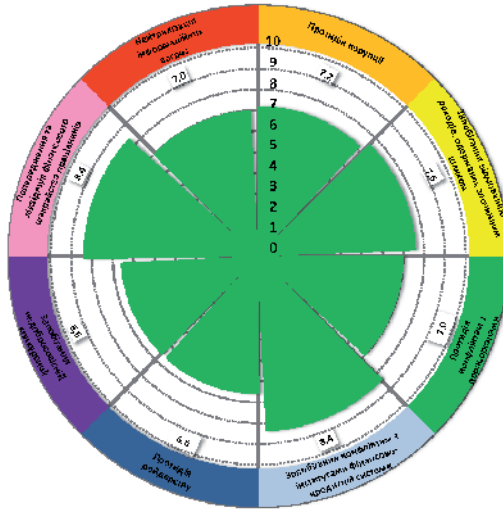


Рис. 2.13. Позиція ТОВ “Західнафтозбут”

Джерело: побудувала автор на основі експертних оцінок

У діяльності МПП “Ірена” (див. рис. 2.14) протидія гібридним фінансовим конфліктам відбувається на доволі низькому рівні, зокрема жоден із параметрів концептуальної моделі не відповідає пороговому значенню (7 балів). Також виявлено значні диспропорції в значеннях сусідніх чинників (відхилення понад 10 %). Тому позицію МПП “Ірена” в концептуальній моделі “Колесо рівноваги суб’єктів підприємництва в гібридних фінансових конфліктах” визначено як нерівноважний стан фінансової безпеки.

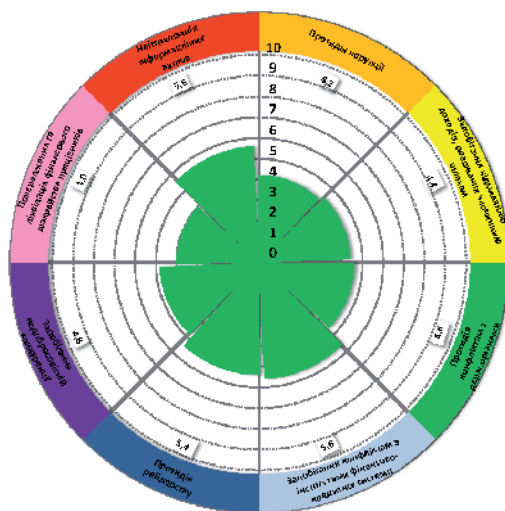


Рис. 2.14. Позиція МПП “Ірена”

Джерело: побудувала автор на основі експертних оцінок

Оцінювані параметри концептуальної моделі ТОВ “ОККО-Бізнес Партнер” (див. рис. 2.15) майже наближені до бажаного стану рівноваги фінансової безпеки, оскільки усі вони визначені на рівні, вищому 7 балів.

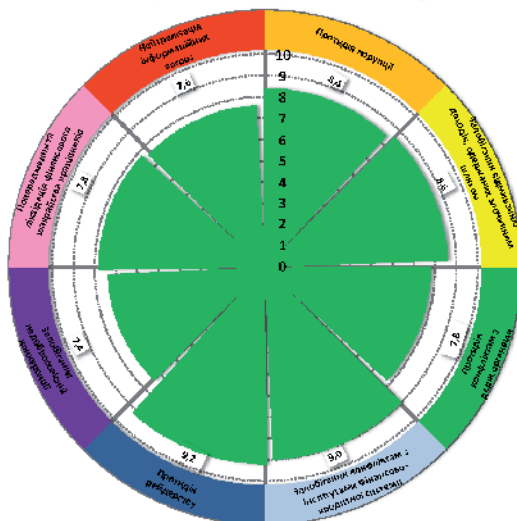


Рис. 2.15. Позиція ТОВ “ОККО-Бізнес Партнер”

Джерело: побудувала автор на основі експертних оцінок

Позитивним моментом функціонування досліджуваного підприємства є висока якість протидії рейдерству та конфліктам з інститутами фінансово-кредитної сфери – 9,2 та 9 балів відповідно. Однак можна констатувати потребу в підвищенні ефективності запобігання іншим видам гібридних фінансових конфліктів, оскільки виявлено порушення пропорційності з іншими досягнутими значеннями показників.

У діяльності ТОВ “Поділлянафтозбут” (див. рис. 2.16) ми виявили більшість із оцінюваних параметрів моделі на рівні, нижчому 7 балів, зокрема ефективність протидії більшості гібридних фінансових конфліктів оцінено експертною групою в межах близько 7 балів. Лише за показником запобігання конфліктам з інститутами фінансово-кредитної сфери досліджуваній суб’єкт підприємництва досяг необхідного мінімального значення – 7 балів.

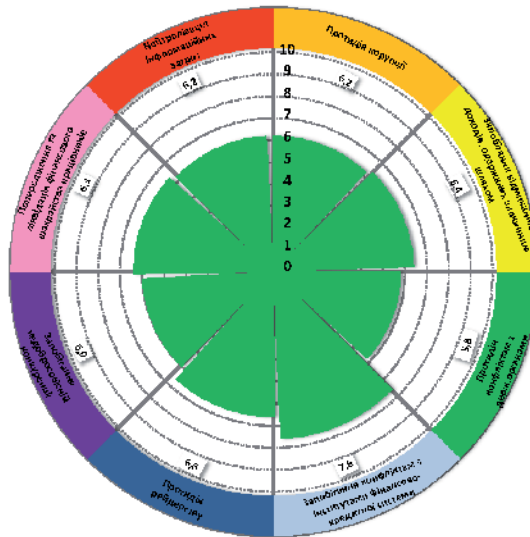


Рис. 2.16. Позиція ТОВ “Поділлянафтозбут”

Джерело: побудувала автор на основі експертних оцінок

Відтак, управлінські дії власників та керівництва необхідно зосередити на налагодженні ефективної роботи у сфері їхньої фінансової безпеки в контексті протидії зловмисним намірам інших учасників ринку й проявам можливого фінансового шахрайства працівників.

Водночас унаслідок військової агресії РФ в Україні було введено воєнний стан, що радикально змінило умови функціонування усіх суб'єктів підприємництва та зумовило зміщення акцентів зі стратегічних пріоритетів розвитку ділових одиниць на оперативно-тактичне реагування на кризові ситуації. Відтак, попри те, що питання забезпечення фінансової безпеки суб'єктів підприємництва в умовах щоденної зміни воєнної ситуації в державі суттєво актуалізувалися, змінилася першочерговість розроблення і впровадження заходів – із середньо- і довгострокового прогнозування майбутнього розвитку ділових одиниць до оперативно-тактичних інструментів кризового менеджменту з метою швидкого реагування на зовнішні виклики, спричинені агресією РФ.

РОЗДІЛ 3. СТРУКТУРНО-КОМПОНЕНТНИЙ АНАЛІЗ ГІБРИДНИХ ФІНАНСОВИХ КОНФЛІКТІВ У СФЕРІ ФУНКЦІОНУВАННЯ ІНСТИТУТУ ВЛАСНОСТІ В УКРАЇНІ

3.1. Фінансове шахрайство працівників як загроза безпечному функціонуванню суб'єктів підприємництва в Україні

Забезпечення ефективного функціонування суб'єктів підприємництва можливе внаслідок раціонального поєднання низки чинників, винятково важливим серед яких є персонал. Водночас працівники ділових одиниць можуть як сприяти досягненню фінансових інтересів, визначених у стратегії їх розвитку, так і бути суб'єктами зловмисних дій щодо їх реалізації. Це може мати свій вияв у вигляді фінансових помилок і шахрайства, що негативно впливає на рівень фінансової безпеки суб'єктів господарювання.

Згідно зі ст. 190 Кримінального кодексу України, “шахрайство” – це заволодіння чужим майном або придбання прав на майно обманом чи зловживанням довірою (предметом шахрайства може бути як чуже майно, так і право на таке майно) [132].

Фінансове шахрайство визначають як кримінологічне явище, що полягає у злочинній діяльності та виражене в системі кримінально-караних та легальних дій, які вчиняють обманом або зловживанням довірою в процесі формування, розподілу та використання грошових фондів з метою отримання матеріальної вигоди [299, с. 233].

Розглядаючи сутність фінансового шахрайства в діяльності суб'єктів підприємництва, варто відзначити наявність таких його ключових характеристик:

- сфера посягання – фінансові відносини щодо формування, розподілу та використання фінансових ресурсів;
- об'єкт посягання – фінансові ресурси, матеріальні цінності, фінансова інформація, інші надбання матеріального й інтелектуального характеру, що становлять або можуть бути трансформовані в майбутньому у фінансову вигоду;
- суб'єкт вчинення – це, здебільшого, посадові особи суб'єктів господарювання, що виконують відповідні службові обов'язки, володіють

необхідними знаннями в галузі фінансового управління, бухгалтерського й податкового обліку, а також в інших сферах його діяльності;

- характер вчинення – злочинний, зловмисний та планомірний;
- механізм реалізації – складний, з використанням різних методів та важелів досягнення мети;

- типові способи вчинення – маніпуляції з обліковими записами, фальсифікування первинних документів, реєстрів обліку і звітності, навмисна зміна записів в обліку, які перекручують суть фінансово-господарських операцій; зумисно неправильна оцінка активів і методів їхнього списання, незаконне отримання в особисту власність грошово-матеріальних цінностей тощо;

- організаційне забезпечення вчинення – використання сукупності сучасних методів і програмно-технологічних засобів, що обслуговують фінансові процеси.

Важливо акцентувати, що при здійсненні фінансового шахрайства зловмисники використовують множинність легальних і протиправних інструментів, що мають переважно прихований характер. Це підтверджує гібридну форму цих злочинів. Тому пропонуємо тлумачити фінансове шахрайство як гібридний фінансовий конфлікт між власниками суб'єкта підприємництва та його найманими працівниками, пов'язаний із отриманням власної вигоди та задоволенням особистих фінансових інтересів останніх всупереч інтересів компанії внаслідок зловживання наданою їм власниками довірою.

Визначаючи змістову характеристику фінансового шахрайства, важливим є вивчення основних суб'єктів злочинних дій з позиції функціональних обов'язків, які ними виконуються, мотивації вчинення зловживань, особистісних якостей тощо. Відтак, на основі аналізу, синтезу й узагальнення наукових досліджень у цій сфері ми виявили такі особливості, властиві для зловмисників цього типу злочинів:

- найбільші можливості для шахрайства (77 %) мають працівники, що працюють у фінансовому відділі, бухгалтерії, відділі продажів, закупівель, у вищому керівництві [110.];

- більшість виявлених випадків шахрайства є непоодинокими. Зазвичай після виявлення одного факту зловживання в процесі фінансового розслідування розкривають нові злочини;

- здебільшого вчиняють шахрайство працівники, які працюють у

компанії тривалий час та репутація яких не дає змоги запідозрити їх у таких діях;

– зазвичай до фінансового шахрайства причетні декілька осіб. Зокрема, у кожному другому випадку це групи з двох–п’яти осіб [155, с. 95-96];

– вчиняють корпоративні злочини переважно чоловіки, причому у віці 36–55 рр. [155, с. 95–96].

Дослідження фінансового шахрайства в розрізі суб’єктів зловмисних дій ми провели шляхом аналізу результатів даних міжнародних асоціацій, що займаються проблемами економічної злочинності, а також на основі проведеного анкетування вітчизняних ділових одиниць. Відтак, згідно з результатами дослідження PwC Україна (див. рис. 3.1), 25 % економічних злочинів вчиняють співробітники підприємства, 25 % становлять шахрайства внаслідок змови між співробітником суб’єкта господарювання і третьою стороною та 41 % – третьою стороною.

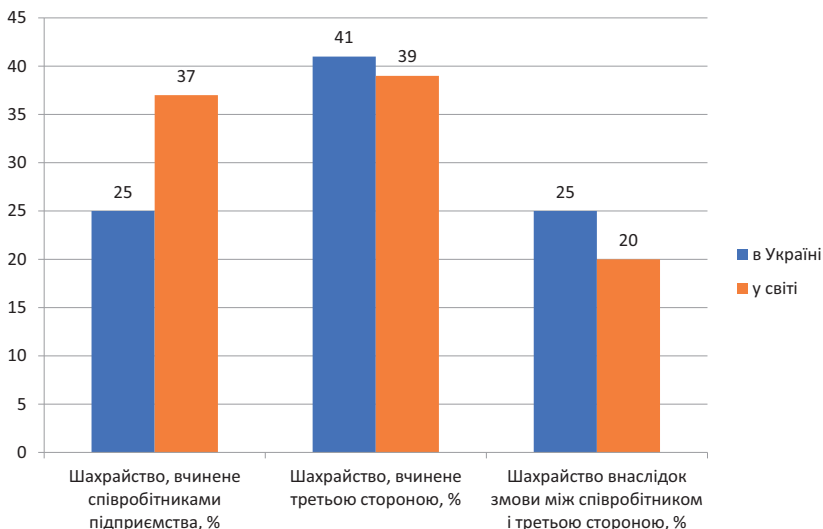


Рис. 3.1. Суб’єкти фінансового шахрайства в підприємницькій діяльності у 2020 р. [41]

Внаслідок проведеного опитування керівників/власників суб’єктів підприємництва на предмет вчиненого фінансового шахрайства, виявлено такі основні суб’єкти зловмисних дій (див. рис. 3.2):

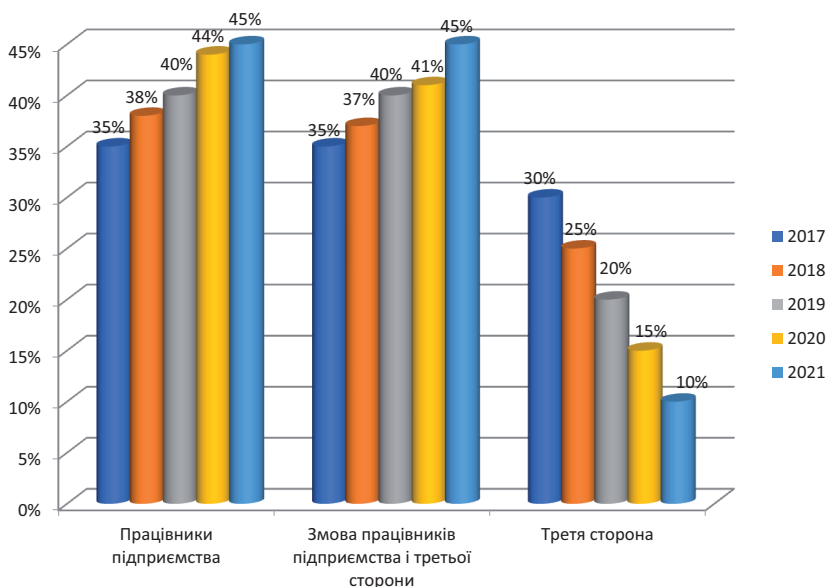


Рис. 3.2. Учасники фінансового шахрайства в діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею пальним в Україні впродовж 2017–2021 рр.

Джерело: сформувала автор за даними анкетування

Щодо масштабів вчинення та видів шахрайства, то у 2020 р. 51 % вітчизняних ділових одиниць зазнали шахрайства порівняно з 48 % у 2018 р. До основних видів економічних злочинів і шахрайства згідно з матеріалами Всесвітнього дослідження економічних злочинів та шахрайства, проведеного PwC Україна, належали такі [41]:

- незаконне привласнення майна – 47 % респондентів;
- хабарництво і корупція – 47 %;
- шахрайство зі сторони клієнтів – 31 %;
- кіберзлочини – 31% респондентів;
- шахрайство у сфері закупівель – 31 %.

Інше дослідження, проведене Association of Certified Fraud Examiners (ACFE) у 2020 р розкрило такі найпоширеніші напрями вчинення шахрайських дій (рис. 3.3): випадки корупції, шахрайство при безготівкових та готівкових розрахунках, операції з готівковими та безготівковими коштами [386].

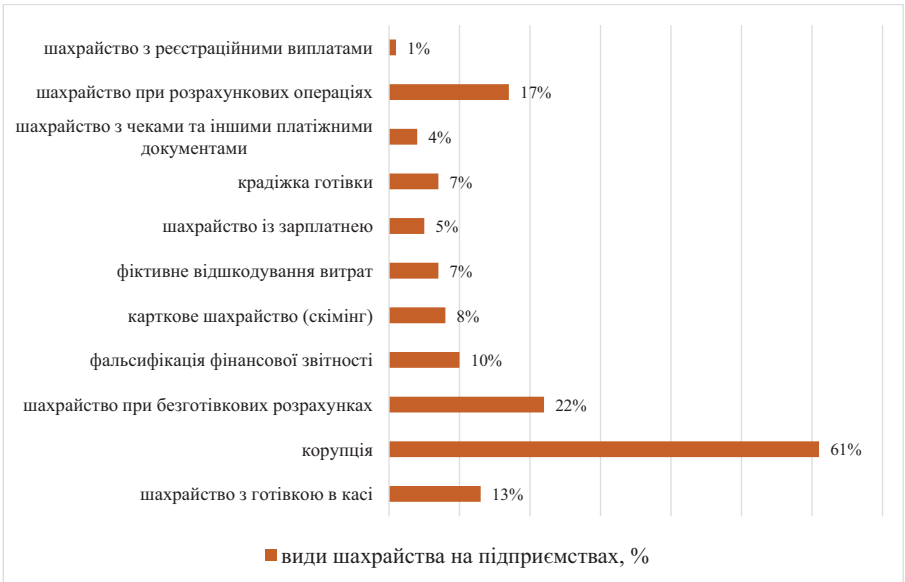


Рис. 3.3. Види та кількість випадків корпоративного шахрайства у світі у 2020 р. [386]

Згідно з рівнями управління й відповідними злочинами, вчинюваними такими працівниками, можна виокремити такі зловживання менеджерів середньої ланки суб'єктів підприємництва:

- змова менеджерів з підрядниками або постачальниками, що дає змогу останнім необґрунтовано завищувати ціни, “нагромаджувати” дебіторську заборгованість або постачати неякісні товари й послуги;
- несанкціонований продаж і використання майна;
- викрадення активів (активи, за різними даними, викрадають від 70 до 95 % працівників українських підприємств) [87];
- оплата роботи підставних осіб;
- фальсифікація бухгалтерських документів і записів, звітів;
- реалізація товарів з відтермінуванням платежу ненадійним покупцям;
- несанкціоновані операції з цінними паперами, матеріальними й нематеріальними активами підприємства.

Щодо сфер діяльності, то у світовому масштабі найбільшу частку випадків шахрайства було зафіксовано в сфері банківської діяльності й фінансових послуг та у виробництві (рис. 3.4).

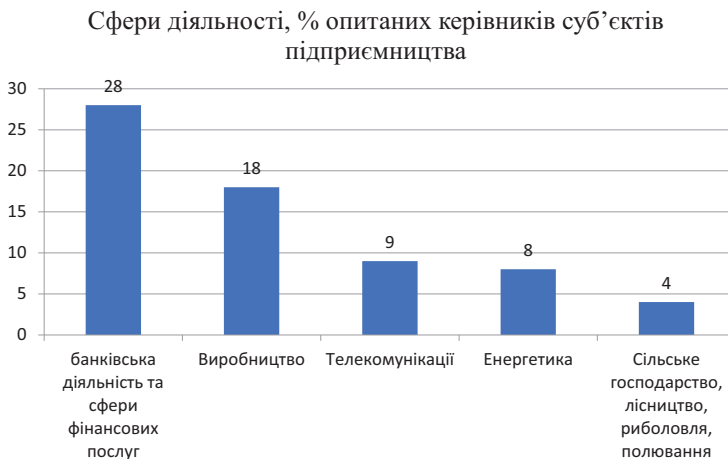


Рис. 3.4. Випадки фінансового шахрайства за сферами діяльності у 2020 р. [386]

Злочини в банківських установах становлять особливу небезпеку для національної економіки загалом, оскільки неминуче знижують рівень їх фінансової безпеки, що своєю чергою зумовлює послаблення довіри до них з боку населення і юридичних осіб. Банківський сектор є особливо чутливим до інформації про фінансову стабільність та спроможність протидіяти внутрішнім і зовнішнім загрозам.

Аналіз практичної діяльності банківських установ та праць учених, що працюють у цій сфері [116; 125; 134; 135; 349; 350], дає підстави виділити такі види фінансового шахрайства в підрозділах банківських установ відповідно до видів діяльності [10, с. 416–422].

У сфері розрахунково-касового обслуговування:

- крадіжка коштів з каси касиром з надією зникнути до початку ревізії каси. Наразі в більшості банків цей вид шахрайства неможливий з огляду на жорсткий контроль та щоденну інвентаризацію залишків у касі;
- фабрикування документів, що приховують нестачу. Після незаконного взяття грошей з каси і неможливості їх повернути відбувається фабрикування документів на суму нестачі;
- зумисна крадіжка коштів, що пояснюється випадковою помилкою касира. За цього способу викрадають невелику суму грошових коштів. Нестачу в касі зловмисник пояснює “несвідомими” помилками;

– крадіжка коштів сторонньою особою. Така можливість виникає у випадку потрапляння в приміщення каси сторонніх осіб;

– приховування залученого депозиту. За цією схемою клієнту видають усі необхідні документи про залучення його коштів на депозит, проте ці суми не оприбутковують. Після закінчення терміну депозиту гроші повертаються клієнту з неоприбуткованих коштів, покладених на депозит іншим клієнтом (т. зв. операція “перекриття”);

– несанкціоноване списання коштів з рахунку клієнта. Цю схему можна реалізувати, якщо бухгалтер неухважний і не стежить за рухом коштів на рахунок свого підприємства. За таких умов гроші можна списувати на третю організацію;

– перерахування коштів від імені банку. Кошти знімають не з розрахункового рахунку клієнта, а роблять платіж від імені банку на фіктивну фірму без документів, що підтверджують операцію;

– підміна справжньої валюти фальшивою. Видавання фальшивих грошових купюр і досі є поширеним явищем в обмінних пунктах. У банківських установах можуть відбуватися зловживання, коли клієнтам видають старі і знищені купюри, які важко згодом реалізувати;

– витягування купюр із пачок. Якщо клієнт отримує достатньо велику суму коштів, то в банку у нього часто немає змоги перерахувати кількість купюр у кожній пачці. І лише згодом, за межами банку, виявляють нестачу;

– обман малоосвічених, довірливих та хворих клієнтів. На практиці дуже часто не лише люди похилого віку, але й чимало осіб середнього віку не завжди уважно читають документи, які підписують, чим можуть скористатись шахраї;

– списання нестачі на інші банківські відділення. У разі доступу працівників розрахунково-касового центру до бухгалтерських документів утворену нестачу часто списують на інші відділення банку, де її можуть виявити лише через значний період часу.

У сфері кредитування необхідно виокремити такі фінансові злочини:

– кредитування позичальників, яких не існує. За цього виду шахрайства до розгляду ухвалюють фальшиві заяви про надання кредиту, підкріплені недостовірною фінансовою звітністю;

– кредит під фіктивну заставу чи поручництво. Типовим для шахраїв явищем є отримання кредиту з подальшим його

неповерненням. Можливі випадки, коли працівники банку за винагороду допомагають отримати кредит за відсутності достатньої застави або поручництва. Оцінку реальної вартості застави як перед одержанням кредиту, так і в міру його погашення повинні здійснювати відповідальні за це особи банку, безпосередньо не пов'язані з працівниками, що видають кредит;

- кредитування з подальшим “відкатом” та подальшим перерозподілом коштів. За цього виду шахрайства недобросовісні працівники банку можуть надавати кредит своїм спілнякам, які потім передають їм усі або частину отриманих коштів. У деяких випадках позики можуть списувати на безнадійні борги;

- необґрунтовані кредити підприємствам, у яких є особиста зацікавленість. За умов, коли вищі посадові особи банку мають фінансові інтереси у комерційних структурах, можливим є кредитування “своїх” підприємств під пільговий відсоток навіть без застави або поручника;

- неправомірне звільнення застави. Банк може зазнати значних збитків через неправомірне звільнення застави під кредит.

У сфері управління залученими ресурсами й цінними паперами варто виділити такі види фінансового шахрайства:

- передача клієнтської бази банкам-конкурентам. Інколи працівники середньої ланки банку передають інформацію про своїх клієнтів банкам-конкурентам та працюють з метою задоволення їхніх інтересів;

- заниження ставок у разі продажу ресурсів на міжбанківському ринку. Працівник у конфіденційному порядку домовляється з іншим банком про продаж ресурсів за заниженою процентною ставкою. Потім різницю (або частину різниці) у доході за реальною і заниженою ставками віддають працівникові, що забезпечив продаж дешевших ресурсів;

- приховування частини виторгу від продажу цінних паперів клієнтів. Клієнти, що продають цінні папери через брокера банку, часто не порівнюють процентний дохід, зазначений у звіті про продаж цінних паперів, отриманому від брокера банку, з ринковим котируванням цінних паперів на дату продажу. Це дає змогу занижувати у звіті про продаж цінних паперів реальну ціну й забезпечувати особистий дохід, часто оформлюваний на третю фірму як комісійні за посередництво. Така діяльність на практиці є недостатньо контрольованою, тому такі крадіжки можуть довго не виявляти. Цей вид шахрайства трапляється не тільки у

разі продажу цінних паперів клієнтів, але й у випадку їхнього придбання, коли у звіті про купівлю цінних паперів наводять ціну, вищу за фактичний біржовий курс;

- продаж в особистих цілях цінних паперів банку. Цей вид шахрайства поширений у закордонних та вітчизняних невеликих банках, коли операції з цінними паперами контролює переважно один працівник;

- зумисна неефективна купівля цінних паперів. За такого виду шахрайства брокер вступає в угоду з емітентами не дуже вигідних цінних паперів або тих, ціна на які штучно завищена. Потім він умовляє клієнта купити пропоновані ним цінні папери, одержуючи від емітентів комісійні.

У сфері здійснення валютних операцій можуть бути такі види фінансових злочинів:

- списання коштів з кореспондентських рахунків свого банку в закордонному банку. З боку працівника банку може бути “нахабне списання” грошей на свій рахунок або рахунок компаньйона. Звичайно, для такого списання використовують фіктивні документи;

- неправильне перерахування курсу валюти. В умовах постійної й динамічної зміни курсу валют відкриваються додаткові можливості для махінацій. Вони ґрунтуються на неправильному перерахуванні курсів валют.

Серед інших видів фінансового шахрайства виділяють зловживання, що їх здійснюють бухгалтери, злочини з банківськими скриньками та фінансові махінації з пластиковими картками.

До шахрайських операцій, які можуть відбуватися через бухгалтерію банку, передусім належать такі:

- заниження комісійних зборів за рахунками клієнтів. У цьому випадку суму належних клієнтові комісійних зборів занижують, а різницю відносять на особистий рахунок бухгалтера або на рахунок підставної фірми;

- маніпулювання з процентами, що нараховують на внески клієнтів. Таке шахрайство відбувається як завищення фактичних відсотків, які нараховують за рахунками, і використання суми завищення для компенсації фіктивних видатків. У невеликих банках, де бухгалтерам дозволено мати доступ до готівки й чужих бухгалтерських записів, можливості для зловживань розширені завдяки одержанню готівки й приховуванню нестачі за бухгалтерськими проведеннями.

Поширеними на сьогодні є злочини з банківськими картками, зокрема такі:

– вдаване опитування в соціальних мережах з розіграшем призів. Це спосіб шахрайства з метою викрадення коштів з картки шляхом надсилання в соціальних мережах та месенджерах повідомлення про виграш грошових призів від імені банку, для отримання яких необхідно надати інформацію про кредитну картку;

– телефонний дзвінок з метою отримати секретні дані. У цьому випадку шахраї обманним шляхом отримують інформацію про платіжну картку по телефону для майбутнього зняття коштів;

– заміна SIM-карти для доступу до онлайн-банкінгу. Це спосіб шахрайства, за якого зловмисники отримують доступ до банківського акаунта жертви шляхом заміни SIM-карти;

– використання незахищених сайтів для вчинення шахрайських дій. Якщо веб-майданчик використовує застарілу технологію передачі даних без шифрування, здійснювати оплату послуг чи товарів в інтернеті небезпечно у зв'язку з відсутністю надійного захисту інформації про кредитну карту та високий ризик шахрайства;

– фішинг. Шахраї отримують секретну банківську інформацію, створюючи веб-сторінки або шляхом відправлення електронних листів на email від імені відомих веб-ресурсів або банків, послугами яких жертва користується та довіряє;

– копіювання даних картки при передачі в руки. Цей вид шахрайства поширений в окремих країнах з високим потоком туристів. Зловмисники у сфері послуг фіксують дані карток клієнтів при здійсненні ними оплати;

– використання для шахрайських дій незахищених мереж Wi-Fi. Цей вид шахрайства передбачає викрадення зловмисниками конфіденційної інформації при використанні онлайн-банкінгу за допомогою мережі Wi-Fi у публічних місцях;

– впровадження шпигунських програм у комп'ютери у громадських місцях. Відомі випадки, коли комп'ютери у місцях загального доступу до інтернету (бібліотеки, інформаційні центри тощо) були обладнані спеціальним програмним забезпеченням для відстежування дій користувачів, запам'ятовування інформації, введеної з клавіатури;

– скімінг для крадіжки даних картки. Шахрайство вчиняється шляхом використання спеціального обладнання для крадіжки даних карти (спеціальні накладки на картридж для картки та на клавіатуру для введення пін-коду, прикріплені міні-відеокамери для запису інформації з карток).

Серед шахрайських дій у банківських установах виявлялися також випадки зловживань із доступом до банківських сховищ, зокрема, шляхом несанкціонованого проникнення в камери для зберігання за відсутності власників за допомогою таємно виготовлених дублікатів ключів клієнтів.

Опитування керівників суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні дало змогу нам виявити найпоширеніші види та динаміку фінансового шахрайства впродовж останніх п'яти років (див. рис. 3.5)

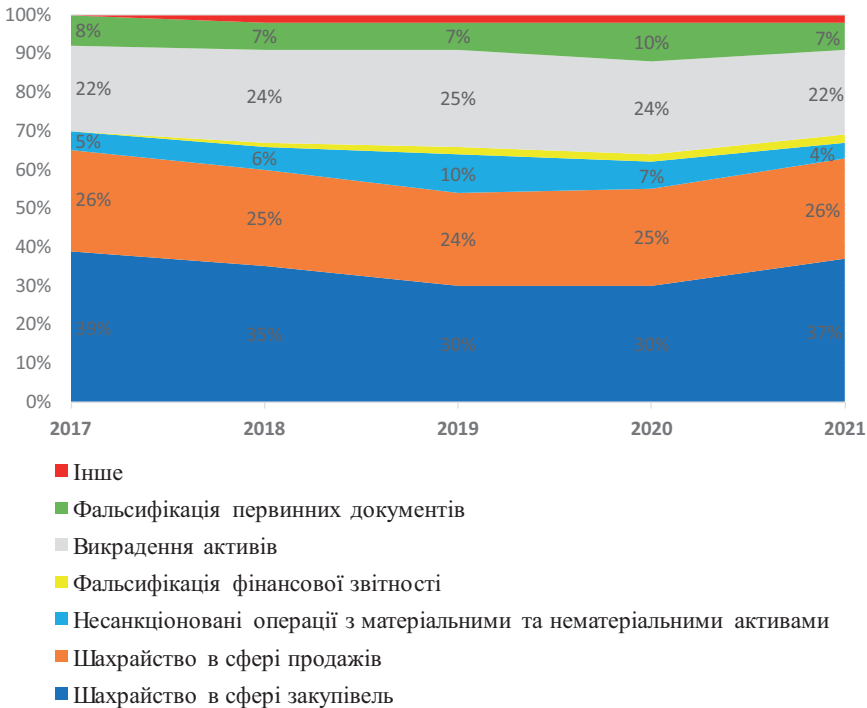


Рис. 3.5. Динаміка випадків фінансового шахрайства в діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні впродовж 2017–2021 рр.

Джерело: сформувала автор на основі анкетування

Як видно з рис 3.5, шахрайство в сфері закупівель та продажів становили найбільшу частку в структурі фінансових злочинів досліджуваних підприємств.

Фінансове шахрайство спричиняє значні деструктивні наслідки для функціонування суб'єктів підприємництва, знижуючи рівень їх фінансової безпеки. За даними досліджень міжнародних організацій ми виявили такі оцінки збитків підприємств упродовж останніх п'яти років:

– Згідно з даними міжнародного звіту “Grant Thornton International Business” економічні злочини працівників трапляються у понад 40 % компаній, які втрачають у цих умовах близько 7 % доходу [277, С. 148].

– За результатами Association of Certified Fraud Examiners (міжнародна організація, яка провадить боротьбу з шахрайством), через шахрайство співробітників підприємства втрачають близько 6 % свого обороту [87].

– Відповідно до результатів дослідження економічних злочинів та шахрайства, проведеного PWC упродовж 9 % опитаних керівників підприємств унаслідок шахрайства отримали збитки більше 1 млн дол. США (рис. 3.6)

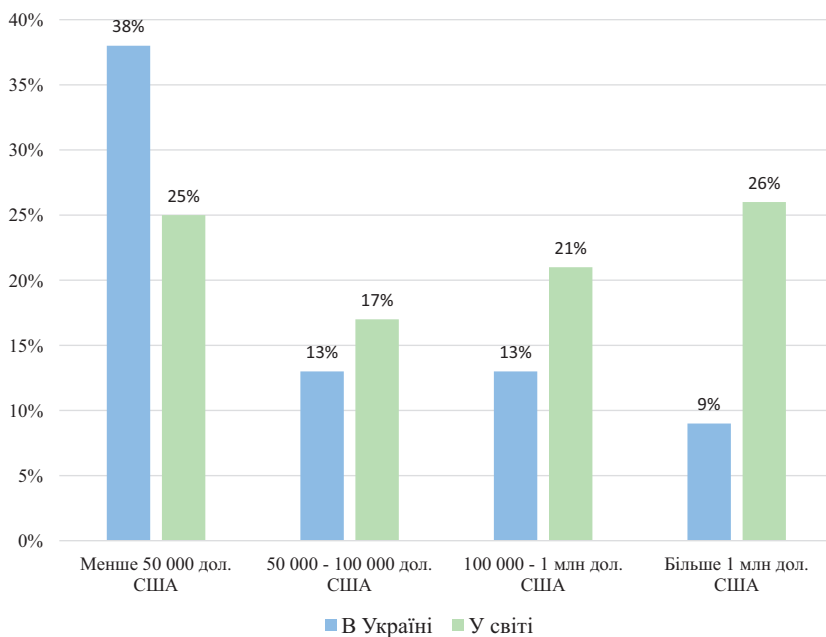


Рис. 3.6. Сума прямих збитків, яких зазнали українські та іноземні організації, дол. США у 2019–2020 рр. [41]

Чимало випадків фінансового шахрайства спричинили катастрофічні наслідки для функціонування суб'єктів підприємництва як в Україні, так і в світі. З метою порівняння вітчизняного і світового досвіду вчинення шахрайства та методів протидії цьому деструктивному явищу в підприємницькій діяльності ми провели аналіз окремих випадків таких зловмисних дій і їх наслідків для фінансової безпеки ділових одиниць. Для прикладу, акціонери американської енергетичної компанії “Enron”, яка за версією ділового видання “Fortune” впродовж низки років займала місце “Найбільш інноваційна компанія Америки” втратили 74 млрд дол. у зв'язку із приховуванням її керівництвом фінансових втрат, отриманих у результаті торгових й інших операцій. Причиною цього був передусім конфлікт інтересів топ-менеджерів, які отримували винагороду за декларований бухгалтерський прибуток та інтересами корпорації в цілому, а також відсутність ефективної системи зовнішнього та внутрішнього контролю в зв'язку з повною довірою інвесторів [259].

Генеральний директор міжнародного концерну в сфері електроніки, інформаційних технологій, медицини та охоронного обладнання “Tусо International Ltd” та CFO здійснювали відмивання коштів через несанкціоновані кредити та продаж акцій шахрайським способом. Втрати компанії внаслідок цього становили 150 млн дол. Комісія з цінних паперів та бірж (SEC) та Окружна прокуратура Манхеттену внаслідок фінансового розслідування виявила використання сумнівних методів бухгалтерського обліку та обсяги позик на значні суми коштів, надані генеральному директору компанії [259].

Інвестиційна компанія “Madoff Investment Securities LLC” залучила шляхом обману 64,8 млрд від інвесторів та сплачувала їм відсотки не за рахунок отриманого прибутку, а з їх же власних коштів або коштів інших інвесторів. Цей вид шахрайства відомий як “Піраміда Понці” (схема масового фінансового шахрайства, вчиненого засновником фінансових пірамід у США і Канаді Чарльзом Понці, за якою виплати надзвичайно високих і нереальних прибутків інвесторам надходили із вкладів нових інвесторів [259].

Поширення фінансового шахрайства в діяльності суб'єктів підприємництва та масштаби впливу на фінансову безпеку потребують застосування, передусім, ефективних інструментів його виявлення.

Аналізуючи дані міжнародних опитувань у цій сфері ми виявили доволі важливий факт – найпоширенішим методом розкриття зловмисних дій у закордонній практиці є повідомлення (див. рис. 3.7).

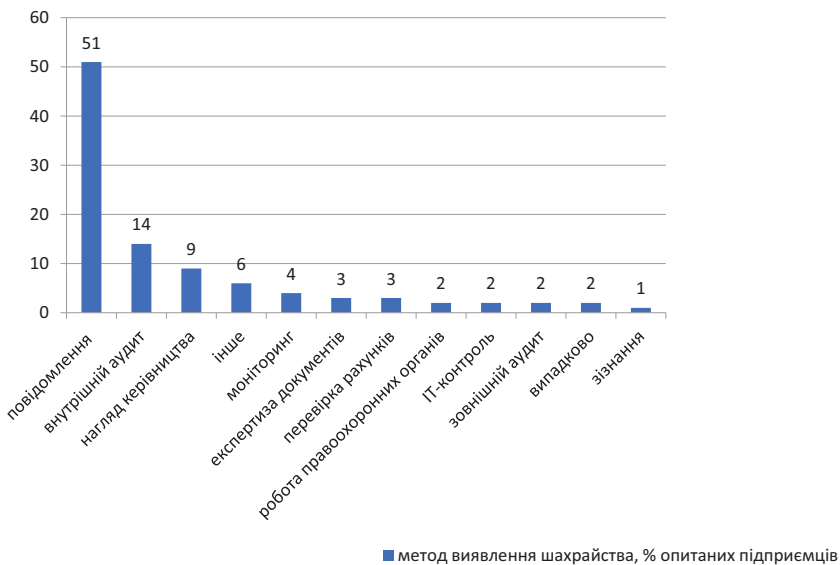


Рис. 3.7. Методи виявлення шахрайства в підприємницькій діяльності у 2020 р. [386]

Основними суб'єктами повідомлень про шахрайства були працівники досліджуваних підприємств (див. рис. 3.8).

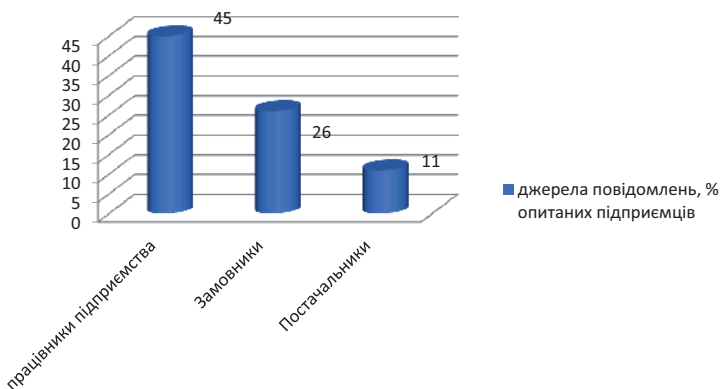


Рис. 3.8. Джерела повідомлень про випадки шахрайства на підприємствах у 2020 р. [386]

Серед способів повідомлень найбільшу частку становили повідомлення шляхом заповнення онлайн-форми та повідомлення поштою (рис. 3.9).

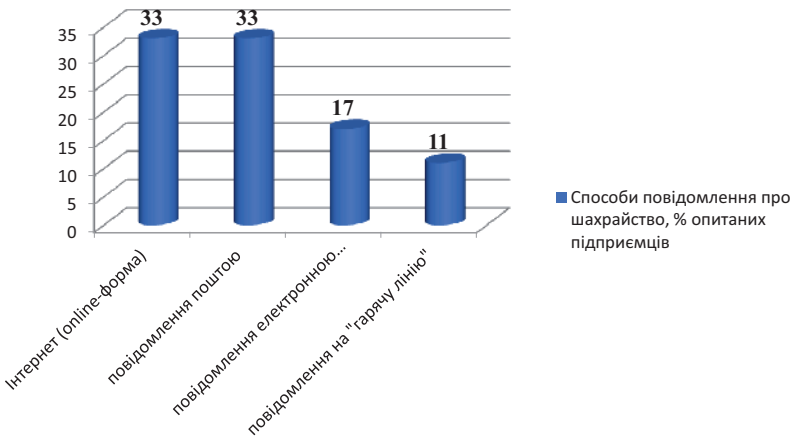


Рис. 3.9. Способи повідомлень про шахрайство на підприємствах у 2020 р. [386]

Окремої уваги заслуговує “гаряча лінія” як спосіб повідомлення про шахрайство в діяльності ділових одиниць. Зокрема, 57 % повідомлень надходило до опитаних суб’єктів господарювання, що мали “гарячу лінію” (див. рис. 3.10).

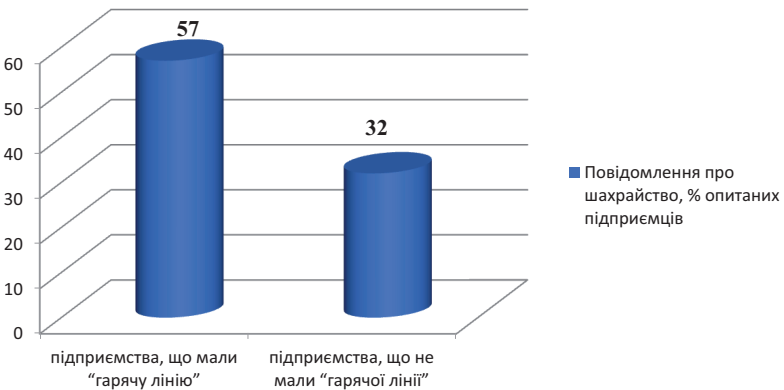


Рис. 3.10. Повідомлення про випадки шахрайства з використанням/невикористанням “гарячої лінії” у 2020 р. [386]

Ефективність використання “гарячої лінії” засвідчують також втричі менші втрати в діяльності тих ділових одиниць, які використовували цей інструмент захисту від фінансової злочинності (рис. 3.11)

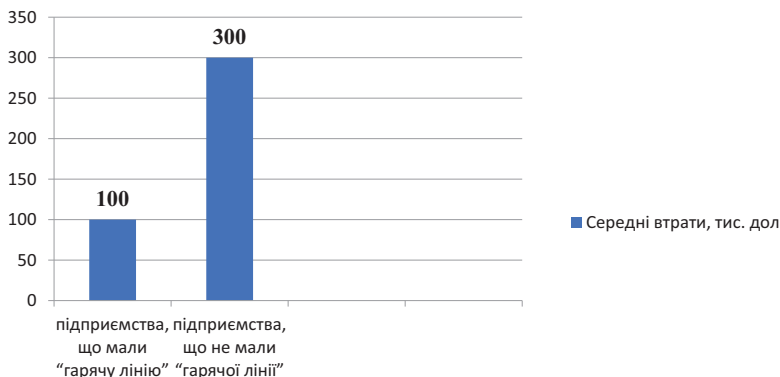


Рис. 3.11. Втрати підприємств від шахрайства відповідно до наявності “гарячої лінії” у 2020 р. [386]

До найефективніших методів боротьби з фінансовим шахрайством відповідно до результатів опитування підприємств, належить зовнішній та внутрішній аудит, наявність Кодексу корпоративної поведінки, нагляд керівництва та сертифікація фінансової звітності (рис. 3.12):

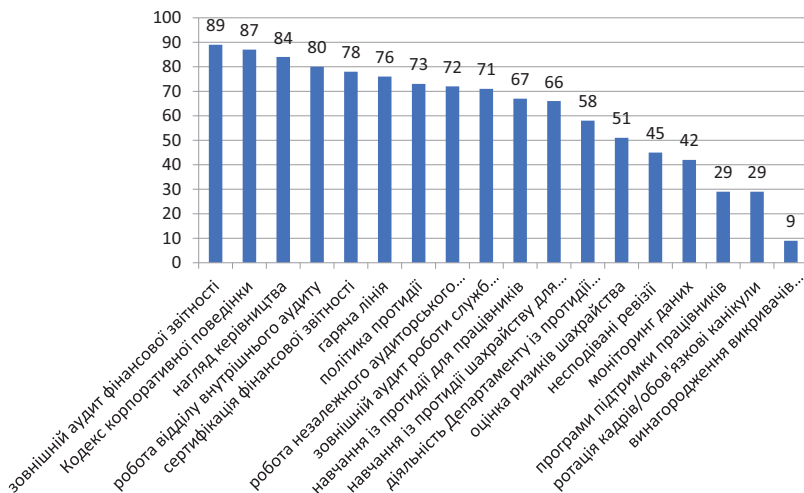


Рис. 3.12. Найпоширеніші способи боротьби з шахрайством у 2020 р. [386]

Щодо способів протидії фінансовому шахрайству, то згідно з результатами дослідження PwC, майже половина керівників підприємств в Україні не проводить взагалі або проводить лише неформальну перевірку й постійний моніторинг доброчесності своїх контрагентів. Лише 59 % українських організацій здійснювали розслідування найбільш значного за наслідками випадку шахрайства та третина респондентів повідомила про нього наглядову раду. Кожне четверте підприємство в Україні не має спеціальної програми з управління ризиками, 22 % респондентів не проводять оцінки ризиків [41].

Окрім виокремлених нами раніше наслідків фінансових злочинів, вчинюваних працівниками у формі втрати доходу, важливо виділити також такі (рис. 3.13):



Рис. 3.13. Наслідки помилок і шахрайства, вчинюваних у фінансовій сфері працівниками суб'єктів підприємництва

Джерело: узагальнено автором на основі проведеного дослідження

Однією із причин поширення фінансового шахрайства є підвищений рівень складності функціонування суб'єктів підприємництва, який притаманний часовому періоду 2020–2022 рр. – пандемія Covid-19, російська гібридна агресія та повномасштабне вторгнення в Україну. В таких умовах зовнішні виклики й загрози фінансовій безпеці концентрують увагу власників й керівників на їхній нейтралізації, позаяк зростає вірогідність негативного впливу на результати фінансово-господарської діяльності суб'єктів господарювання саме від працівників. Водночас, аналіз наукових праць, присвячених вивченню проблем

фінансових зловживань [25; 62; 110; 301] і проведене нами опитування керівників/власників суб'єктів підприємництва на предмет вчиненого фінансового шахрайства їх співробітниками, дав змогу виділити такі вагомі причини посадових зловживань і помилок, вчинюваних у фінансовій сфері (рис. 3.14):



Рис. 3.14. Систематизація причин фінансового шахрайства та помилок вчинюваних працівниками суб'єктів підприємництва

Джерело: узагальнено автором на основі проведеного дослідження

Різні рівні повноважень працівників призводять до різного рівня наслідків і втрат. Здебільшого, шахрайство керівників вищої ланки управління становить найбільш вагомую загрозу фінансовій безпеці суб'єктів підприємництва через значущість фінансових рішень, ухвалюваних ними, водночас в умовах діджиталізації й зростання злочинів із конфіденційною інформацією працівник нижчої ланки управління, спричинивши витік комерційної таємниці шляхом несанкціонованого доступу до інформаційної мережі, також може спричинити деструктивний вплив на діяльність підприємства значного масштабу. Масштабність деструктивного впливу посадових помилок та шахрайства на фінансову безпеку ділових одиниць зумовлює, передусім, встановлення ознак, за якими їх можна виявити. На нашу думку, основними з них є такі (рис. 3.15):

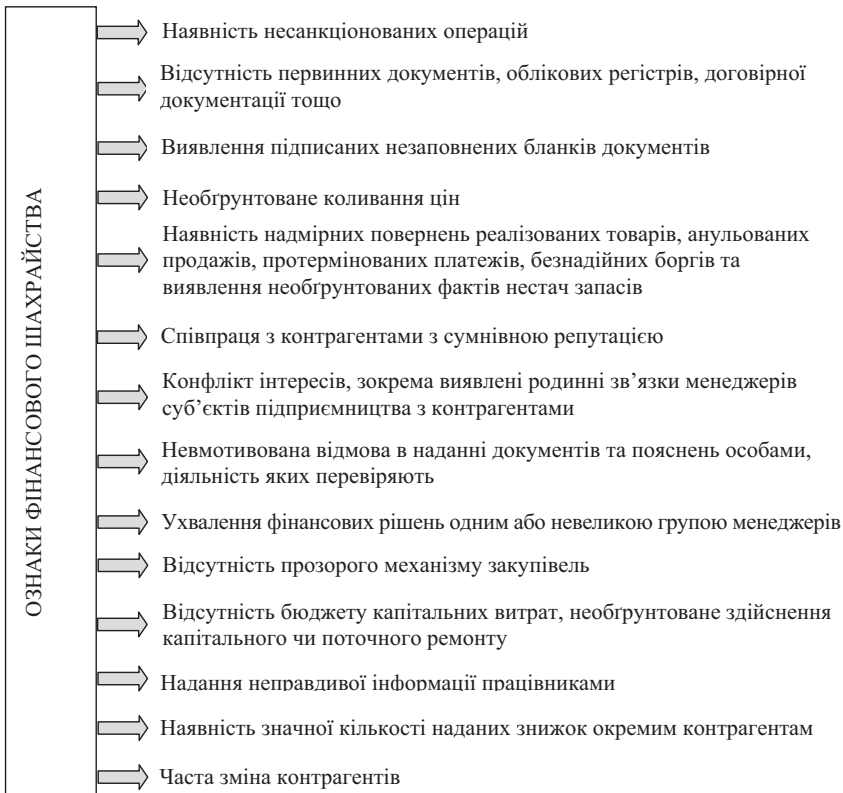


Рис. 3.15. Систематизація ознак фінансового шахрайства у діяльності суб'єктів підприємництва

Джерело: сформувала автор

Гібридний характер фінансового шахрайства потребує врахування загроз, що можуть генеруватися працівниками різного рівня й налагодження їх ефективної роботи шляхом скорочення як випадків фінансових зловживань, так і посадових помилок. Водночас першочергово це стосується працівників фінансових служб підприємства, до яких належать фінансові директори, менеджери, головні бухгалтери, скарбники, аудитори, ревізори й інспектори.

Вимоги до рівня й якості професійної підготовки персоналу повинні бути чітко й детально визначені. Ці критерії повинні бути регламентовані правовими актами на державному рівні та корпоративною культурою і нормативними документами на рівні підприємств. Водночас в умовах гібридних фінансових конфліктів дотримання лише формальних вимог компетентності до окремих категорій фінансових працівників недостатньо. Потрібно встановлювати критерії їх особистісних характеристик, особливостей компетентності в нестандартних ситуаціях.

Цікавим є підхід до визначення компетентності з функціональних позицій американським ученим Л. Пітером [382]. На підставі аналізу значного обсягу фактичного матеріалу з різноманітних сфер життя він сформулював емпіричне узагальнення, відоме під назвою “Принцип Пітера”: в ієрархії кожний індивід має тенденцію підніматися до свого рівня некомпетентності.

Ми проаналізували підходи вчених до розуміння компетентності, зокрема такі:

– компетентність – особисті характеристики індивіда, що зумовлюють максимально високий рівень виконання роботи [352, с. 56];

– компетентність – це типова модель поведінки, що охоплює знання, навички, спосіб мислення, які можуть використовуватися поодиночі, або в різних комбінаціях для успішного досягнення найвищої ефективності в роботі [362, с. 245];

– компетентність – це інтегративне утворення особистості, що інтегрує в собі знання, уміння, навички, досвід і особистісні властивості, які обумовлюють прагнення, здатність і готовність розв’язувати проблеми і завдання, що виникають у реальних життєвих ситуаціях, усвідомлюючи при цьому значущість предмета і результату діяльності” [50, с. 24];

– компетентність – спроможність особистості сприймати та відповідати на індивідуальні і соціальні потреби; комплекс ставлень, цінностей, знань та навичок [139, с. 92];

– компетентність – це інтегрована характеристика якості особистості, результативний блок, сформований через досвід, знання, вміння, ставлення, поведінкові реакції, або спеціально структуровані (організовані) набори знань, умінь, навичок і ставлень, що їх набувають у процесі навчання і які дозволяють людині визначати і розв’язувати, незалежно від ситуації, проблеми, характерні для певної сфери діяльності [256].

У нормативно-правових актах поняття “компетентність” визначається як динамічна комбінація знань, умінь і практичних навичок, способів мислення, професійних, світоглядних і громадянських якостей, морально-етичних цінностей, яка визначає здатність особи успішно здійснювати професійну та подальшу навчальну діяльність і є результатом навчання на певному рівні вищої освіти [216.].

Компетентність має складну, багатогранну та різнопланову природу, дослідження якої дало нам змогу виділити такі складові фінансової компетентності й відповідні критерії оцінювання кожної з них (див. рис. 3.16).

Інтелектуальна складова компетентності передбачає наявність певних знань, потрібних для виконання професійних обов’язків, постійне їхнє оновлення шляхом відслідковування найновіших досягнень вітчизняної та зарубіжної науки, що належать до сфери фінансового управління та фінансової безпеки. На важливості інтелектуальної складової фінансової безпеки наголошує також І. Ревак [260].

Нормативна складова компетентності передбачає обсяг прав та обов’язків працівників фінансової служби, встановлених законодавством й посадовими інструкціями суб’єкта підприємництва.

Функціональна складова компетентності виявляється у здатності працівників фінансової служби діяти в різних умовах, швидко адаптуватися до раптових змін й належно виконувати свої професійні обов’язки. В умовах цифровізації економічних процесів необхідним навиком є також володіння сучасними інформаційними технологіями та засобами забезпечення конфіденційних даних від кіберзагроз.

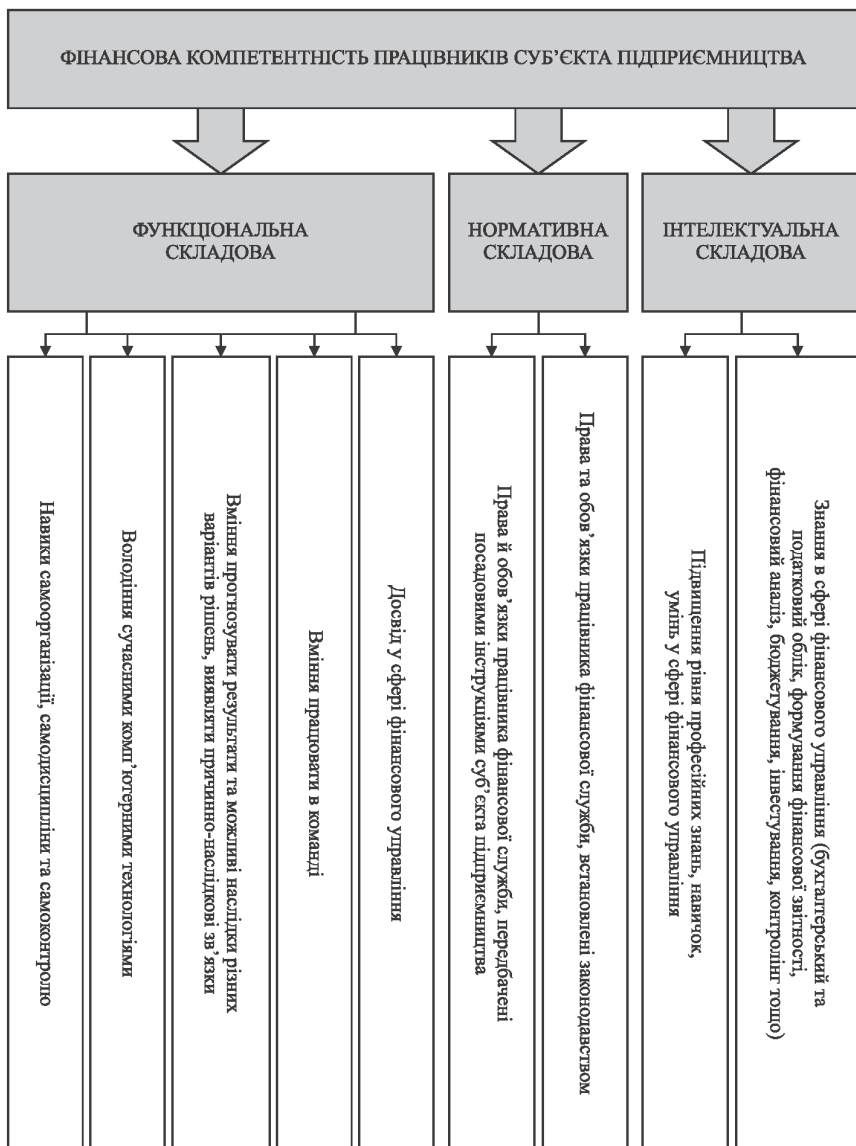


Рис. 3.16. Складові фінансової компетентності працівників

Джерело: розробила автор

Водночас високий рівень фінансової компетентності працівників не унеможливує фінансові зловживання з їх сторони. Згідно з теорією

Дональда Крессі “Трикутник шахрайства” (Donald Cressey's Fraud triangle) (рис. 3.17) для виникнення злочинів у фінансовій сфері, що вчиняються співробітниками, необхідно виконання трьох умов: необхідність (motive), можливість (opportunity) та обґрунтування (rationalization).



Рис. 3.17. “Трикутник шахрайства” Дональда Крессі (Donald Cressey's Fraud triangle) [358, С. 29-40]

Мотивом до вчинення фінансового шахрайства зі сторони персоналу ділових одиниць може бути як погіршення власного фінансового становища й термінова потреба у фінансових ресурсах, так і особистісні характеристики працівників. Можливості (opportunity) для вчинення економічних злочинів персоналом з’являються за відсутності контролю за кожною зі сфер фінансово-господарської діяльності та зростають у період кризових ситуацій, зокрема під час пандемії Covid-19 кількість випадків шахрайства зросла в зв’язку зі зміщенням уваги власників та топ-менеджменту із питань управління фінансовою безпекою на втримування своїх позицій на ринку. Обґрунтуванням (rationalization) до вчинення шахрайства зі сторони працівників є незадовільний рівень їхньої заробітної плати та інших складових мотиваційного забезпечення. Випадки шахрайства також є більш поширеними у колективах з некомфортною психологічною атмосферою.

Щоб протидіяти шахрайству в підприємницькій діяльності, необхідно намагатись усунути розкриті в “трикутнику шахрайства” умови, що, на наш погляд, можна реалізувати шляхом реалізації таких заходів (рис. 3.18):



Рис. 3.18. Напрями протидії виникненню умов для вчинення шахрайства згідно з “Трикутником шахрайства” Дональда Крессі

Джерело: доповнила автор на основі [358]

Пандемія Covid-19 зумовила виникнення нового формату виконання посадових обов'язків працівниками суб'єктів підприємництва – дистанційно. Це своєю чергою зумовило виникнення нових загроз фінансовій безпеці зі сторони працівників через важкість здійснення контролю. Крім того, фінансова криза, спричинена карантинними обмеженнями, погіршила фінансове становище багатьох працівників, що підвищило ризики виникнення фінансових злочинів зі сторони персоналу із деструктивними сутнісними характеристиками.

На наш погляд, одним із способів усунення чинника мотиву до вчинення шахрайства є комплексна оцінка благонадійності працівників під час їхнього прийняття на роботу, яка сприятиме виявленню осіб, що схильні до недобросовісної та непродуктивної поведінки на робочому місці.

Необхідність оцінки благонадійності працівників підтверджується результатами наукового дослідження ефективності різних методів, що використовуються в практиці прогнозування результативності кандидатів на відповідних посадах, які опублікували 1998 р. професори Ф. Шмідт і Дж. Хантер [387, с. 262–274]. Результативність працівників, здебільшого, оцінювали із врахуванням рейтингу керівників, звітних даних щодо результатів виробництва, рівня продажів тощо. Отримані результати дослідження (див. додаток Д) підтвердили, що попри те, що оцінка розумових здібностей працівників є необхідною базовою вимогою і становить основу їхніх професійних знань та навиків, це, однак, не виключає наявності у працівників високого фахового рівня особистісних характеристик, що сприяють шахрайству. Відтак, використання тестів на благонадійність дає змогу не лише прогнозувати деструктивну поведінку кандидатів при прийнятті їх на роботу, але й планувати її результативність.

Важливість психологічної, а саме – емоційної компетентності персоналу, яку визначають EQ (Emotional Quotient або Emotional Intelligence) – емоційним показником інтелекту підтверджують також дослідження Д. Гоулмана, згідно з яким успіх управлінської роботи на 85 % визначається цим показником, і лише на 15 % – загальновідомим IQ (Intelligence Quotient) [369].

Психологи Дж. Майер, Д. Карузо, П. Саловой [364; 379] відзначають, що люди, які володіють високим рівнем EQ, здатні до швидшого прогресу в певних галузях і більш ефективного використання своїх здібностей. Відтак, хоча емоції та інтелект зазвичай розмежовують між собою, насправді вони є взаємопов'язаними. Погоджуємося також з О. Підхонним [195, с. 82], що навички емоційної компетентності дають змогу керівникам використовувати свої емоції та емоції підлеглих як цінний інформаційний ресурс.

Пропонуємо оцінювання благонадійності працівників здійснювати за такими їх психологічними характеристиками (рис. 3.19).

Аналіз проблематики фінансового шахрайства працівників з позицій фінансового й соціально-психологічного підходів дав нам можливість виявити складність мотивів зловмисників, гібридність шахрайських дій та причини виникнення фінансового шахрайства (неякісна кадрова перевірка під час приймання на роботу, проблеми формування корпоративної культури; прогалини менеджменту).

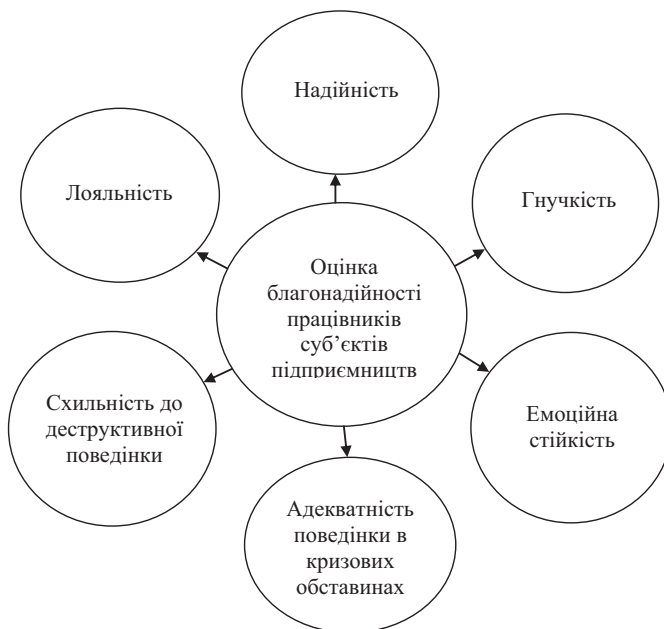


Рис. 3.19. Систематизація психологічних характеристик для оцінювання благонадійності працівників

Джерело: розробила автор

Водночас важливим є також з'ясування чинників, які зумовлюють поширення фінансового шахрайства в підприємницькій діяльності. Відтак, з метою забезпечення фінансової безпеки ділових одиниць, на нашу думку, вагоме значення має також сформована на підприємстві система реагування на розкриття шахрайських схем й покарання зловмисників. У цьому контексті нам імпонує метафоричний підхід, який 1982 р. описали Дж. Вілсон і Дж. Келлінг у теорії “розбитих вікон” [376], де йдеться про безкарність як ключову проблему поширення фінансових злочинів. Учені порівнюють випадки злочинів із розбитими вікнами в будинку. Відповідно до цієї теорії, якщо хтось розбив скло в будинку і ніхто не встановив нове, то незабаром жодного цілого вікна в цьому будинку не залишиться. Люди схильні порушувати звичні норми поведінки, коли бачать, що інші теж так вчиняють. Злочинність є неминучим результатом безкарності попередніх зловживань. І якщо проводити аналогію із недобросовісними працівниками, які здійснюють фінансове шахрайство в діяльності суб'єктів підприємництва, то один непокараний суб'єкт

зловмисних дій – це одне “розбите вікно”, що може стати основою для появи нових тіньових схем і фінансових зловживань у діяльності суб’єктів підприємництва.

Підсумовуючи, вважаємо, що ефективна протидія фінансовому шахрайству працівників у діяльності ділових одиниць повинна ґрунтуватися на системі як запобігання, так і покарання таких злочинів.

3.2. Рейдерство як конфліктна форма перерозподілу власності в Україні

Одним із поширених способів забезпечення економічного розвитку суб’єктів підприємництва, розширення діяльності й сфер впливу на ринку є процеси злиття і поглинання. Стратегії злиття і поглинання ґрунтуються на рівноправному, за взаємною згодою сторін, злитті й поглинанні ділових одиниць, чим забезпечуються значні конкурентні переваги. Водночас консолідація бізнесу в Україні відбувається всупереч світовим закономірностям розвитку процесів злиття та поглинання і має свої характерні риси:

- недостатній рівень захисту прав власності та прав інвесторів, унаслідок чого виникає значний ризик втрати вкладень;
- вплив політичної складової на функціонування бізнесу в країні;
- низький рівень правової культури;
- наявність корупційної складової в схемах перерозподілу бізнесу;

У світовій практиці для аналізу рівня захисту прав власності використовують міжнародний індекс захисту прав власності (The International Property Right Index (IPRI)), уведений 2007 р. Міжнародним Альянсом прав власності. Він враховує такі основні складові:

- правове та політичне середовище (Legal and Political Environment (LP)): незалежність судової системи та неупередженість судів, верховенство закону, політична стабільність, рівень корупції;
- забезпечення прав на фізичну власність (Physical Property Rights (PPR)): захист фізичних прав власності, реєстрація власності, доступність позик;
- забезпечення прав на інтелектуальну власність (Intellectual Property Rights (IPR)): захист інтелектуальних прав власності, патентний захист, рівень “піратства”.

Дослідження динаміки позиції України в міжнародному рейтингу захисту прав власності впродовж 2010–2022 рр. засвідчило досить низькі значення цих показників (див. табл. 3.1., рис. 3.20).

Таблиця 3.1

Динаміка позицій України в міжнародному рейтингу захисту прав власності впродовж 2010–2022 рр.

Роки	Показники				
	Загальний бал IPRI	Глобальний ранг	Регіональний ранг	Субіндекс захисту прав фізичної власності (Physical Property Rights Subindex)	Субіндекс захисту прав інтелектуальної власності (Intellectual Property Rights Subindex)
2010	4,149	93/129	17/129	4,798	3,928
2011	4,000	113/129	24/25	4,400	4,200
2012	4,000	115/129	25/25	4,400	4,200
2013	4,200	108/129	23/25	4,800	4,300
2014	4,300	84/129	11/25	5,333	5,650
2015	3,926	105/129	21/25	4,871	4,070
2016	3,933	113/129	24/25	5,051	4,320
2017	3,424	123/129	24/25	3,378	4,419
2018	4,282	92/129	15/25	5,726	4,436
2019	4,432	109/129	23/25	5,747	4,578
2020	4,466	105/129	22/25	5,772	4,563
2021	4,453	106/129	25/25	5,800	4,400
2022	3,980	105/129	25/25	4,220	4,390

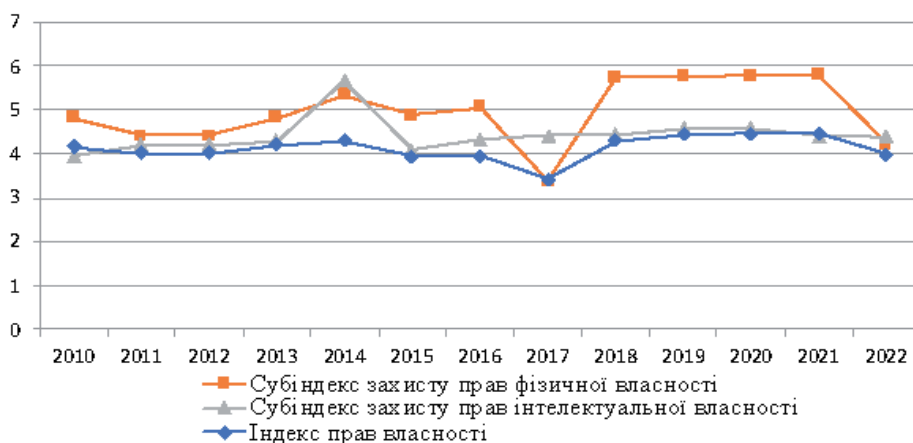


Рис. 3.20. Динаміка позицій України в міжнародному рейтингу захисту прав власності впродовж 2010–2022 рр.

Джерело: побудувала автор на основі [94]

З табл. 3.1 та рис. 3.20 видно, що упродовж 2010–2022 рр. Україна в міжнародному рейтингу захисту прав власності, попри незначні покращення окремих субіндексів у певні роки, в цілому посідає незадовільні позиції. У 2020 р. оцінка міжнародного індексу захисту прав власності дещо зросла порівняно з 2019 р. до значення 4,466, що становило 22-ге місце в регіоні Центрально-Східної Європи та Центральної Азії та 105-те у світі. Субіндекс прав фізичної власності в Україні збільшився на 0,025 до 5,772, а субіндекс прав інтелектуальної власності зменшився на 0,015 до 4,563. Однак у 2021 р. значення IPRI знизилося до 4,453, та становило у 2022 р. – 3,980 [94].

Виявлені негативні тенденції пов'язані передусім із багатолітніми складними стагнаційними процесами у правовому середовищі, що, попри окремі позитивні зрушення внаслідок змін до законодавства у сфері захисту прав власності в Україні, не можуть радикально швидко змінити ситуацію.

Зокрема, О. Островська, Ю. Гавриленко [178, с. 288] пропонують залежно від отриманого значення показника IPRI проводити оцінювання рівня ризику настання недружного поглинання шляхом присвоєння країнам відповідного класу (табл. 3.2). Згідно з цим підходом, Україна належить до класу 2 (високий рівень) за рівнем ризику недружного поглинання.

Таблиця 3.2

**Шкала оцінки рівня ризику
недружного поглинання на макрорівні [178, с. 288]**

Значення індексу	Клас	Рівень ризику недружного поглинання
0–2,5	Клас 1	Катастрофічний
2,6–5	Клас 2	Високий
5,1–7,5	Клас 3	Нижчий середнього
7,6–10	Клас 4	Низький

Неналежний рівень захисту прав власності в Україні зумовив виникнення та поширення рейдерства, за якого контроль над активами суб'єктів підприємництва реалізують з порушенням інтересів власників.

Ми виявили різноманіття наукових підходів до тлумачення сутності поняття “рейдерство”, зокрема такі:

– рейдерство (англ. reider) – набіг, раптовий напад. Рейдером в англословних країнах називали особу, яка входила до невеликого мобільного озброєного угруповання, що пересувається, вчиняючи напади, а також морських піратів [284, с. 147];

– рейдерство – це процес захоплення власності фірми або перехоплення оперативного управління за допомогою спеціально створеного та розіграного бізнес-конфлікту. Рейдерська діяльність – це передусім складна й командна робота висококваліфікованих спеціалістів – юристів, економістів, аналітиків, бухгалтерів, аудиторів, силовиків, спрямована в відповідне русло організатором, що має адміністративний і фінансовий ресурс [96, с. 19];

– рейдерство – процес захоплення фірми у власність проти волі її власників/власника, що виконують реалізацію різних протиправних дій з боку захоплювача з метою швидкого перепродажу об’єкта рейдерського нападу чи подальшого управління ним [14];

– рейдерство – поглинання та (або) захоплення майна установ, підприємств, організацій, які здійснюються як незаконними, так і законними методами, всупереч інтересам їх власника [56, с. 26];

– рейдерство – діяльність, мета якої – поглинання іншої компанії за допомогою псевдологічних методів і технологій, що створюють враження уявної законності дій [67, с. 5];

– рейдерство – процес, який складається із законних, напівзаконних та незаконних дій осіб, що спрямовані на захоплення або поглинання суб’єктів господарювання будь-якої форми власності та їхнього майна з метою встановлення повного контролю [264, с.103];

– рейдерство – цілеспрямована зміна права власності на акції та підприємницькі активи за допомогою неправосудних судових та адміністративних рішень і протиправної діяльності професійних учасників ринку цінних паперів, які обслуговують обіг та облік цінних паперів певного акціонерного товариства, та/або посадових осіб акціонерного товариства [4];

– рейдерство – напад на підприємство, установу, ділянку лісового фонду, жилий будинок, квартиру, інше майно незалежно від форм власності, вчинене за попередньою змовою групою осіб, поєднаним із

застосуванням фізичного чи психічного насильства або з погрозою застосування такого насильства, небезпечного для життя чи здоров'я особи, з використанням штучно створеного майнового конфлікту і підроблених або інших нелегітимних документів чи незаконних судових рішень для надання нападу вигляду законних дій, з метою протиправного заволодіння майном у великих розмірах або встановлення контролю над оперативним управлінням таким майном [55, с.79];

– рейдерство – систематична недружня діяльність на ринку корпоративного контролю, спрямована на несилове (або силове) отримання контролю над активами інших суб'єктів економічної діяльності всупереч їх волі, як законними, так і незаконними методами, із завданням їм економічних та інших видів збитків, що здійснюється з використанням недостатності правової бази, шляхом ініціювання бізнес-конфліктів та з корупційним використанням державних, адміністративних та силових ресурсів [115, с. 62];

– рейдерство – це вилучення майна на формально законних підставах, в основі виникнення яких є злочин, зловживання правом, прогалини в законі чи системні недоліки функціонування державних інститутів (судової та правоохоронної систем, системи реєстрації юридичних осіб тощо) [77];

– рейдерство – порушення законодавства, пов'язані з протиправним поглинанням та захопленням суб'єктів господарювання, позбавленням їх права власності, використанням судів з цією метою [275, с. 259];

– рейдерство – протиправні дії, спрямовані на придбання і встановлення контролю над активами юридичної особи чи підпорядкування й обмеження її діяльності всупереч волі власників під будь-якою загрозою, що негативно впливає на фінансову безпеку [63, с. 159];

– рейдерство – протиправне захоплення підприємства проти волі його власника (власників) різноманітними способами з метою подальшого розпорядження ним як у власних інтересах, так і в інтересах третіх осіб або його усунення з ринку господарювання [192, с. 57].

Окремі науковці ототожнюють рейдерство з корпоративним конфліктом. Однак дії рейдерів, хоча й пов'язані часто з ініціюванням корпоративного конфлікту, відбуваються з порушеннями цивільного та корпоративного законодавства. Корпоративний конфлікт у рейдерських схемах є лише формальним приводом для захоплення підприємства. Відтак, пропонуємо під рейдерством розуміти гібридний фінансовий

конфлікт щодо зміни контролю над фінансово-господарською діяльністю суб'єкта підприємництва та заволодіння його активами.

Рейдерство, як гібридний фінансовий конфлікт, характеризується складним характером його реалізації. Аналіз підходів вчених до вивчення цього явища [14; 17; 63; 67; 77; 143; 168] дав змогу виразити його зміст шляхом виокремлення та систематизації таких основних сутнісних характеристик (див. рис. 3.21).

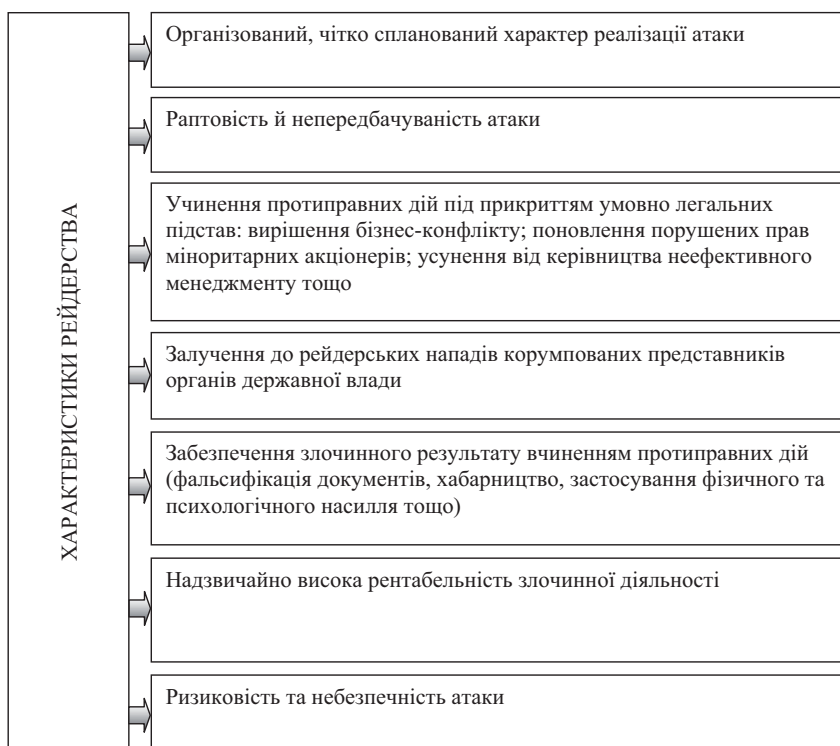


Рис. 3.21. Систематизація сутнісних характеристик рейдерства

Джерело: розробила автор

Основними об'єктами протиправного захоплення суб'єктів підприємництва є їхні активи. Зазвичай загроза агресивних дій рейдерів властива діловим одиницям, які здійснюють рентабельну діяльність, мають високий економічний потенціал, а також у їхній власності наявні високовартісні об'єкти нерухомості, привабливі земельні ділянки, обладнання та новітні технології.

До типових мотивів протиправного захоплення належать: заволодіння активами ділових одиниць; збільшення частки агресора на ринку й усунення конкурентів.

Від здобуття Україною Незалежності рейдери використовували різні способи протиправного заволодіння бізнесом, які можна умовно поділити на нелегальні – “чорне рейдерство”, умовно легальні (“біле рейдерство”) та їхнє поєднання (“сіре рейдерство”) (табл. 3.3):

Таблиця 3.3

Характеристика основних видів рейдерства в Україні

ВИД РЕЙДЕРСТВА	ХАРАКТЕРИСТИКА	ЗАСОБИ РЕАЛІЗАЦІЇ
“БІЛЕ РЕЙДЕРСТВО”	Використання прогалин вітчизняного законодавства та неточностей й упушень внутрішньої документації суб’єкта підприємництва	Маніпуляції з акціями та частками товариств, використання недоліків у законодавстві; придбання кредиторської заборгованості, перегляд результатів приватизації тощо
“ЧОРНЕ РЕЙДЕРСТВО”	Злочинна діяльність з привласнення чужого майна з використанням шахрайських схем, незаконних судових рішень за співучасті корумпованих працівників органів державної влади тощо	Ухвалення незаконних рішень щодо активів товариств шляхом корупційної взаємодії з державними органами; фальсифікація та знищення документів, викрадення печаток, підроблення підписів керівництва суб’єкта підприємництва; незаконне перехоплення управління, створення паралельних органів управління суб’єктом підприємництва; використання психологічного тиску та фізичного насильства над власниками й керівництвом суб’єкта підприємництва
“СІРЕ РЕЙДЕРСТВО”	Злочинна діяльність, у ході якої використовують сукупність заходів як “білого рейдерства”, так і “чорного рейдерства”	Часткова фальсифікація документів, скуповування акцій, шантаж, маніпулювання рішеннями зборів акціонерів, підкуп суддів, ініціювання справи про банкрутство тощо

Джерело: розробила автор

Одним із різновидів рейдерської діяльності є грінмейл. Це сукупність зловмисних дій окремих учасників суб’єкта підприємництва, спрямованих на дестабілізацію ситуації в ньому з метою примусу інших учасників чи

акціонерів придбати частки чи акції грінмейлера за ціною, вищою від ринкової. Виділяють такі ознаки грінмейл [148, с. 22]:

- є результатом активних або пасивних дій учасників чи акціонерів або їх об'єднаних груп;
- спрямоване на створення відповідного негативного для товариства та акціонерів результату у визначеній формі шляхом шантажу;
- має на меті отримання винагороди за утримання від дій або вчинення певних дій у майновій чи немайновій формі;
- є формою втручання третіх осіб у діяльність комерційної організації;
- ґрунтується на факті володіння грінмейлерами певної кількості часток чи акцій або можливості прямо чи опосередковано розпоряджатися наданою їм певною кількістю часток чи акцій за допомогою права голосу;
- спрямоване на створення для товариства певних негативних наслідків у фінансово-майновій сфері та отримання таких вигод і привілеїв, які не можна законно отримати за наявних умов господарського обігу;
- має формально законний характер, що передбачає певну послідовність дій формально-законного характеру, які є заздалегідь спланованим зловживанням певною особою або групою осіб правами власників.

Зокрема, І. Дмитрієв здійснює поділ рейдерів на рейдерів-замовників (фізична або юридична особа, що фінансує рейдерську атаку); рейдерів-найманців (особи, що працюють під керівництвом великих фірм, які надають їм усі необхідні ресурси для захоплення); незалежних рейдерів (працюють самостійно за власні ресурси, отримують прибуток від атаки). Відповідно до можливостей і технологій захоплення вчений виокремив рейдерів вищого, середнього та нижчого рівнів (див. рис. 3.22).

Відтак, визначено, що найвищою результативністю характеризуються рейдерські атаки, вчинені рейдерами вищого рівня, оскільки вони мають велику кількість інструментів для захоплення ділових одиниць, зокрема державний адміністративний ресурс.

Рейдери середнього рівня – це інвестиційні компанії та професійні компанії-рейдери. Їх відмінністю є те, що професійні рейдери працюють на замовлення інших компаній, а інвестиційні – захоплюють підприємства за власні кошти з метою отримання доходу від ефективно розміщених інвестицій.

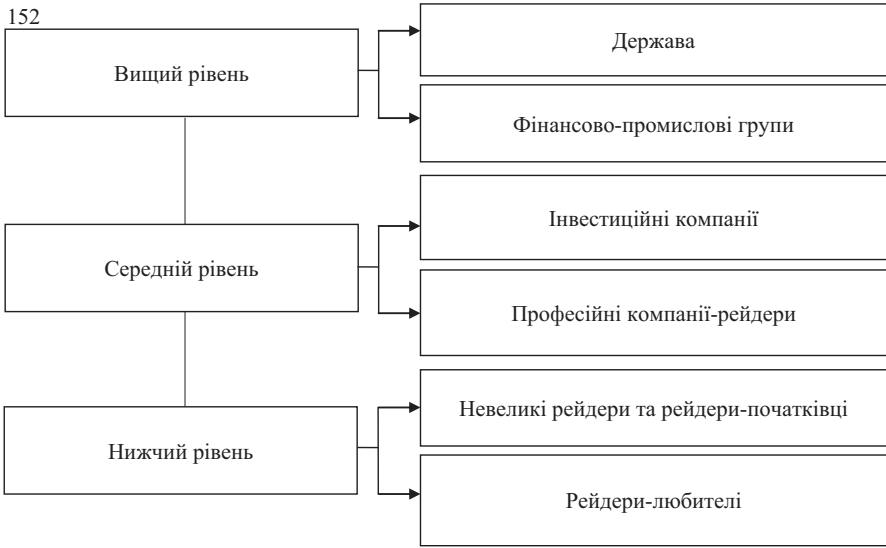


Рис. 3.22. Ієрархія рейдерів [67, с. 12]

Аналіз протиправного захоплення бізнесу в Україні впродовж 2015–2022 рр. засвідчив зростання кількості рейдерських атак, лише в останні роки спостерігається тенденція до скорочення випадків протиправних захоплень (див. рис. 3.23).

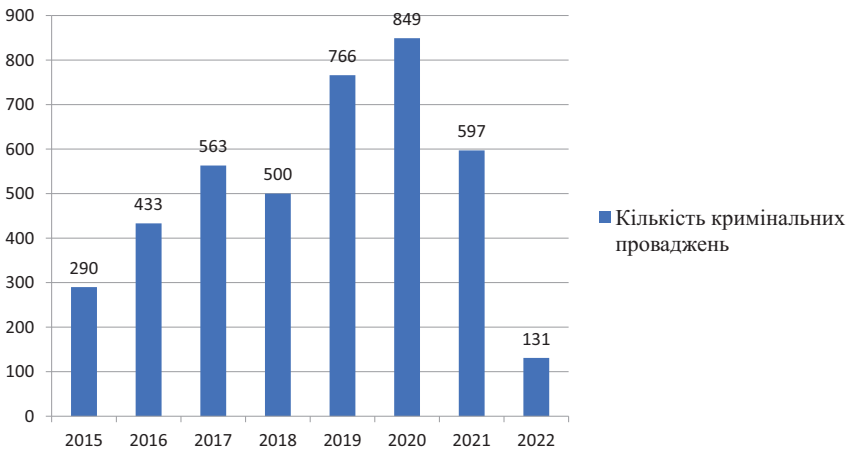


Рис. 3.23. Динаміка кримінальних проваджень за фактами рейдерства в Україні впродовж 2015–2022 рр. [270]

Як видно з рис. 3.23, в 2015 р. було відкрито 290 кримінальних проваджень за фактами рейдерства, в 2016 р. – 433, 2017 р. – 563, 2018 р. – 500, 2019 р. – 766, 2020 р.– 849, 2021 – 597. За 10 місяців 2022 р. кількість кримінальних проваджень про рейдерство зменшилась порівняно з відповідним періодом 2021 р. у більш ніж 5 разів – з 597 до 131.

Водночас до суду доходить лише 43 % зареєстрованих справ. Найчастіше розглядають справи про рейдерство, що стосуються таких злочинів, як підроблення документів, що подаються для державної реєстрації юридичної особи, протидія господарській діяльності та протиправне заволодіння майном (рис. 3.24).

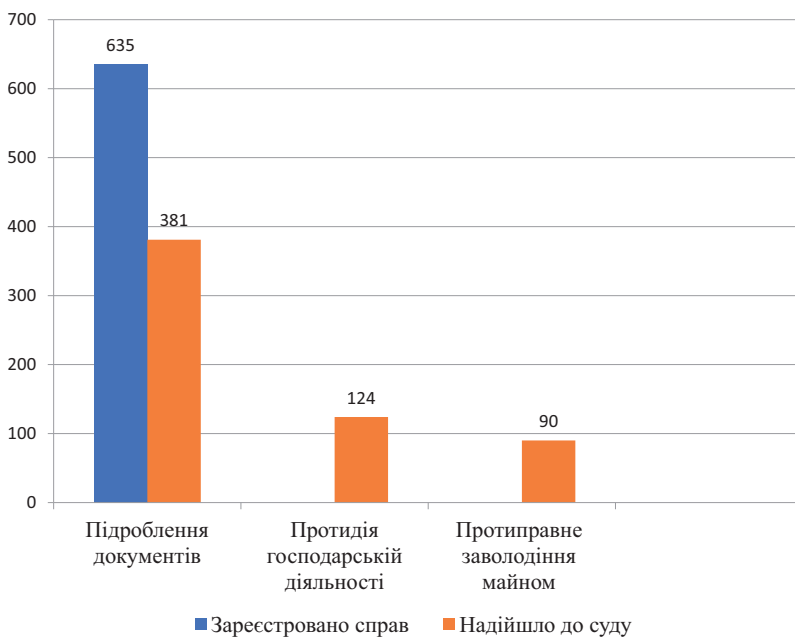


Рис. 3.24. Злочини, за якими найчастіше розглядають справи про рейдерство у 2021 р. [270]

Аналіз стану та динаміки незаконних захоплень у регіональному розрізі впродовж 2013–2019 рр. дав змогу зробити висновки, що найбільше рейдерство було поширено в Київській, Львівській, Дніпропетровській, Харківській та Херсонській областях (табл. 3.4).

**Динаміка протиправних захоплень впродовж 2013–2019 рр.
в регіонах із найбільшим показником рейдерства [278]**

Область	Роки						
	2013	2014	2015	2016	2017	2018	2019 (січень– травень)
Київська	35	55	128	186	260	237	115
Львівська	15	9	18	12	8	13	6
Дніпропетровська	20	14	7	18	53	40	15
Харківська	23	10	19	20	37	45	20
Херсонська	31	21	24	17	11	22	8

Серед суб'єктів підприємництва, що зазнали рейдерських атак від здобуття Україною Незалежності – ПАТ “Броварський завод будівельних конструкцій”, ПАТ “Агрофірма “Провесінь”, ПрАТ НВЦ “Борщатівський хіміко-фармацевтичний завод”, ПрАТ “Дарниця”, ПАТ “Фармак”, ПАТ “Миколаївський суднобудівний завод “Океан”, ПАТ “Електроприлад”, ПАТ “Дрогобицький машинобудівний завод”, ПАТ “Київенерго”, ПАТ “Львівобленерго”, ПАТ “Полтаваобленерго”, ПАТ “Чернігівобленерго”, ПАТ “Сумиобленерго”, ПАТ “ДТЕК “Дніпрообленерго”, ПАТ “Прикарпаттяобленерго” та інші (перелік досліджуваних підприємств, на які було здійснено рейдерські атаки, подано в додатку М).

Згідно з даними Спілки українських підприємців (СУП) профільному комітету бізнес-асоціації довелося відстоювати корпоративні права або права власності 15 компаній-членів бізнес-асоціації. За результатами дослідження “Портрет українського підприємця”, проведеного СУП у вересні 2020 року, 54 % власників бізнесу однією з основних проблем підприємницької діяльності в Україні називали незахищеність приватної власності та рейдерство [307].

Від здобуття Україною Незалежності було виявлено функціонування близько 50 рейдерських груп, зокрема згідно з даними експертного опитування Центру дослідження корпоративних відносин до найбільших рейдерських груп належали такі: “Приват” (100 % голосів експертів), “Фінанси і Кредит” (54,6 %), “Альфа-Груп” (45,5 %), СКМ (36,4 %), ІСД (27,3 %), “ТАСС” (18,6 %),

“Інтерпайп” (18,2 %). За даними Антирейдерського союзу підприємців, середньорічна кількість протиправних захоплень сягала 3 000 з результативністю атак 80–90 %, що за експертною оцінкою становила понад 3 млрд дол. [17].

Однією із першопричин поширення рейдерства в Україні була непрозорість і складність приватизаційних процесів. За підсумками реформ державного сектора економіки від здобуття Україною Незалежності 50,2 % об’єктів державної форми власності було приватизовано значним подрібненням цілісних майнових комплексів; понад 70 % приватизованих підприємств набули нового власника з використанням позаконкурсних процедур. Окрім того, зберігалася висока частка юридичних осіб, які мали формальний статус підприємств державної форми власності, що не позбулися цього статусу за умов фактичної зміни права власності. Подрібнення майнових комплексів, певна сумнівність зміни власника та наявність невирішених питань належності власності спричинила загострення конфлікту інтересів серед нових власників між собою та державою [13].

Окрім того, масштаби рейдерства і темпи його поширення визначають такими основними чинниками:

- правовий механізм захисту прав власників;
- якість законодавчої бази, що регламентує різні аспекти фінансової діяльності суб’єктами господарювання;
- ефективність роботи державних інститутів щодо захисту прав власників;
- рівень розвитку ринку корпоративного контролю;
- рівень конфліктогенності здійснення фінансово-господарської діяльності;
- рівень “прозорості” грошових потоків суб’єктів підприємництва;
- дієвість судової системи в Україні;
- відокремленість бізнесу від політики;
- рівень корупції органів державної влади;
- рівень правової культури;
- прозорість процесів приватизації.
- якість функціонування правоохоронної та судової систем;
- характер політичної ситуації в країні;
- правова відповідальність за рейдерські злочини;

Щодо правової відповідальності, то окремо необхідно звернути увагу, що визначення терміну “рейдерство” не закріплено на законодавчому рівні і не визначено у Кримінальному кодексі України як окреме кримінально-каране діяння. Розслідування рейдерства провадиться за ознаками злочинів, передбачених іншими статтями Кримінального кодексу, зокрема такими групами злочинів [132]:

1. Злочини, спрямовані на порушення прав законних власників і захоплення підприємств застосуванням насильства: завдання тілесних ушкоджень різного ступеня тяжкості (ст. 121–123); умисне знищення або пошкодження майна (ст. 194); протидія законній господарській діяльності (ст. 206); протиправне заволодіння майном підприємства, установи, організації (ст. 206-2); групове порушення громадського порядку (ст. 293); хуліганство (ст. 296); захоплення державних або громадських будівель чи споруд (ст. 341); примушування до виконання чи невиконання цивільно-правових зобов’язань (ст. 355); самоправство (ст. 356). Аналізуючи кримінальні справи, порушені за супутніми рейдерству злочинами, виявлено такі [153]:

– злісне хуліганство та нанесення умисного середньої тяжкості тілесного ушкодження на території заводу ЗБК-135 на вул. Бориспільській, 19 у Києві (ч. 1 ст. 122, ч. 4 ст. 296 КК України);

– хуліганство та заподіяння тілесних ушкоджень під час захоплення санаторію у м. Алупка, що призвело до тимчасового припинення нормальної роботи лікувальної установи (ч. 4 ст. 296, ч. 2 ст. 121 КК України);

– захоплення території та приміщень ВАТ “Кременчуцький сталеливарний завод” (ч. 2 ст. 194, ст. 293 КК України);

– вчинення насильницьких дій під час захоплення будівельного майданчика торговельного центру ТОВ “Таміра” (ч. 1 ст. 122, ч. 3 ст. 189, ч. 3 ст. 296 КК України);

– замах на захоплення групою невстановлених осіб у кількості близько 50 осіб адміністративного приміщення ВАТ “Черкасигаз”, що призвело до порушення нормальної роботи підприємства (ст. 341 КК України);

– примус генерального директора ТОВ “С” до виконання цивільно-правових зобов’язань щодо управління майном підприємства (ч. 2 ст. 355 КК України);

– захоплення групою невстановлених осіб орендованих ТОВ “Медінжсервіс” нежитлових приміщень (ст. 206 КК України).

2. Злочини, що спрямовані на порушення прав законних власників і захоплення підприємств обманом: шахрайство (ст. 190 КК України); викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шахрайством чи зловживанням службовим становищем або їхнє пошкодження (ст. 357); підроблення документів, печаток, штампів та бланків, їхній збут, використання підроблених документів (ст. 358); незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359); несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361). Серед кримінальних справ за цими злочинами можемо навести такі:

- укладання угоди про передачу ТОВ “Фортуна банк” об'єктів нерухомого майна ВАТ “Дніпрофарм” у м. Дніпро (ч. 4 ст. 190 КК України);

- незаконне відчуження будівлі готельного комплексу “Русь” унаслідок незаконного його продажу директором ТОВ “С”, який володів документами готельного комплексу (ч. 4 ст. 190 КК України).

Ці приклади є вагомим підтвердженням гібридної природи рейдерства та тісного взаємозв'язку усіх гібридних фінансових конфліктів. Шахрайство в цьому випадку є складовою рейдерського захоплення, що полягає в розкраданні майна суб'єктів господарської діяльності або набуття права на це майно шляхом:

- обману (навмисного повідомлення свідомо неправдивої інформації з метою одержання матеріальної або іншої особистої вигоди), що може полягати як в активних діях (підроблення документів), так і бездіяльності (приховування інформації, що має суттєве значення);

- зловживання довірою (використання з корисливою метою, у супереч майновим інтересам потерпілого, довірливого ставлення потерпілого до злочинця, яке у більшості випадків учинення шахрайства поєднується з обманом);

- заволодіння майном унаслідок зловживання службовим становищем трапляється в разі, коли його суб'єктом є службова особа, яка, відповідно до обійманої посади, правомочна управляти чи розпоряджатися майном (має владні повноваження щодо впливу на осіб, яким це майно ввірене), а

відповідні дії кваліфікують за сукупністю злочинів, передбачених ст. 190 і 364 КК України;

– отримання матеріальної вигоди за кошти власника або законного володаря майна внаслідок обману або зловживання довірою без ознак шахрайства (передача майна в економічно недоцільну (неефективну) оренду; списання коштів та майна підприємства на придбання цінних паперів, що не мають реальної ринкової вартості, та інші дії з метою доведення підприємства до банкрутства).

3. Злочини, пов'язані з протиправною діяльністю службових осіб, що дають змогу правоохоронним органам притягати винних до відповідальності за дії, пов'язані з рейдерством на кожному з його етапів:

1. Збір інформації: ст. 162 “Порушення недоторканності житла”; ст. 163 “Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер”; ст. 182 Порушення недоторканності приватного життя”; ст. 231 “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю”; ст. 232. “Розголошення комерційної або банківської таємниці”; ст. 232-1 “Розголошення або використання неоприлюдненої інформації про емітента або його цінні папери”; ст. 359 “Незаконне використання спеціальних технічних засобів негласного отримання інформації”; ст. 361-2 “Несанкціоновані збут або розповсюдження інформації з обмеженим доступом” та ін.

2. Початок рейдерського захоплення: ст. 366 “Службове підроблення”; ст. 358 “Підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів”; ст. 353 “Самовільне присвоєння владних повноважень або звання службової особи”; ст. 205 “Фіктивне підприємництво”.

3. Заміна керівництва, примушування до продажу акцій: ст. 129 “Погроза вбивством”; ст. 195 “Погроза знищення майна”; ст. 146 “Незаконне позбавлення волі або викрадення людини”; ст. 189 “Вимагання”.

4. Неправомірні дії щодо активів: ст. 364 “Зловживання владою або службовим становищем”; ст. 365 “Перевищення влади або службових повноважень”; ст. 343 “Втручання в діяльність працівника

правоохоронного органу”; ст. 376 “Втручання в діяльність судових органів”; ст. 219 “Доведення до банкрутства”.

5. Підкуп службовців державних органів, що належить до кримінально-караних діянь, передбачених ст. 368 КК України “Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою” та ст. 369 “Пропозиція, обіцянка або надання неправомірної вигоди службовій особі”.

Відтак, дослідження сукупності злочинів, які пов’язані з протиправною діяльністю державних службовців, що використовуються в протиправних захопленнях підприємств, засвідчують взаємозв’язок таких гібридних фінансових конфліктів як рейдерство та корупція.

Зокрема, С. Титаренко [285, с. 71] виділяє спільні ознаки злочинів, які полягають у протиправному захопленні суб’єктів підприємництва:

- злочини вчинюються в управлінській і майновій сферах та безпосередньо посягають на сукупність правовідносин, пов’язаних із забезпеченням державного захисту суб’єктів господарювання від рейдерства та інших форм протиправного втручання в процес їх нормальної діяльності;

- діяння полягають у захопленні управлінського контролю над суб’єктами господарювання та належними їм активами застосуванням насильства, обману або поєднання цих двох способів протиправної поведінки;

- злочини вчиняються у формі співучасті з розподілом ролей або професійними організованими групами чи злочинними організаціями;

- злочини посягають на правовідносини приватної власності, які виступають додатковим об’єктом рейдерських посягань;

- ці діяння вчинюються переважно з прямим умислом, корисливою мотивацією та чіткими цільовими установками.

Проаналізувавши першопричини виникнення рейдерства, пов’язані зі складністю й непрозорістю процесів приватизації та сукупність чинників, які вплинули на подальше поширення цього деструктивного явища в Україні, можемо констатувати, що проблема захисту прав власності залежить значною мірою від якості її правового вирішення та соціально-економічної й політичної ситуації в країні. Водночас в умовах військової агресії в Україні ця проблематика набула абсолютно нового змісту, актуалізуючи потребу першочергового фізичного захисту об’єктів власності.

Розвиток рейдерства в Україні має значні негативні наслідки макроекономічного, політичного та соціального характеру (рис. 3.25).

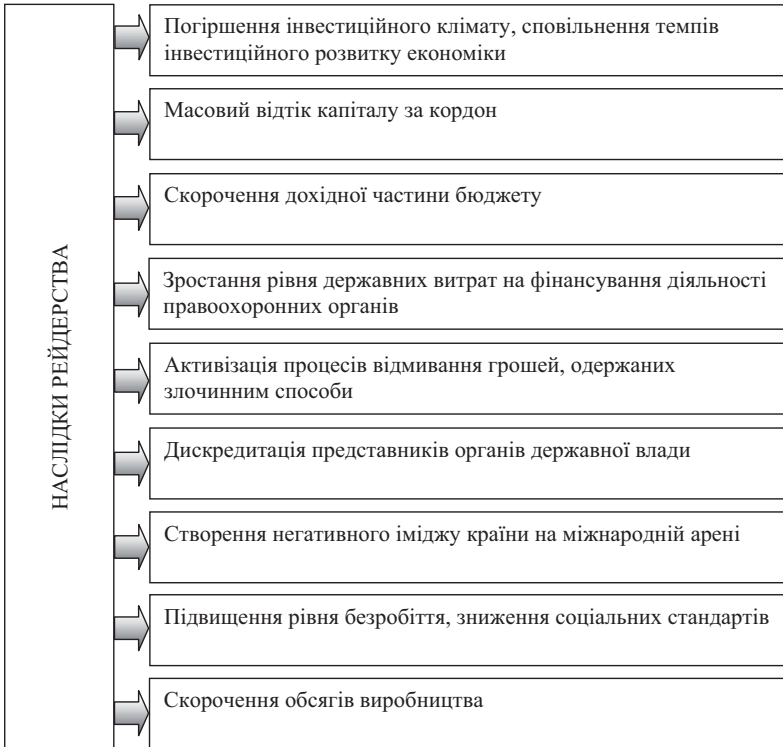


Рис. 3.25. Наслідки рейдерства в Україні

Джерело: розробила автор

Це суспільно небезпечне явище негативно впливає не лише на фінансову безпеку окремих ділових одиниць, а й на фінансову безпеку держави загалом. Його загроза для фінансових інтересів країни виявляється в негативному впливі на її міжнародний імідж, інвестиційну привабливість національних підприємств. Адже рівень і темпи іноземного інвестування залежать, передусім, від внутрішньої політичної стабільності в країні, тенденцій ринкових реформ, раціональності законодавства й гарантій недоторканості приватної власності.

Для повноти розуміння рейдерства як гібридного фінансового конфлікту необхідно розкрити особливості його вчинення. Відтак,

доцільно зазначити, що протиправне захоплення суб'єктів підприємництва передбачає сукупність скоординованих дій працівників різних напрямів, до основних із яких можуть належати такі:

- юридичний відділ, до якого входять кваліфіковані фахівці в галузі права, що використовують недосконалість чинних нормативно-правових норм, їхні неточності та прогалини в корисних цілях рейдерів, розробляючи пакети документів, у тому числі підроблені, для порушення кримінальних, господарських справ, ініціювання перевірок;

- аналітичний відділ, що відповідає за збір й аналізування інформації про суб'єкт підприємництва – об'єкт агресивних дій;

- відділ стратегічного аналізу, який розробляє стратегію рейдерського захоплення ділової одиниці;

- PR-агентства, функціями яких є поширення дезінформації про захоплюваний суб'єкт підприємництва з метою створення негативного іміджу в суспільстві;

- силові структури у формі різних приватних охоронних агенцій, функціонал яких використовується у випадках “чорного рейдерства”, зокрема фізичного захоплення об'єктів власності.

Розглядаючи напрями роботи, за якими, зазвичай, відбувається рейдерська атака, доцільним, на нашу думку, є проведення аналогії з реалізацією стратегії міждержавного гібридного конфлікту. Відтак, можемо акцентувати, що росія цілеспрямовано й послідовно реалізовувала сукупність заходів на кожному із таких етапів стратегії гібридної війни:

- підготовчий етап – дослідження чинників, на основі яких було зроблено вибір стратегії гібридної агресії (політичні, економічні, соціальні, інформаційні, військові та інші ресурси, наявні для використання у гібридній війні в країні-агресора та у держави-об'єкта агресивних дій; прогнозоване співвідношення між результативністю досягнення визначеної мети та негативними наслідками в зовнішньополітичній і економічній сферах, які може отримати держава-агресор унаслідок реалізації своїх агресивних намірів,) й формування ідеологічних, політичних та військових передумов майбутньої агресії;

- етап “м'якого примусу” – опосередкований вплив держави-агресора, що здійснювався шляхом використання своїх геополітичних, економічних та інших переваг над країною-об'єктом агресії з метою змусити її політичне керівництво діяти на вигідних для себе умовах;

- етап поєднання в єдиному комплексі фінансово-економічних та інших засобів боротьби зі застосуванням збройних сил;
- етап повномасштабного військового вторгнення.

Порівнюючи рейдерські атаки суб'єктів підприємництва й російську гібридну війну, можемо констатувати, що за своєю сутністю й сукупністю етапів та заходів, що реалізуються, ці конфлікти є схожими. Візуальну інтерпретацію основних етапів рейдерського захоплення подано на рис. 3.26.

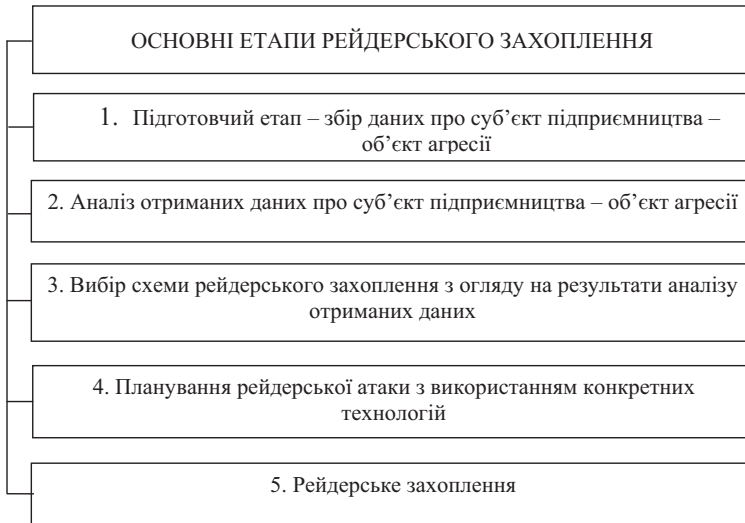


Рис. 3.26. Структурно-логічна схема реалізації рейдерського захоплення суб'єкта підприємництва

Джерело: розробила автор

На підготовчому етапі рейдерської атаки відбувається збір інформації про всі складові функціонування суб'єкта підприємництва-об'єкт агресії, зокрема дані фінансової та податкової звітності, матеріали управлінського обліку, статутних документів, відомостей з реєстру акціонерів, протоколів ради директорів, трудових договорів; дані про особливості управління, фінансову політику, активи та зобов'язання, керівництво підприємницької структури.

Важливо наголосити, що під час збирання такої інформації значну увагу приділяють даним, що компрометують керівництво суб'єкта підприємництва, а також всім аспектам функціонування, що роблять його вразливим до дій зловмисників. Рейдери оцінюють систему охорони ділової одиниці, аналізують її здатність протидіяти можливому захопленню, зокрема, досліджують

можливість залучення для свого захисту судових органів і прокуратури, органів державної влади.

Усі чинники, які аналізує рейдер перед захопленням суб'єкта підприємництва, умовно пропонуємо розділити на загальні умови функціонування, сильні та слабкі сторони суб'єкта підприємництва (рис. 3.27).

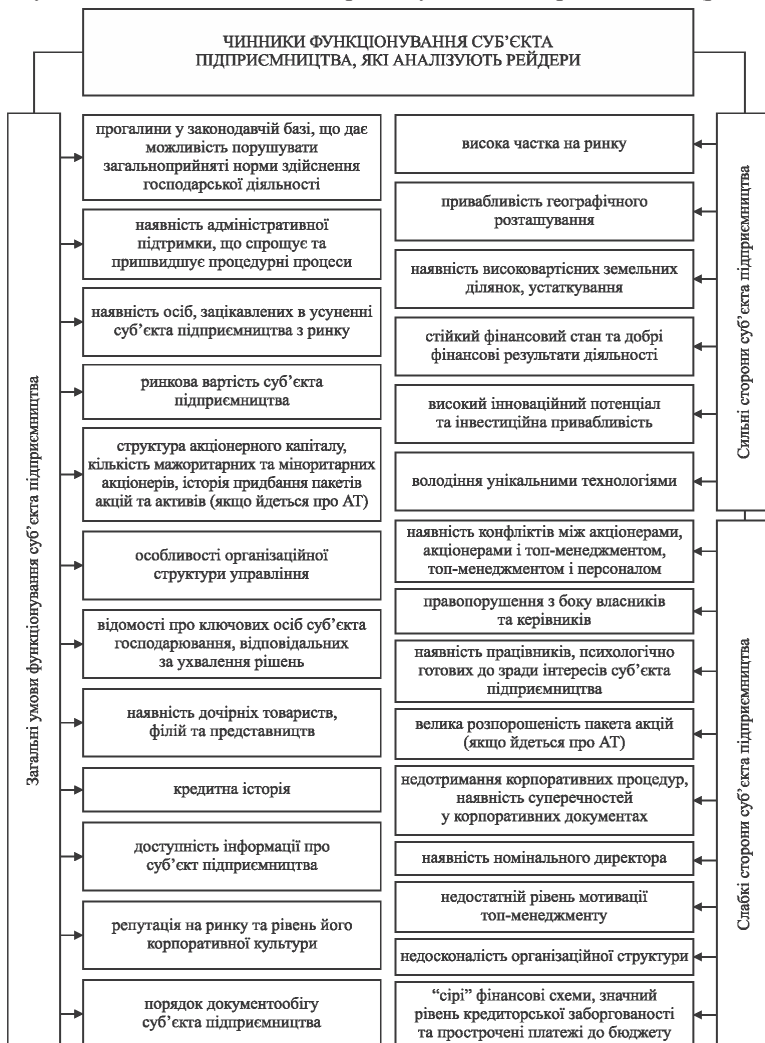


Рис. 3.27. Чинники функціонування суб'єкта підприємництва, які аналізують рейдери

Джерело: розробила автор

Інформацію про суб'єкт підприємництва можна отримати із зовнішніх та внутрішніх джерел. Із внутрішнього середовища ділової одиниці дані, важливі для рейдера, отримують, зазвичай унаслідок несанкціонованого проникнення в її комп'ютерну мережу, сервери, системи зберігання баз інформації; прослуховування розмов, отримання конфіденційної інформації за допомогою підкупу або шантажу працівників, а також зумисно впроваджених агентів в організаційну структуру підприємства.

Інформацію із зовнішнього середовища суб'єкта підприємництва рейдери можуть отримати як з легальних, так і з нелегальних джерел, що подано на рис. 3.28.



Рис. 3.28. Зовнішні джерела інформованості рейдера про суб'єкт підприємництва

Джерело: розробила автор

Насамперед відбувається пошук відкритої інформації, до якої є вільний доступ, здійснюючи моніторинг довідників, повідомлень ЗМІ, аналізуючи матеріали презентацій, виставок і конференцій. Також рейдери можуть одержувати конфіденційні дані, застосовуючи корупційні зв'язки з органами державної влади, зокрема, ініціюючи різні перевірки.

Інформацію про суб'єкт підприємництва часто отримують через благодійні організації, а також постачальників і споживачів підприємства. Інколи рейдери з метою отримання конфіденційних даних захопленого підприємства вдаються до проведення фальшивих конкурсів, ведуть фіктивні перемовини про купівлю його продукції тощо.

Наступний етап рейдерської атаки передбачає ретельний аналіз зібраної інформації на предмет вивчення ринкової позиції суб'єкта підприємництва, оцінки його фінансового стану, ринкової вартості, інвестиційної привабливості тощо. Важливу роль в аналізі функціонування ділових одиниць відводять прогалинам та недолікам в організації фінансового менеджменту захопленого підприємства. Ці вразливості враховуються рейдерами в цілях подальшого тиску на власників та керівництво.

На підставі отриманих результатів аналізу вибирають схему рейдерського захоплення з плануванням конкретних технологій, які використовуватимуть.

Від здобуття Україною Незалежності й до сьогодні рейдерство постійно видозмінювалося та характеризувалося наявністю різних схем протиправного захоплення. Зокрема, на певному етапі розвитку суспільства та наявного законодавчого захисту інтересів власників існували такі схеми рейдерських атак в Україні:

- рейдерство через акціонерний капітал;
- рейдерство через кредиторську заборгованість;
- рейдерство через вплив на керівництво підприємства;
- позбавлення власності внаслідок оскарження результатів приватизації.

Рейдерське захоплення суб'єкта підприємництва через акціонерний капітал здебільшого відбувається за наявності розпорошеного акціонерного капіталу та реалізується за такою схемою (рис. 3.29).



Рис. 3.29. Схема рейдерського захоплення через акціонерний капітал

Джерело: розробила автор

Структурно-логічну схему рейдерського захоплення суб'єктів підприємництва шляхом впливу на його керівництво подано на рис. 3.30.

Наділений значними повноваженнями найманий директор може сприяти швидкому виведенню майна з підприємства на підконтрольні рейдеру структури або ж шляхом ухвалення нераціональних рішень зумисно доводити його до критичного стану. Аналізуючи дані про склад керівництва та його особливості, рейдер здійснює вибір важелів впливу на нього, серед яких поширеними є підкуп, шантаж та інші форми психологічного тиску, сфабриковане кримінальне переслідування тощо.

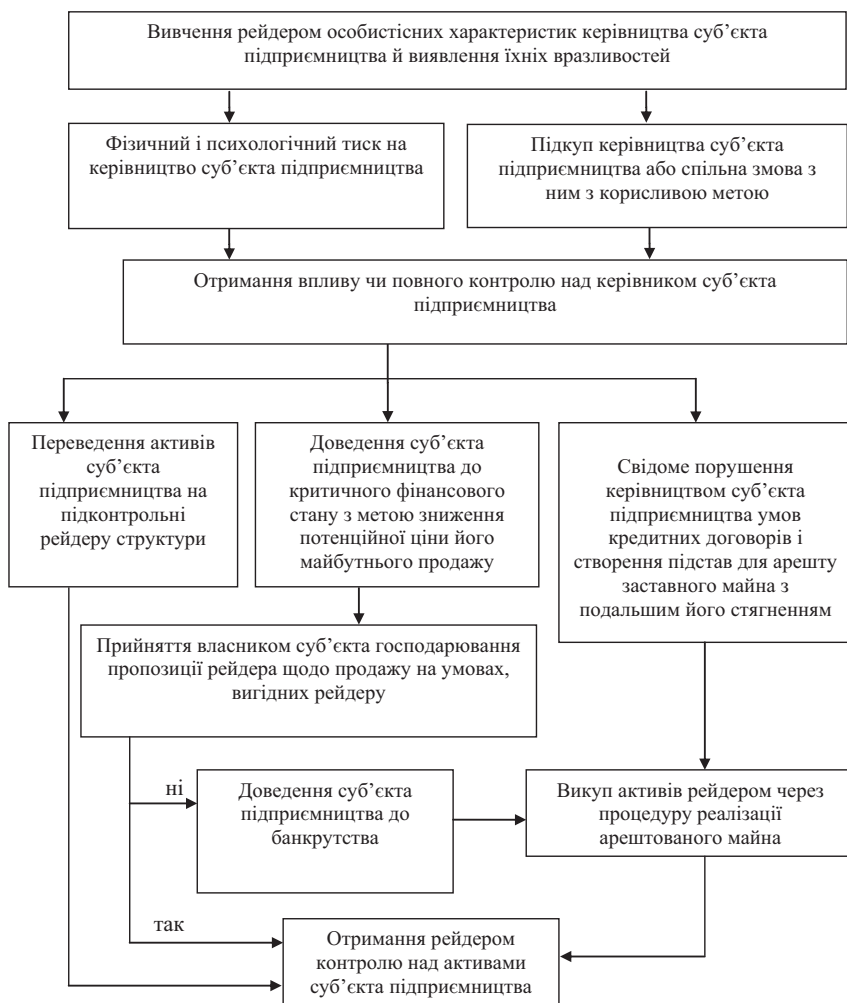


Рис. 3.30. Структурно-логічна схема рейдерського захоплення суб'єкта підприємництва шляхом впливу на його керівництво

Джерело: розробила автор

Рейдерська схема із використанням критичного рівня кредиторської заборгованості захоплюваного підприємства передбачає викуп рейдером зобов'язань суб'єкта підприємництва та пред'явлення їх до одноразової оплати. Візуальну інтерпретацію цієї схеми подано на рис. 3.31.



Рис. 3.31. Структурно-логічна схема рейдерського захоплення суб'єкта підприємництва через кредиторську заборгованість

Джерело: розробила автор

Під час рейдерського захоплення найчастіше використовують технології взаємодії з власниками, представниками державних органів влади, ЗМІ, приватними охоронними структурами (рис. 3.32). Технології взаємодії з власниками передбачають різноманітні перемовини, що часто відбуваються з елементами психологічного тиску, зокрема, залякування, шантажу тощо. Окрім того, рейдери активно застосовують технології взаємодії з державними органами. Як зазначає О. Литвак з позиції кримінолога й цивіліста, жодна рейдерська атака не закінчиться успішно, якщо вона не супроводжується прикриттям з боку державних структур, правоохоронців і суду [143, с. 40]. В цьому контексті, погоджуємось із думкою В. Молодик, що якщо це не відстежує місцева влада, то це

свідчить або про забезпечення цими органами такого захоплення, або про їхню економічну некомпетентність, професійну непридатність [160, с. 67].

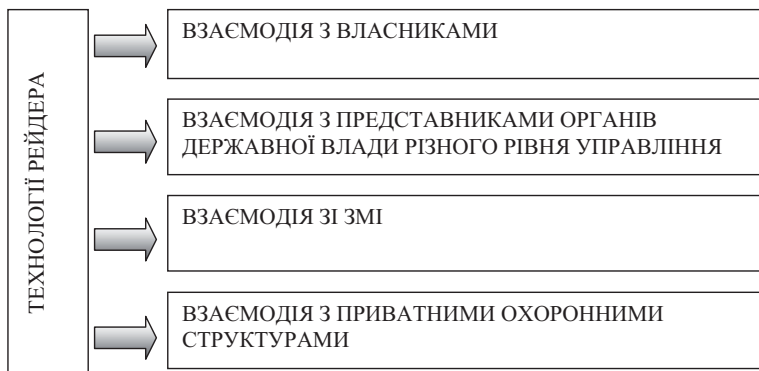


Рис. 3.32. Технології рейдерських атак

Джерело: розробила автор

Основними цілями адміністративного тиску на товариство є створення умов, за яких:

- неможливе швидке виведення активів (накладення арешту на активи підприємства, а також заборона укладати господарські договори щодо відчуження чи обтяження активів тощо);
- ускладнено фінансово-господарську діяльність підприємства та створено передумови його фінансового виснаження (збільшення кількості перевірок діяльності різними відомствами, створення перешкод в отриманні дозвільних документів, анулювання ліцензій, затримка в розмитненні придбаних за кордоном обладнання та товарів, відмова в проведенні державної реєстрації тощо);
- унеможливлено для ключових акціонерів перерозподілити акції з метою захисту (порушенням щодо таких акціонерів кримінальних справ тощо).

Серед напрямів адміністративного тиску на суб'єкти підприємництва з ціллю рейдерства, зокрема, акціонерної форми власності, виділяють такі [44, с. 27–28]:

- кримінально-правовий – ініціювання “замовних” кримінальних справ, у межах яких можуть накладати арешти на майно та застосовувати

запобіжні заходи до окремих осіб – посадових осіб та ключових акціонерів товариства для психологічного тиску на них;

- податковий – організація податкових перевірок щодо товариства та його контрагентів з метою відволікання уваги від рейдерських дій;

- поліцейський – проведення низки перевірок стосовно осіб та товариства – тактика перевірки може бути різною залежно від виду діяльності;

- прокурорський – забезпечення протидії слідству у кримінальних справах проти рейдерів (перевірка, об'єднання та переміщення кримінальних справ з метою їх закриття або припинення провадження);

- контрольний – організація перевірок правил ведення товариством господарської діяльності, дотримання законодавства про охорону праці тощо;

- ліцензійний – організація документальних перевірок та перевірок дотримання умов ліцензування охоронних, юридичних та аудиторських підприємств, які в межах своїх функцій повинні гарантувати безпеку товариства (з метою їхньої нейтралізації);

- міжнародний – ужиття заходів щодо спрямування майнових суперечок за межі юрисдикції України;

- господарсько-процесуальний – ініціювання низки господарських позовів у різних регіонах з певним періодом їхнього подання з метою не виграшу в суді, а створення безперервного потоку судових засідань (як забезпечення рішень, унаслідок ухвалення яких можуть накладати заборону на відчуження майна).

Адміністративний тиск на суб'єкт підприємництва зазвичай реалізується шляхом корупційної взаємодії з правоохоронними органами, візуальну інтерпретацію якої подано на рис. 3.33.

Технології взаємодії зі ЗМІ передбачають формування вигідної для рейдерів громадської думки у вигляді об'єктивного обґрунтування зміни керівництва суб'єкта підприємництва з метою його подальшого захоплення. Відтак, медійні заходи здебільшого спрямовані на компрометування керівництва підприємства для позбавлення його підтримки акціонерів. PR-технологи рейдера розробляють матеріали, що дискредитують менеджмент ділової одиниці та одночасно характеризують вигоди від зміни власника, зокрема, у ЗМІ можуть поширювати неправдиву інформацію про незадовільний фінансовий стан суб'єкта

підприємництва, невиконання ним зобов'язань перед контрагентами, анулювання ліцензій тощо.

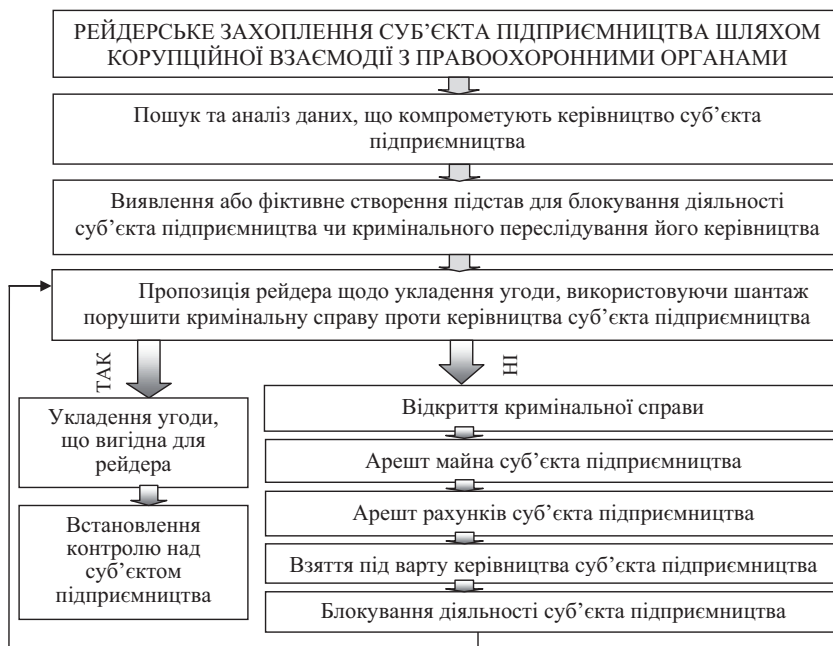


Рис. 3.33. Структурно-логічна схема рейдерського захоплення суб'єкта підприємництва з використанням корупційної взаємодії з правоохоронними органами

Джерело: розробила автор

Упродовж 1991–2000 рр. було поширеним відверто кримінальне рейдерство, часто із застосуванням фізичного насильства, відтак рейдери в процесі захоплення суб'єкта підприємництва часто застосовували технології взаємодії зі силовими структурами при вчиненні низки таких злочинів, як вимагання, примус до укладання угод, шахрайство, викрадення людей, знищення майна, залякування, фізичне насильство тощо.

Проведене нами дослідження 57-ми рейдерських захоплень в Україні (перелік підприємств подано в додатку Е) засвідчило такі особливості їх вчинення з використанням визначених нами вище технологій (див рис. 3.34):

Аналіз рейдерських атак, що відбувалися в Україні з часу проголошення Незалежності по сьогоднішній засвідчили значну частку використання адміністративного ресурсу при вчиненні протиправних захоплень, чимало підприємств зазнало силового захоплення бізнесу, за допомогою маніпуляцій з власниками було вчинено рейдерські атаки на 30 % досліджуваних ділових одиниць. Також проведений нами аналіз показав, що ЗМІ значною мірою (25 % підприємств) сприяли протиправним поглинанням в Україні.

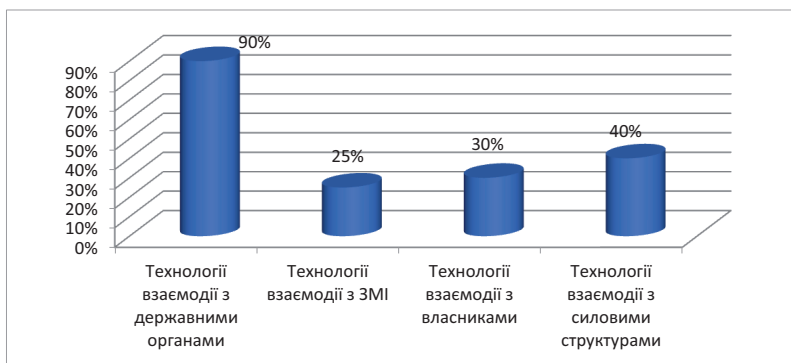


Рис. 3.34. Технології, які використовували рейдери при захопленні суб'єктів підприємництва в Україні впродовж останніх 30-ти рр.

Джерело : сформувала автор на основі дослідження підприємств (Додаток М)

Окремо необхідно зупинитися на так званому “реєстраційному” рейдерстві, що реалізувалося шляхом внесення змін до державних реєстрів на підставі поданих державному реєстратору підроблених рішень органів управління підприємства, договорів про відчуження, рішень суду тощо. За цієї схеми рейдери подавали реєстратору протокол зборів учасників товариства (інші документи, відповідно до яких права переходили до третьої особи), а реєстратор своєю чергою здійснював відповідну реєстраційну дію та передавав корпоративні права такій особі [71, с. 117–118].

До рейдерських схем, пов'язаних із незаконною державною реєстрацією належали такі [271]:

- використання підроблених документів щодо переходу права власності на корпоративні права або нерухоме майно;

– вчинення реєстраційної дії на підставі підробленого або неіснуючого рішення суду;

- підкуп реєстратора або нотаріуса;
- викрадення електронного ключа реєстратора.

Рейдерство еволюціонувало від ранньої своєї форми, так званого “рекету”, що характеризувалося фізичним та психологічним насильством (погрозами, шантажем, вимаганням тощо) до більш інтелектуального виду, що передбачає використання важелів впливу в документообігу та функціонуванні державних реєстрів.

Протидія використанню незаконної державної реєстрації в схемах протиправного захоплення підприємств є одним із пріоритетних завдань держави в особі низки уповноважених органів. Так, Міністерством юстиції України впродовж 2021 р. реалізовано заходи, що дали змогу забезпечити позитивну динаміку у сфері адміністративного оскарження державної реєстрації нерухомості та бізнесу. Зокрема кількість скарг, що надходять на розгляд Міністерства юстиції України щодо дій у Державному реєстрі речових прав на нерухоме майно і в Державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, сукупно зменшилася на 16 % – у 2021 р. надійшло 3 261 скарга, у 2020 р. – 3 863. Упродовж 2021 р. Колегією з розгляду скарг на рішення, дії або бездіяльність державного реєстратора, суб’єктів державної реєстрації, територіальних органів Міністерства юстиції було опрацьовано 3 496 скарг. Цей показник на 30 % перевищив показник 2020 р. – 2 694 скарги. Проте кількість задоволених скарг зменшилася: 1 057 скарг у 2021 р. і 1 104 скарги у 2020 р. Тобто якщо у 2020 р. було скасовано 41 % оскаржуваних реєстраційних дій із загальної кількості розглянутих, то у 2021 р. цей показник знизився до 30 %. Тож, при збільшенні кількості розглянутих скарг спостерігається суттєве зменшення відсотка обґрунтованих скарг. Кількість незаконних реєстраційних дій у 2021 р., порівняно з 2020 р., скоротилася майже на 50 % [185].

Радою бізнес-омбудсмена в Україні з травня 2015 року було отримано та опрацьовано 114 скарг щодо роботи державних реєстраторів, зокрема у 2019 р. – 35 скарг на роботу державних реєстраторів, що на 18 % більше

порівняно з попереднім роком, а за 2020 р. – було отримано 27 таких скарг [186].

Для посилення захисту бізнесу, фізичних осіб та їх майна в умовах воєнного стану було прийнято Закон України “Про внесення змін до деяких законів України щодо удосконалення механізму протидії рейдерству” № 2255-IX від 12.05.2022 р. Законом передбачено можливість проведення реєстраційних дій в автоматичному режимі з використанням Єдиного державного веб-порталу електронних послуг; удосконалено механізм оскарження державної реєстрації щодо нерухомого майна та бізнесу; запроваджено норму про неможливість розірвання договору оренди сільськогосподарської землі без згоди учасників товариства [217].

10.10.2022 набрав чинності також Закон України “Про гарантування речових прав на об’єкти нерухомого майна, які будуть споруджені в майбутньому” № 2518-IX від 15.08.2022 р., яким визначено нові механізми гарантування державою речових прав на об’єкти незавершеного будівництва та майбутні об’єкти нерухомості, право на виконання будівельних робіт щодо яких отримано [219].

Водночас з метою протидії рейдерству необхідне подальше удосконалення чинного законодавства, зокрема відокремленням рейдерства від інших видів злочинної діяльності та визначивши його як окремих склад злочину в Кримінальному кодексі України.

Окрім державної політики у сфері боротьби з рейдерством, важливим також є управлінський підхід власників та керівників суб’єктів підприємництва щодо протидії протиправному захопленню. Однак згідно з виявленими нами результатами дослідження, 93–95 % власників і керівників вітчизняних підприємств недооцінюють заходи щодо попередження рейдерства й звертаються щодо отримання юридичної допомоги лише на етапі вчинення агресивних дій [307].

В якості метафоричного інструментарію пояснення причин поширення рейдерства в Україні як одного із найбільш небезпечних гібридних фінансових конфліктів можна використати теорію “сірого носорога”, згідно якої очевидні прояви ризикових ситуацій недооцінюють менеджмент та власники суб’єктів підприємництва, що призводить до катастрофічних наслідків у майбутньому.

Щоб протидіяти рейдерству, суб'єкти підприємництва повинні проводити моніторинг підозрілих явищ, дій та чинників внутрішнього та зовнішнього середовища з метою виявлення ознак можливих агресивних дій. Це дасть змогу вчасно розпізнати та убезпечитись без зловмисних ринкових намірів. Відтак, пропонуємо враховувати такі ознаки ймовірної рейдерської атаки (рис. 3.35):

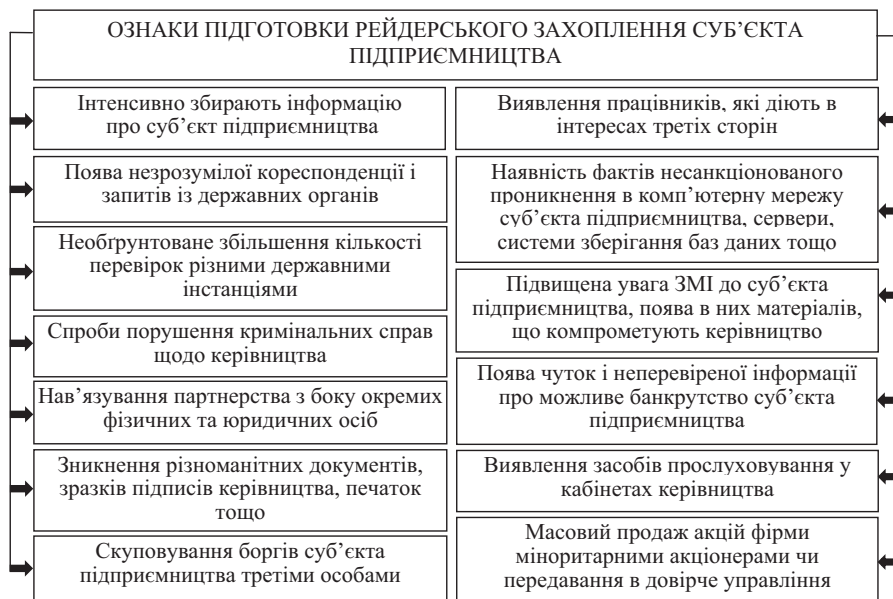


Рис. 3.35. Систематизація типових ознак підготовки рейдерського захоплення

Джерело: розробила автор

Пропоновані індикатори раннього виявлення загрози рейдерства, дають змогу передбачити в системі забезпечення фінансової безпеки суб'єктів підприємництва функціональні обов'язки працівників відповідних відділів, які б здійснювали моніторинг таких ознак. Для прикладу PR-відділ та IT-відділ повинні бути уповноважені відстежувати інформацію про підприємство, його власників і керівництво у ЗМІ, соціальних платформах тощо з метою вчасного виявлення дезінформації чи інших маніпуляцій даними. Працівники служби безпеки ділової одиниці – проводити перевірку робочих кабінетів керівництва на наявність вмонтованих засобів

прослуховування, відділ правового забезпечення у випадку немотивованого збільшення кількості перевірок державними органами – перевіряти їх на правочинність. Постійний моніторинг ранніх ознак рейдерства спільними зусиллями відповідних служб суб'єктів підприємництва дасть змогу вчасно виявити загрозу рейдерського захоплення та вжити заходи щодо її нейтралізації.

3.3. Недобросовісна конкуренція як системна проблема фінансової безпеки суб'єктів підприємництва в Україні

Структурні перетворення, що відбуваються в Україні, ускладнені політичною нестабільністю та фінансовою кризою внаслідок пандемії Covid-19 та воєнного стану, призводять до обтяжливих наслідків для ділових одиниць і зумовлюють поширення недобросовісної конкуренції – гібридного фінансового конфлікту між суб'єктами господарювання, що здійснюються із застосуванням при їх вирішенні як класичних засобів конкурентної боротьби, так і методів протиправної поведінки, зокрема шпигунської економічної діяльності, шантажу, кіберзлочинів тощо.

Фінансові кризи локального чи глобального масштабу завжди загострюють економічне суперництво між суб'єктами господарювання, що призводить до поширення використання учасниками ринку недобросовісних конкурентних дій. Це генерує загрозу фінансовій безпеці суб'єктів підприємництва та завдає шкоди їх споживачам та державі в цілому в зв'язку із погіршенням іміджу країни у світовому масштабі. Відтак, ключовим принципом забезпечення свободи підприємницької діяльності є державний захист конкуренції, недопущення зловживання монопольним становищем на ринку та неправомірного обмеження конкуренції, а також будь-яких інших проявів недобросовісної конкурентної боротьби.

Початком розвитку законодавства про недобросовісну конкуренцію в європейських країнах стала Паризька конвенція про охорону промислової власності від 20 березня 1883 р. [249], в якій містяться положення про те, що всі країни-учасниці зобов'язані протистояти недобросовісній конкуренції. В Україні відносини, пов'язані зі захистом

від недобросовісної конкуренції, регулюються Законом України “Про захист від недобросовісної конкуренції” [236], Законом України “Про захист економічної конкуренції” [237], Законом України “Про Антимонопольний комітет України” [214], Законом України “Про публічні закупівлі” [251]. Однак, незважаючи на наявність значної законодавчої бази в сфері захисту економічної конкуренції, кількість випадків недобросовісної конкурентної боротьби щороку збільшується. Відтак, можемо констатувати, що чим більше загострюється конкурентна боротьба, тим серйознішими є прояви недобросовісної конкуренції. Це пояснюється тим, що в умовах висококонкурентних ринків підвищується рівень непередбачуваності поведінки ділових одиниць, що, своєю чергою, спричиняє порушення рівноваги окремих виробничих процесів, чинників виробництва, цін тощо.

Недобросовісні конкурентні дії зумовлюють деструктивний вплив на фінансові результати суб’єктів підприємництва й знижують рівень їхньої фінансової безпеки.

Водночас серед науковців й досі не вироблено єдиного підходу до розуміння сутності поняття “недобросовісна конкуренція”, зокрема в економічній літературі трапляються такі погляди на його тлумачення:

– недобросовісна конкуренція – це будь-які дії у конкуренції, що суперечать правилам, торговим та іншим чесним звичаям у підприємницькій діяльності. Згідно цього підходу окремо виділяються дії, що призводять до монопольного становища на ринку [64];

– недобросовісна конкуренція – це антиконкурентні дії суб’єктів господарювання чи бездіяльність, пов’язані з порушенням чинного законодавства, торгових правил та звичок, прав на інтелектуальні продукти, вимог добропорядності і справедливості шляхом вчинків, здатних ввести громадськість в оману, дискредитувати конкурента [12];

– нечесна конкуренція – це діяльність господарського суб’єкта, спрямована на одержання комерційної вигоди і забезпечення домінуючого становища на ринку за рахунок обману споживачів, партнерів, інших господарських суб’єктів і державних органів [177].

Відповідно до Закону України “Про захист від недобросовісної конкуренції” від 07.06.1996 р. № 236/96-ВР недобросовісною конкуренцією є будь-які дії у конкуренції, що суперечать торговим та

іншим чесним звичаям у господарській діяльності [236]. Відповідно до законодавства такими діями можуть бути:

- неправомірне використання ділової репутації суб'єкта господарювання, зокрема неправомірне використання позначень, неправомірне використання товару іншого виробника, копіювання зовнішнього вигляду виробу, порівняльна реклама;

- створення перешкод суб'єктам господарювання у процесі конкуренції та досягнення неправомірних переваг у конкуренції, зокрема дискредитація суб'єкта господарювання, схилення до бойкоту суб'єкта господарювання, схилення постачальника до дискримінації покупця (замовника), підкуп працівника, посадової особи постачальника, підкуп працівника, посадової особи покупця (замовника), досягнення неправомірних переваг у конкуренції, поширення інформації, що вводить в оману;

- неправомірне збирання, розголошення та використання комерційної таємниці, зокрема неправомірне збирання комерційної таємниці, розголошення комерційної таємниці, схилення до розголошення комерційної таємниці, неправомірне використання комерційної таємниці.

При досить широкому тлумаченні сутності поняття “недобросовісна конкуренція” не завжди вдається правильно класифікувати ті чи інші способи конкурентної діяльності. Нечіткі межі між чесною та недобросовісною конкуренцією є передумовою виникнення гібридних фінансових конфліктів, основними проявами яких є економічне шпигунство, вплив на споживачів шляхом маніпулювання інформацією, підробка продукції конкурентів, підкуп і шантаж, корупція, шахрайство з фінансовою звітністю, обдурювання споживачів шляхом приховування дефектів тощо. Так, при здійсненні недобросовісної конкуренції часто використовують технології взаємодії із працівниками підприємства з метою отримання конфіденційної фінансової інформації та даних, що становлять комерційну таємницю. Це різноманітні перемовини, що часто відбуваються шляхом підкупу або з елементами психологічного тиску, зокрема, залякування, шантажу тощо. Крім того, недобросовісні конкуренти активно застосовують технології взаємодії з державними органами й унаслідок використання корупційних механізмів

отримують конкурентні переваги на ринку. Особливе місце в процесі здійснення недобросовісної конкурентної діяльності відводять технологіям взаємодії зі ЗМІ. Метою замовних PR-компаній є формування вигідної для конкурентів громадської думки про діяльність підприємства-об'єкта недобросовісних конкурентних дій і, здебільшого, спрямовані на компрометування його керівництва та продукції чи послуг, які ним пропонуються на ринку. У ЗМІ можуть поширювати неправдиву інформацію про незадовільний фінансово-господарський стан підприємства, невиконання ним зобов'язань перед контрагентами, анулювання ліцензій тощо.

Недобросовісна конкуренція є виявом конфлікту фінансових інтересів учасників ринку. Її сутність полягає в тому, що за допомогою сукупності прихованих важелів впливу відбувається перерозподіл прибутків й стимулів удосконалення організації виробництва на користь зловмисників у вигляді недобросовісних конкурентів, що порушує справедливі закони ринкової взаємодії учасників. Відтак, пропонуємо розуміти під недобросовісною конкуренцією гібридний фінансовий конфлікт між суб'єктом підприємництва та його конкурентами, що виникає внаслідок порушення чинного законодавства й норм ділового етикету останніми з метою одержання неправомірних конкурентних переваг, комерційної вигоди і забезпечення домінуючого (монопольного) становища на ринку.

Проводячи аналогію з міжнародними гібридними конфліктами, можемо констатувати, що на світових ринках часто здійснюється цінова й нецінова дискримінація окремих країн, що розвиваються й перебувають у процесі трансформації економіки. Водночас, як і на мікроекономічному рівні, коли рейдери можуть використовувати інструменти недобросовісної конкуренції для захоплення підприємств, й навпаки, конкуренти можуть усувати суб'єкт господарювання з ринку шляхом його протиправного поглинання, у світовому масштабі відбуваються такі ж гібридні протистояння. Для прикладу росія, переслідуючи політичні цілі захоплення України, тривалий час використовувала недобросовісні конкурентні методи, серед яких – впровадження дискримінаційних умов торгівлі, маніпулювання цінами на значущі для економіки України товари, блокування транзиту українських товарів в інші країни. Внаслідок використання росією

торговельної війни як інструменту гібридної агресії Україна неодноразово подавала позови до Світової організації торгівлі, зокрема, в 2016 р. – щодо обмеження росією імпорту українських вагонів і обладнання. Згодом росією було введено заборону на прямі транзитні перевезення вантажів з України в Казахстан і Україною було подано новий позов до СОТ на неправомірність обмеження транзиту товарів через територію росії в треті країни – Казахстан і Киргизстан.

Використання інструментів недобросовісної конкуренції як у міждержавних протистояннях, так і на мікроекономічному рівні можемо охарактеризувати такими основними ознаками:

- активність та планомірність вчинення зловмисних дій конкурентами;
- прихований протиправний характер дій конкурентів;
- наявність тіньових мотивів у конкурентів, у тому числі, політичних;
- спрямованість реалізованих антиконкурентних заходів на досягнення неправомірних переваг у конкурентній боротьбі;
- деструктивність наслідків зловмисних дій у формі фінансових і репутаційних збитків для об'єкта агресії.

Аналіз основних тенденцій поширення недобросовісної конкуренції на основі звітних даних Антимонопольного комітету України впродовж 2019–2021 рр. [181] дав змогу виявити, що у 2019 р. було припинено 2 071 порушення конкурентного законодавства, з яких майже 40 % становили антиконкурентні узгоджені дії. Загальна вартість закупівель, на яких було виявлено змови, становила понад 10 млрд грн. У 2020 р. було припинено 1 624 порушення конкурентного законодавства, з яких значний обсяг порушень – змови на публічних закупівлях. Загальна вартість закупівель, на яких було виявлено змови, перевищувала 7 млрд грн. Розмір накладених штрафів становив 1,6 млрд грн. Найпоширенішим видом недобросовісних дій, які здійснювалися з метою досягнення неправомірних переваг у конкуренції, було поширення інформації, що вводить в оману. Цей вид порушення склав 85 % від загальної кількості дій, що належать до недобросовісної конкуренції суб'єктів господарювання [262].

У 2021 р. було виявлено загалом 1 675 порушень, зокрема змов під час закупівель – на загальну вартість понад 13 млрд грн, що суттєво перевищує показник 2020 р. Сума накладених штрафів у межах виявлених порушень склала понад 7 млрд грн [181].

Відтак, можемо констатувати, що впродовж останніх років дослідження засвідчують, що значного поширення набули порушення у вигляді змов при проведенні публічних закупівель.

Дослідження проявів недобросовісної конкуренції в практиці вітчизняних суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею пального в Україні, засвідчило такі найбільш поширені їх випадки впродовж 2017–2021 рр. (рис. 3.36).

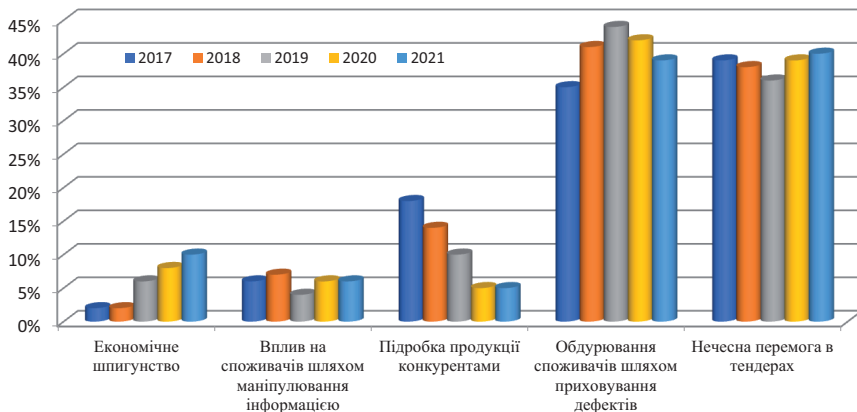


Рис. 3.36. Прояви недобросовісної конкуренції в діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні впродовж 2017–2021 рр.

Джерело : сформувала автор на основі анкетування

Як видно з рис. 3.36, основними злочинними діями конкурентів у досліджуваній сфері діяльності були нечесна перемога в тендерах та обдурювання споживачів шляхом приховування дефектів.

Недобросовісна конкуренція становить вагому загрозу фінансовій безпеці суб'єктів підприємництва, зокрема згідно з результатами опитування керівників вітчизняних ділових одиниць, проведеного РwC у 2020 р., недобросовісна конкуренція була одним із трьох економічних злочинів, які мали найбільш суттєвий вплив на їхнє функціонування, враховуючи як фінансові збитки, так й інші негативні наслідки (рис. 3.37).



Рис. 3.37. Вплив недобросовісної конкуренції на результати фінансово-господарської діяльності українських компаній у 2020 р. [41]

Щоб забезпечити належний рівень фінансової безпеки суб'єкти підприємництва повинні протидіяти гібридним фінансовим проявам у формі недобросовісної конкуренції. Водночас, щоб ухвалювати ефективні стратегічні фінансові рішення, необхідна інформаційна обізнаність про партнерів та конкурентів. Відтак, можемо констатувати на необхідності реалізації двостороннього завдання власниками та керівництвом ділових одиниць – здійснювати конкурентну розвідку та забезпечувати захист власної конфіденційної інформації й комерційних даних від конкурентів.

Варто зауважити, що у вітчизняній фаховій літературі часто ототожнюють поняття “конкурентна розвідка” й “промислове шпигунство”, що не є коректним.

Вважаємо, що призначенням конкурентної розвідки є отримання даних щодо:

- ринкових тенденцій з метою розроблення власної стратегії розвитку;
- можливих інструментів тиску, які можуть застосовуватися конкурентами з метою вироблення адекватних засобів протидії їм;
- особливостей функціонування конкуруючих на ринку суб'єктів господарювання з метою виявлення їхніх слабких сторін, й на цій основі покращення власної ринкової позиції;
- місткості споживчого ринку з метою прогнозування власного фінансового стану;
- можливостей розширення діяльності в інших регіонах;

– умов співробітництва конкурентів з партнерами з метою налагодження ділових зв'язків.

Промислове (ділове) шпигунство – це збір конфіденційної інформації та даних комерційної таємниці, які є об'єктом захисту на законодавчому рівні й за зловживання ними передбачено правову відповідальність. Цей вид злочинної діяльності на сьогодні набув суттєвого поширення й становить вагомую загрозу фінансовій безпеці суб'єктів підприємництва, зокрема сучасна форма його прояву, зумовлена стрімким розвитком інформаційних технологій – кібершпигунство, яке здійснюється шляхом прихованого відстежування, розшуку, збирання та викрадання конфіденційної інформації конкурентами з використанням кібернетичного простору. Натомість, конкурентна розвідка передбачає збір інформації про конкурентів, яку вони оприлюднюють у відкритих джерелах. Відтак, важливою відмінною рисою конкурентної розвідки й промислового (ділового) шпигунства є дотриманням чинних законодавчих норм і відповідність етичним стандартам.

Окрім того, конкурентна розвідка передбачає вивчення змін чинного законодавства у сфері діяльності суб'єктів господарювання, кадрових потоків працівників, які можуть мати вплив на їхнє функціонування, політичної ситуації в країні, міжнародної ситуації тощо.

Цікавим у контексті забезпечення фінансової безпеки є метафоричний підхід до розуміння конкурентної розвідки американського дослідника Г. Мейера [380], який порівнює її з навігаційною системою корабля або літака, що дає змогу оцінити місце суб'єкта підприємництва в зовнішньому середовищі й визначити загрози його функціонування та можливості розвитку.

Узагальнюючи погляди вчених та враховуючи результати дослідження практичних аспектів здійснення конкурентної розвідки в міжнародній практиці, пропонуємо під конкурентною розвідкою розуміти діяльність, яка полягає у здійсненні сукупності заходів із використанням легальних методів отримання інформації суб'єктом підприємництва про його конкурентів з метою розроблення ринкової стратегії розвитку та протидії загрозам, генерованим недобросовісними конкурентами. Способи отримання інформації при здійсненні конкурентної розвідки й ділового шпигунства подано на рис. 3.38.

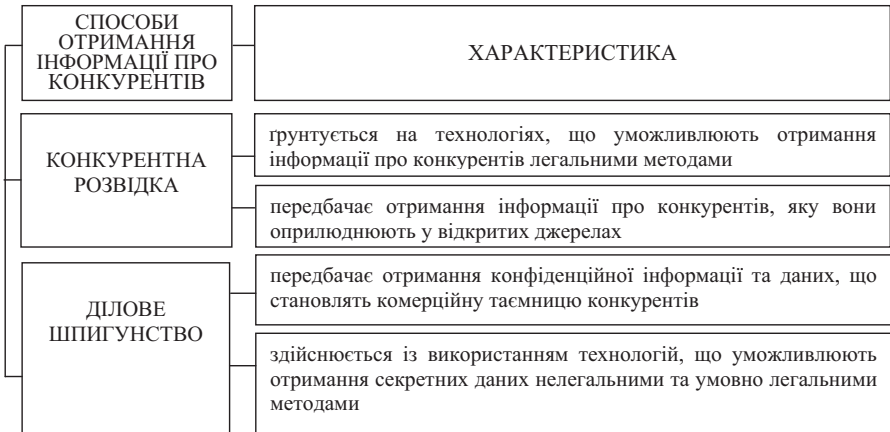


Рис. 3. 38. Характеристика способів отримання інформації при здійсненні конкурентної розвідки та ділового шпигунства

Джерело: розробила автор

Серед основних джерел інформації, що використовується при здійсненні недобросовісної конкуренції, варто виокремити такі:

- матеріали галузевих конференцій, виставок, семінарів;
- дані, розміщені на соціальних платформах суб'єктів підприємництва;
- аналітичні дослідження вітчизняних та міжнародних агенцій;
- маркетингові тести конкурентів;
- інформація щодо змін ціни й упакування продукції конкурентів;
- відгуки споживачів про продукцію (роботи, послуги) конкурентів, розміщені на інтернет-платформах.

Можна констатувати, що на сьогодні, в умовах глобалізації та діджиталізації, мережа Internet стала основним джерелом отримання розвідувальної інформації. Однак, на думку експертів, в Інтернеті в придатному для використання у конкурентній розвідці вигляді можна знайти лише близько 10–15 % необхідної інформації, решта 85–90 % – отримується в результаті порівняння, інтеграції та аналізу численних розрізнених даних, що є можливим тільки із застосуванням спеціальних програмних інструментів [161, с. 429].

У вітчизняній практиці господарювання ще недостатньо уваги приділяється конкурентній розвідці, водночас згідно з даними опитування міжнародної платформи щодо вивчення й впровадження технологій

конкурентної розвідки “Crayon”, проведеного у 2021 р. 42 % керівників суб’єктів підприємництва планують інвестувати в заходи із конкурентної розвідки та збільшити штат фахівців у цій сфері, понад 50 % – планують збільшити використання технологій конкурентної розвідки [93].

Активного поширення на сьогодні набуває розвідка на основі відкритих джерел (OSINT). Зокрема, згідно з результатами спільноти OSINT “Molfar” серед 90 досліджуваних підприємств, які займаються OSINT у США і Україні 82 % надають послуги з конкурентної розвідки; 32 % організацій, що здійснюють конкурентну розвідку, використовують власне програмне забезпечення для доступу до існуючих баз даних, аналізу і моніторингу конкурентів; 19 % – застосовують стороннє програмне забезпечення для виконання досліджень, зокрема, такі програмні продукти, як LexisNexis, Factiva, Westlaw; 41 % компаній надають офлайн-сервіси, такі як приховане спостереження, аудит системи ІТ-безпеки або розробка стратегії протидії шпигунству [9].

Недобросовісна конкуренція, як і різноманіття методів боротьби з нею наявні у всіх країнах світу. Подолати повністю це явище складно, адже в умовах ринкової форми господарювання завжди існує частка суб’єктів підприємництва, які заради економічної вигоди вдаються до різних інструментів конкурентної боротьби, які можуть бути недобросовісними. Однак, щоб забезпечити належний рівень фінансової безпеки ділових одиниць, важливим є розроблення стратегії його діяльності з дотриманням балансу інтересів учасників ринку (рис. 3.39).

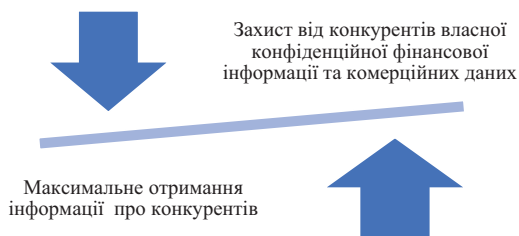


Рис. 3.39. Баланс фінансових інтересів учасників ринку при здійсненні конкурентної діяльності

Джерело: розробила автор

Відтак, суб’єктам підприємництва необхідно здійснювати конкурентну розвідку щодо інших учасників ринкового оточення з метою забезпечення інформаційної обізнаності про них та готовності до потенційно загрозливих

дій з їх сторони та одночасно забезпечити максимально можливий захист внутрішнього середовища від проявів промислового (ділового) шпигунства.

В умовах ринкової економіки, що характеризується мінливістю й невизначеністю значної кількості чинників складно забезпечити баланс фінансових інтересів між конкуруючими підприємствами. Однак створення дієвої системи регулювання конкурентних відносин з ефективним співвідношенням саморегулювання та державного регламентування конкурентної діяльності є необхідною умовою забезпечення розвитку як економіки країни загалом, так і індивідуальних ділових одиниць. Тому на державному рівні необхідно постійно проводити пошук шляхів удосконалення механізму регулювання конкуренції, а на рівні суб'єктів підприємництва важливо дотримуватися ділового етикету при здійсненні конкурентної діяльності, однак у разі наявності даних конкурентної розвідки щодо потенційної загрози недобросовісних конкурентних дій – своєчасно вживати ефективних заходів протидії їм.

3.4. Критичні наслідки фінансових небезпек у формі корупції

Корупція є однією із ключових загроз фінансовій безпеці України, оскільки гальмує економічний розвиток держави, знижує інвестиційну привабливість суб'єктів господарювання, підвищує рівень фінансової злочинності в суспільстві. Крім того, чимало вітчизняних та зарубіжних експертів та політиків світового масштабу сприймають корупцію як інструмент у гібридній війні. Зокрема, Президент США Джо Байден, зазначав: “Російські операції з дезінформації, кібератаки та енергетична політика отримали значну увагу. Водночас недостатньо висвітлені способи, якими росії вдалося ефективно експортувати корупцію у вразливі суспільства, що спотворює їх політику та економіку” [351].

Досліджуючи сутність поняття “корупція”, варто передусім відзначити неоднозначність етимології цього слова. Згідно з одним із підходів термін “корупція” бере свій початок від латинського слова “*corruptio*”, що означає підкуп, продажність посадових осіб органів публічної влади, громадсько-політичних діячів. Відповідно до іншого підходу поняття “корупція” походить від давньоримських дефініцій “*correi*” (декілька учасників зобов'язальних відносин щодо певної справи, відповідного предмета) та “*rumpere*” (ламати, руйнувати, пошкоджувати, порушувати, скасовувати,

підкупувати), поєднання яких у самостійну філологічну конструкцію зумовило виникнення категорії “*corruptere*”, що в загальному вигляді розумілось як групова деструкція, дія певної групи з кількох пов’язаних між собою діловими відносинами осіб, спрямована на порушення законного порядку та ходу судового процесу або управління суспільними справами” [84, с. 45]. Щодо зародження та еволюції явища корупції, то корупція існувала вже в часи Стародавнього Єгипту. Зокрема, у знайденому стародавньому єгипетському папірусі згадується про факти корупції серед державних службовців фараона. Історичний аналіз зародження корупції в Київській Русі засвідчує перші згадування про це явище у літописах XIII століття, зокрема у Двінській уставній грамоті 1397–1398 рр., де міститься визначення незаконної винагороди за здійснення офіційних владних повноважень – “мздоїмство” або “посула”. Також згадується “посула” в якості хабара у Псковській судній грамоті (1462–1471 рр.) [117, с.4].

Протидіяти корупції намагалися в часи Стародавнього Риму шляхом [36, с. 4]:

1. Визнання неприпустимим долучення сенаторів до окремих сфер діяльності: “заборона займатися морською торгівлею, фінансовими операціями, а також казенними підрядами”.

2. Намагання протидіяти деградації суспільній моралі, що зумовлювало розширення середовища для поширення корупції. З цією метою у Римі приймали та запроваджували закони про розкіш – “*leges sumptuariae*”. Зокрема “Закон про подарунки” (*lex Cincia de donationibus*) 204 р. до н. е. обмежував їх розмір від клієнта патрону та запроваджував заборону на деякі види дарунків і форми дарування; деякими законами (Закон Гая Орхідія 181 р. до н. е., Закон Фаннія 161 р. до н. е.) суворо регламентувалося проведення масових заходів – званих обідів та вечерь (аж до визначення кількості гостей та обсягу коштів, які дозволялося витратити).

3. Спеціальне законодавство щодо обмеження розмірів окремих різновидів власності, що може перебувати в руках осіб або їхніх родин або ж користування деякими благами: “Закон Клавдія (*lex Claudia de nave senatorum*) 218 р. до н. е. забороняв сенаторам та їхнім сім’ям володіти кораблями, що вмщували понад 300 амфор (ці норми повторно використав Цезар у 59 р. до н. е. в *lex de heretundis*); Закон Оппія (*lex Oppia*) 215 р. до н. е. забороняв римським жінкам мати понад пів унції

золота, носити різнокольоровий одяг, їздити у візках по Риму й інших містах або навколо них на відстані милі, окрім днів державних і релігійних свят”.

4. Обмеження обсягів споживання: Закон Публія Ліцинія Красса Муціана 131 р. до н. е. впроваджував обмеження кількості м'яса, що могло споживатися.

Про корупцію згадується також у релігійних джерелах. Відтак, першу антикорупційну заповідь дав Господь через Мойсея, який записав те, що почув із неба: “Дарів не приймай, бо дари сліпими роблять зрячих і перекручують справу правих” (Ісх. 23:8) [172, с. 54]. У Старому Завіті йдеться, що Мойсей проповідував проти прийняття подарунків, тому що вони “засліплюють очі” та призводять до несправедливості. У Корані зафіксовано спеціальну заборону платити хабарі. Пророк Мохаммед застерігав, що Аллах прокляне всіх, хто платить та бере хабарі, а також того, хто сприяв цьому. Будда зазначав, що коли правитель, керуючи державою, шукає вигоди, то це врешті-решт призведе до деформації сутності суспільних відносин та ігнорування принципів справедливості [3, с. 17].

Сприйняття корупції як деструктивного явища мало здебільшого морально-етичний характер, що з часом еволюціонувало й набуло наукового розуміння. Згідно з традиційним або нормативно-ціннісним підходом під корупційними діями та проявами розуміють такі, що кидають виклик загальноприйнятим морально-етичним та нормативно-правовим нормам, є антиподами таких суспільних ціннісних поглядів-переконань, як “загальне благо” та “суспільна користь”. Грошово-фінансовий характер корупційних дій для отримання особистої вигоди не обов'язковий, вона може виявлятися у просуванні службовими сходами корупціонера, його близьких або осіб з його оточення [170, с. 102].

Згодом корупцію як наукову категорію почали досліджувати в розрізі політології. Так, на думку Джеймса Брайса, корупція може бути реалізована шляхом підкупу державних службовців, спекуляцією з документами; спекуляціями для вигоди кандидатів. Д. Брайс уважав, що основним елементом корупції є підкуп державних службовців [353, с. 150].

Зокрема, Дж. Най обґрунтовував, що “корупція є поведінкою, яка відхиляється від нормального виконання обов'язків державним

чиновником з метою отримання приватної (сімейної, кланової), матеріальної або статусної вигоди” [381, с. 417].

На переконання К. Фрідріха, хоча корупція є явищем однозначно негативним, повна перемога над корупцією – утопічне завдання, їй “потрібно давати енергійну відсіч, щоб хвороботворні паростки не поширювалися і не руйнували політичну систему” [368, с. 482]. Учений розцінював як індикатор корумпованості влади ступінь консенсусу в суспільстві, а політичну опозицію і вільні засоби масової інформації називав факторами, що стримують корупцію [368, с. 15].

Серед сучасних підходів до розуміння корупції трапляються такі:

– корупція – соціальне явище, яке охоплює всю сукупність корупційних діянь, пов’язаних із неправомірним використанням особами, уповноваженими на виконання функцій держави, наданої їм влади, службових повноважень, відповідних можливостей з метою задоволення особистих інтересів чи інтересів третіх осіб, а також інших корупційних правопорушень, у тому числі й тих, які створюють умови для вчинення корупційних діянь чи є приховуванням їх або потуранням [151, с. 6];

– корупція – соціально небезпечне явище, змістом якого є система негативних поглядів, настанов і діянь службових осіб інститутів влади та управління, державних і недержавних підприємств, організацій і установ, політичних партій та громадських організацій, спрямованих на задоволення особистих, групових або корпоративних інтересів шляхом використання свого службового становища, всупереч інтересам суспільства та держави [166, с. 62];

– корупція – це пряме використання посадовою особою свого службового становища з метою особистого збагачення та підкупність, продажність урядовців і громадських діячів [37, с. 258];

– корупція – злочинна діяльність у сфері політики та державного управління, яка полягає у використанні посадовими особами довірених їм прав та владних повноважень для особистого збагачення [274, с. 120];

– корупція – форма зловживання владою, пов’язана з підкупом посадових осіб та процес, пов’язаний із використанням посадовою особою своїх повноважень, з метою особистого збагачення, використовуючи підкуп та дачу хабарів [305, с. 220];

- корупція – протизаконне діяння посадових осіб, спрямоване на особисте збагачення та стійкий зв'язок представників владно-управлінських структур зі злочинним середовищем і сприяння йому у протиправній діяльності шляхом використання наданих їм державою повноважень [283, с. 20];

- корупція – складне соціальне явище, яке негативно впливає на всі аспекти політичного і соціально-економічного розвитку суспільства та держави, загрожує демократії та правам людини, реалізації принципу верховенства права, підриває соціальну справедливість, легітимність публічних інститутів, добробут, завдає шкоди суспільству, соціальному прогресу та національній безпеці [265, с. 69].

Чимало дослідників у своїх працях визначали деструктивні наслідки корупційних дій. Зокрема, В. Гарашук наголошує, що корупція дискредитує діяльність державного апарату і руйнує основні принципи, на які спирається демократична держава, принципи рівності громадян перед законом, справедливості, неупередженості правосуддя, захищеності людини правоохоронними структурами від різного роду протиправних посягань і свавілля чиновників та ін. [45, с. 12].

Сар Дж. Пундей зазначає: “Корупція не є інфекцією, яку раптом може “підхопити” здорове суспільство. Вона є наслідком явищ і тенденцій політики, економіки та розвитку держави”. Автор наголошує, що корупція “носить характер злочинної діяльності у політичній сфері, що призводить до дискредитації апарату державного управління” [257, с. 19].

У Законі України “Про запобігання корупції” від 14.10.2014 р. [225] термін “корупція” тлумачиться як використання особою наданих їй службових повноважень чи пов'язаних із ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди особі, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов'язаних із ними можливостей. Засади запобігання, виявлення, розслідування та розкриття корупційних правопорушень в Україні визначено Законом України “Про Національне антикорупційне бюро України” від 14.10.2014 р. [241].

У Декларації ООН про боротьбу з корупцією і хабарництвом у міжнародних комерційних операціях встановлено елементи хабарництва [59]:

- пропозицію, обіцянку або передачу будь-яких виплат, подарунків або інших благ, прямо або побічно, будь-якою приватною або державною корпорацією, в тому числі транснаціональною корпорацією, окремою особою якої-небудь держави будь-якій державній посадовій особі або обраному представникові іншої країни як неправомірної винагороди за виконання або утримання від виконання цією посадовою особою або представником своїх обов'язків у зв'язку з тією чи іншою міжнародною комерційною операцією;

- вимогу прийняття або отримання, прямо або опосередковано, будь-якою посадовою особою або обраним представником будь-якої держави виплат, подарунків або інших благ у будь-якої приватної або державної корпорації, в тому числі транснаціональної корпорації, або окремої особи з іншої країни як неправомірної винагороди за виконання або утримання від виконання цією посадовою особою або представником своїх обов'язків у зв'язку з тією чи іншою міжнародною комерційною операцією.

Дослідження еволюції поняття “корупція” від його розуміння як антиморального деструктивного суспільного явища до аналізу його через політичну, соціально-економічну та правову призму дає підстави зробити висновок, що корупція в загальному розумінні порушує інтереси одних сторін на користь інших.

В більшості випадків йдеться про конфлікт фінансових інтересів, який реалізується в прихованій формі шляхом хабарництва, підкупу, протекціонізму, лобізму і т. д. Множинність засобів досягнення фінансових цілей, що мають прихований характер, доводить гібридну природу такого фінансового конфлікту.

Всеукраїнською Мережею Добросесності та Комплаєнсу (UNIC) виявлено особливості взаємодії держави та бізнесу “Корупційні ризики у діяльності органів влади: погляд бізнесу” шляхом опитування 305 представників суб'єктів підприємництва [88]. Згідно з одержаними результатами, дві третини респондентів ідентифікують корупцію, як чинник, що перешкоджає веденню бізнесу; 82 % представників підприємств вважають, що корупція в Україні є поширеним явищем, 61 %

– дуже поширеним; 40 % респондентів зазначають про наявність підприємств, які перебувають під патронажем державних службовців та політиків. Дослідження засвідчує глибинний взаємозв’язок між корупцією та поширенням недобросовісної конкуренції.

Водночас, згідно з опитуванням населення “Доброчесний бізнес: здобутки та можливості”, проведеного UNIC, у суспільстві існує запит на доброчесність. Так, двоє із трьох респондентів повністю згодні з висловлюваннями: “Для мене важливо купувати продукцію та послуги у виробника, який декларує високий рівень доброчесності”, “Репутація і доброчесність компанії для мене настільки ж важливі, як ціна та якість” [88].

Оцінку корупційних процесів в Україні за допомогою дослідження міжнародних індексів проведемо передусім на основі аналізу індексу сприйняття корупції (Corruption Perceptions Index, CPI) та показника корупції за субіндексом правового та політичного середовища міжнародного індексу прав власності (IPRI). Динаміку зміни цих показників подано на рис. 3.40, рис. 3.41.

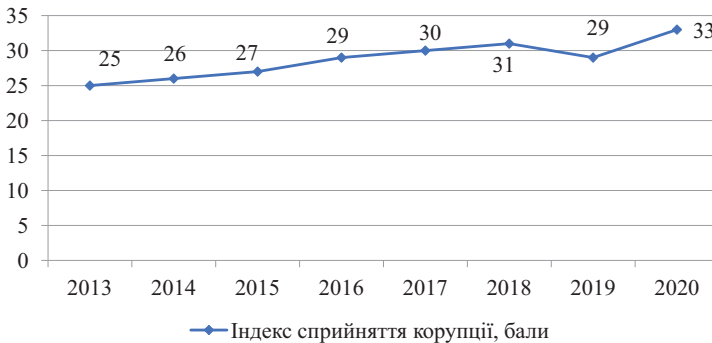


Рис. 3.40. Динаміка зміни індексу сприйняття корупції в Україні впродовж 2013–2020 рр. [86]

Відтак, аналіз зміни індексу сприйняття корупції впродовж 2013–2020 рр. засвідчив незначне зростання цього показника в 2020 р. порівняно з 2019 р. до 33 балів зі 100 можливих, що відповідає 117 місцю із 180 країн у списку CPI [86].

Оцінка міжнародного індексу прав власності (IPRI) за субіндексом політичного та правового середовища, що охоплює показник контролю

над корупцією (табл. 3.5, рис. 3.41) впродовж 2010–2020 рр., показала, що в 2020 р. значення цього показника в субіндексі знизилося порівняно з 2019 р. до 3,253, що відповідає 113 місцю зі 129 країн у списку IPRI [94].

Таблиця 3. 5

**Оцінка корупції в Україні за субіндексом
правового та політичного середовища IPRI**

Показники			
Роки	Контроль корупції	Глобальний ранг	Регіональний ранг
2010	3,563	97/129	22/25
2011	3,200	106/129	23/25
2012	3,000	111/129	23/25
2013	3,000	116/129	23/25
2014	2,900	87/129	11/25
2015	2,816	114/129	24/25
2016	3,010	115/129	25/25
2017	3,040	117/129	25/25
2018	3,318	106/129	21/25
2019	3,432	107/129	21/25
2020	3,253	113/129	25/25

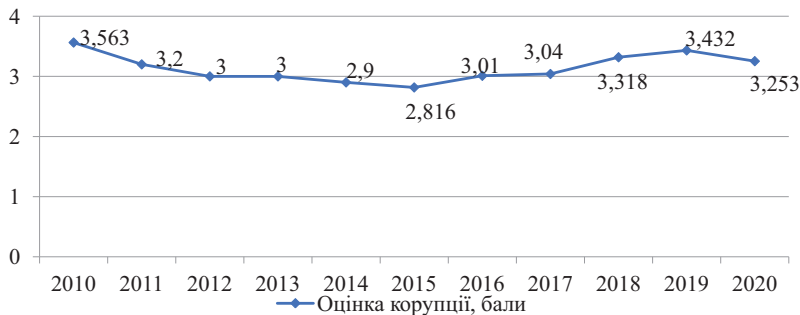


Рис. 3.41. Оцінка корупції за субіндексом правового та політичного середовища IPRI в 2010–2020 рр.

Джерело: сформовано на основі [94]

За допомогою Індексу TRACE Matrix, який розраховує міжнародна асоціація TRACE International для приватного сектора економіки, можна визначити ризик виникнення корупції при здійсненні господарської діяльності в конкретній країні. Індекс відображає результати аналізу корупційних ризиків за такими показниками, як взаємодія бізнесу та

держави, антикорупційне законодавство та контроль за його дотриманням, прозорість діяльності уряду та державних установ, контроль корупції зі сторони громадянського суспільства (див. табл. 3.6, рис. 3.42).

Таблиця 3.6

Індекс TRACE Matrix в Україні впродовж 2014–2020 рр. [91]

Роки	Показники					
	Ранг	Загальна оцінка корупційного ризику, бали	Показник взаємодії бізнесу та держави, бали	Антикорупційне законодавство та контроль за його дотриманням, бали	Прозорість діяльності уряду та державних установ, бали	Контроль корупції громадянським суспільством, бали
2014	132	64	69	52	53	49
2016	133	67	72	56	56	49
2017	127	53	65	36	52	38
2018	105	54	67	53	48	36
2019	122	57	74	54	50	36
2020	98	49	57	59	43	36

Джерело: сформувала автор на основі [91]

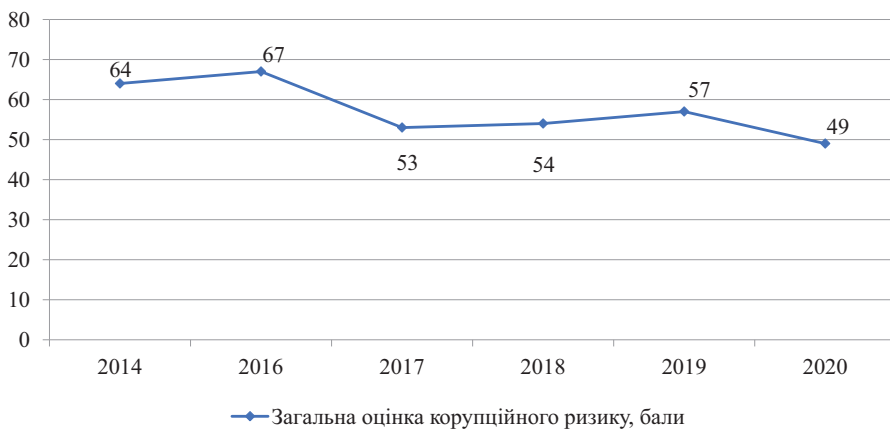


Рис. 3.42. Динаміки зміни Індексу TRACE Matrix в Україні впродовж 2014–2020 рр. [91]

Як видно з даних табл. 3.6 та рис. 3.42, на яких подано динаміку зміни показників Індексу TRACE Matrix в Україні впродовж 2014–2020 рр., в 2020 р. за більшістю параметрів Україна дещо покращила свої позиції порівняно з 2019 р. та загальна оцінка корупційного ризику становила 49 балів (1 бал означає найменший рівень ризику, а 100 – найбільший).

З метою систематизації корупційних дій у підприємницькій діяльності пропонуємо їх поділяти відповідно до таких критеріїв (див. рис. 3.43):



Рис. 3.43. Класифікація корупційних дій у підприємницькій діяльності

Джерело: розробила автор

1) За суб'єктом корупційних дій:

– працівники (менеджери середньої та вищої ланок управління підприємством, рядові співробітники);

– контрагенти (менеджери середньої та вищої ланок управління підприємством, рядові співробітники);

– державні службовці.

2) За періодичністю здійснення корупційних дій:

– корупційні дії постійного характеру;

– нерегулярні корупційні дії.

3) За ініціатором корупційних дій:

– особа, що отримує хабар;

– особа, що пропонує хабар.

4) За видом корупційних дій:

– корупція внаслідок зловживань з конфіденційними даними;

– корупція внаслідок зловживань у сфері закупівель;

– корупція внаслідок порушень нормативних вимог (охорони здоров'я, праці, навколишнього середовища тощо);

– корупція внаслідок зловживань у сфері оподаткування, антиконкурентної, антимонопольної діяльності;

– корупція внаслідок фаворитизму.

Розглянемо прояви корупції в розрізі критеріальної ознаки – за суб'єктом корупційних дій (рис. 3.44).

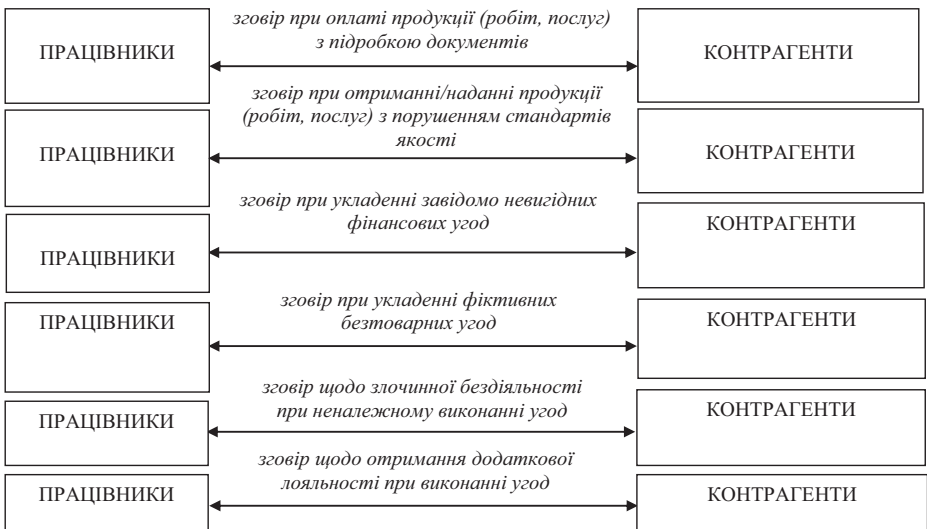


Рис. 3.44. Корупційні взаємозв'язки між працівниками суб'єкта підприємництва і його контрагентами

Джерело: розробила автор

Визначивши можливі корупційні взаємозв'язки між працівниками суб'єкта підприємництва і його контрагентами, дослідимо, які з них були виявлені в діяльності досліджуваних нами підприємств упродовж 2017–2021 рр. (рис. 3.45):

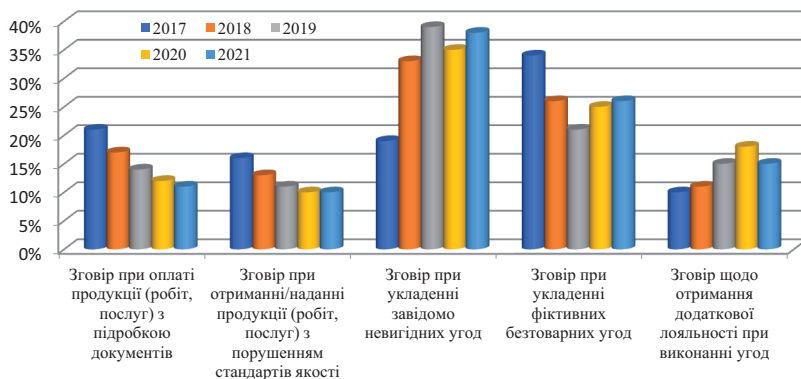


Рис. 3.45. Корупційні взаємозв'язки, виявлені в діяльності досліджуваних суб'єктів підприємництва впродовж 2017–2021 рр.

Джерело : сформувала автор на основі анкетування

Як видно з рис. 3.45, найбільшу частку серед злочинів корупції посідали зговір при укладенні завідомо не вигідних угод та зговір при укладенні фіктивних безтоварних угод.

Наявність випадків корупційної взаємодії працівників суб'єктів підприємництва із контрагентами з метою задоволення власних фінансових інтересів, що порушує інтереси власників, вимагає від керівництва проведення аналізу доброчесності як персоналу, так і благонадійності контрагентів. Однак згідно з дослідженням PwC на сьогодні майже половина опитаних керівників ділових одиниць в Україні не здійснює взагалі або проводить лише неформальну перевірку доброчесності своїх контрагентів [41].

Попри деструктивні наслідки для власників суб'єктів підприємництва, що завдані недобросовісним персоналом, корупція як гібридний фінансовий конфлікт може також сприяти розвитку іншого виду гібридного фінансового конфлікту – недобросовісної конкуренції шляхом порушення конкурентних механізмів ринку. Відтак, корупція дискредитує базові принципи ринкової конкуренції в країні через тіньове отримання

переваг тими учасниками підприємницької діяльності, які використовують корупційні зв'язки. А це своєю чергою спричиняє негативні репутаційні наслідки для держави, відображаючись втратою її позицій у міжнародних індексах, ускладнює партнерські відносини з іншими країнами й міжнародними інституціями, що призводить до скорочення іноземного інвестування, унеможлиблює отримання кредитів.

Отже, запобігання та протидія корупції як гібридному фінансовому конфлікту є складним багатоаспектним процесом як на рівні держави, суб'єктів підприємництва, так і суспільства загалом, що потребує інтеграції спільних зусиль щодо зниження її рівня шляхом реалізації комплексу заходів як на стадії запобігання, так і на етапі реагування на вчинені корупційні злочини.

РОЗДІЛ 4.

ВПЛИВ ДЕСТРУКТИВНИХ ІНСТИТУЦІЙНИХ ТРАНСФОРМАЦІЙ НА ФІНАНСОВУ БЕЗПЕКУ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ

4.1. Інформаційне середовище суб'єктів фінансових відносин як об'єкт захисту

Стрімкі темпи цифровізації економіки, що значною мірою прискорились в умовах пандемії Covid-19, зумовлюють постійне й широкомасштабне використання сучасних інформаційних технологій. Це спрощує та пришвидшує вирішення ділових завдань, створює принципово нові можливості для економічної співпраці, обміну інформацією. Водночас з'являються нові загрози їх конфіденційній інформації, зростає кіберзлочинність, що завдає матеріальних і репутаційних збитків суб'єктам підприємництва.

У контексті забезпечення фінансової безпеки суб'єктів підприємництва в розрізі її інформаційної складової важливим є з'ясування сутності понять “інформація”, “конфіденційна інформація”, “комерційна таємниця”, “комерційні секрети”. Відтак, відповідно до Закону України “Про інформацію” інформацією визначено будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Конфіденційну інформацію визначено цим законом як відомості, що перебувають у користуванні або розпорядженні окремих фізичних чи юридичних осіб, і їх поширюють за бажанням відповідно до передбачених умов [239].

Загалом інформацію суб'єктів підприємництва класифікують за певними ознаками, зокрема [136, с. 183]:

а) за легальністю виділяють:

– легальну інформацію (збирання такої інформації не суперечить законодавству та моральним нормам. Це дані ділових одиниць, які оприлюднюють відповідно до вимог чинного законодавства, рекламні проспекти, продукція і послуги, наукові статті, публікації в засобах масової інформації, галузеві журнали, довідники тощо);

- напівлегальну інформацію (поширення й збирання такої інформації суперечить морально-етичним нормам. Це відомості про переговори з партнерами, взаємовідносини і моральну атмосферу в колективі тощо);

- нелегальну інформацію (секретні дані суб'єкта підприємництва, витік яких завдає йому економічних збитків).

б) за рівнем важливості групують так:

- рівень 1 – життєво важлива інформація, несанкціонований витік якої загрожує функціонуванню суб'єкта господарювання;

- рівень 2 – важлива інформація, ліквідація наслідків витоку якої є складним процесом та пов'язана з великими витратами;

- рівень 3 – корисна інформація, витік якої завдає значної матеріальної шкоди суб'єкту господарювання, однак не загрожує його функціонуванню загалом;

- рівень 4 – несуттєва інформація, витік якої не завдає матеріальних збитків суб'єкту господарювання і не впливає на його функціонування.

Вважають, що інформація, яка належить до перших трьох рівнів важливості, становить комерційну таємницю суб'єктів підприємництва.

Щодо розуміння понять “комерційна таємниця” та “комерційні секрети”, то нам імпонує науковий підхід, який сформулював В. Задірака [83, с. 352], згідно з яким комерційна таємниця – це економічні інтереси, які приховують з комерційних міркувань, та відомості про різні сфери фінансової, виробничо-господарської, управлінської, науково-технічної діяльності суб'єктів господарювання, охорона яких зумовлена інтересами конкуренції та можливою загрозою їх економічній безпеці. Комерційні секрети – форма прояву комерційної таємниці. Вони є інформацією у вигляді документів, схем, виробів, що належать до комерційної таємниці суб'єкта підприємництва, та об'єктом захисту його служби безпеки від можливого зазіхання викраденням, вивідуванням, витоком інформації. Їх необхідно розрізняти за ознаками:

- сферою комерційної таємниці (технологічні, виробничі, фінансові, організаційні, маркетингові, інтелектуальні, рекламні);

- належністю власнику (власність фірми, групи підприємств, окремої особи, групи осіб тощо).

Документам, що містять комерційні секрети, необхідно присвоювати гриф “конфіденційно”, “суворо конфіденційно”, “конфіденційно лише адресату” тощо [83, с. 352].

Секретність в умовах гібридних агресій дає змогу підвищити рівень захисту суб'єктів підприємництва від проявів гібридних фінансових конфліктів. Зокрема врахування цього принципу дає змогу протидіяти недобросовісній конкуренції у формі протиправних дій з прихованого використання торгової марки, підроблення продукції конкурента, оманливої реклами, підкупу, шантажу тощо. З метою запобігання протиправному захопленню секретність допомагає забезпечити захист конфіденційних даних ділових одиниць від їх використання рейдерами для розроблення схем і технологій планової атаки.

Зловмисники зазвичай перехоплюють секретну інформацію суб'єктів підприємництва шляхом несанкціонованого доступу до неї, що, на думку фахівців у сфері інформаційної безпеки [83, с. 352], є незаконним збиранням інформації, яка становить комерційну таємницю, незаконним використанням секретної інформації особою або підприємством, не уповноваженим на це її власником.

Відтак, необхідним елементом захисту конфіденційної інформації є визначення відомостей, що становлять комерційну таємницю та носіїв секретних даних. Тож, пропонуємо під носієм секретних даних розуміти особу, обізану в них (керівників і виконавців, допущених до комерційних секретів). Дані, що становлять комерційну таємницю суб'єктів підприємництва, ми визначили в табл. 4.1.

Таблиця 4.1

Відомості, що становлять комерційну таємницю суб'єкта підприємництва

СФЕРА СУБ'ЄКТА ПІДПРИЄМНИЦТВА	ВІДОМОСТІ, ЯКІ СТАНОВЛЯТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ
ФІНАНСОВА ДІЯЛЬНІСТЬ	Інформація про прибутки (збитки), грошові потоки від операційної, фінансової, інвестиційної діяльності; дані про обсяги й умови кредитування, інформація про інвестиції, дані фінансових бюджетів, фінансові прогнози, банківські рахунки; податкові декларації тощо
РИНКОВІ УМОВИ	Умови договорів, дані про ціни та знижки, специфікацію продукції; обсяг, динаміку й тенденції виробництва; ринкова політика й маркетингова стратегія; відносини зі споживачами, репутація на ринку; інформація про торгових агентів; дані про канали й методи збуту; рекламна стратегія тощо
ВИРОБНИЦТВО	Відомості про технічний рівень обладнання, техніко-економічні характеристики виробів; дані про плановані терміни створення виробів; дані про модифікацію й модернізацію устаткування, виробничі потужності; відомості про організацію виробництва, розміщення й розмір виробничих приміщень і складів; відомості про

Продовження таблиці 4.1

ІННОВАЦІЇ	Відомості про інноваційні технології; стан й характеристики програмного й комп'ютерного забезпечення; дані науково-дослідних робіт тощо
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ	Дані про склад торгових клієнтів, представників і посередників; потреби в сировині, матеріалах, комплектуючих вузлах і деталях, джерела задоволення цих потреб; транспортні й енергетичні потреби
КАДРИ	Відомості про кількість і склад працівників, їхню заробітну платню за посадами, а також про наявність вільних робочих місць
УПРАВЛІННЯ	Відомості про застосовувані й перспективні методи управління; відомості про перемовини щодо злиття; умови продажу; відомості про участь посадових осіб суб'єкта підприємництва в складі інших ділових одиниць, визначення осіб, що ухвалюють важливі управлінські рішення
ІНШІ СФЕРИ	Відомості про систему безпеки, принципи й методи організації захисту комерційної таємниці

Джерело: розробила автор

Розсекречення зазначеної вище інформації може значно зашкодити інтересам суб'єктів підприємництва у випадку заволодіння нею конкурентами, здатними на несумлінну боротьбу на ринку, рейдерами, що можуть мати наміри заволодіти його активами, недобросовісними працівниками з метою задоволення власних фінансових інтересів тощо.

Водночас підприємницька діяльність у сучасних умовах діджиталізації тісно пов'язана з одержанням, нагромадженням, опрацюванням і використанням різноманітних інформаційних потоків, що надходять з різних джерел. Окрім того, конфіденційна інформація кожного суб'єкта господарювання може перебувати у складі таких джерел (рис. 4.1):

Працівники підприємства та суб'єкти його економічного оточення є одним із найважливіших джерел конфіденційної фінансової інформації, оскільки вони можуть одночасно бути джерелом конфіденційної фінансової інформації та суб'єктом зловмисних дій. Це керівники всіх рівнів управління, обслуговуючий персонал, робітники, продавці

продукції, клієнти, партнери, постачальники, покупці тощо. Документи містять усі дані про склад, стан і діяльність будь-якого суб'єкта підприємства, що привертає до них підвищену увагу зловмисників.



Рис. 4.1. Джерела конфіденційної фінансової інформації суб'єктів підприємства

Джерело: розробила автор

Важливим джерелом конфіденційної інформації про ділову одиницю можуть бути публікації в різному вигляді, зокрема книги, статті, матеріали конференцій, семінарів, симпозіумів тощо. Значну частину секретної інформації можна одержати з так званих “відкритих джерел” – преси, передач радіо й телебачення, звітів компаній, внутрішніх видань суб'єктів підприємства, брошур і рекламних проспектів, які поширюють на галузевих ярмарках і спеціалізованих виставках.

До групи технічних засобів забезпечення функціонування суб'єктів підприємства належать телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, кіносистеми, системи часофікації, охоронні й пожежні системи та інші, які за параметрами можуть бути джерелами перетворення акустичної інформації в електричні й електромагнітні поля, здатні утворювати

електромагнітні канали витоку конфіденційної інформації. Особливу групу засобів становлять автоматизовані системи обробки даних, тому що вони володіють великою інформаційною ємністю. У них містяться мільйони й мільярди бітів конфіденційної інформації, витік якої може завдати шкоди суб'єкту підприємництва.

Технічні носії як джерела конфіденційної інформації зумовлені високим темпом зростання парку технічних засобів, що перебувають в експлуатації, їхнім широким застосуванням у всіляких сферах.

Особливим джерелом інформації є продукція, яку виробляє суб'єкт підприємництва, оскільки її характеристики становлять значний інтерес для конкурентів. Кожний етап життєвого циклу нової продукції – від задуму та макета до серійного виробництва – супроводжується специфічною інформацією, що в разі її перехоплення конкурентами може завдати значних збитків суб'єкту підприємництва. Відтак, нова продукція, яку готують до серійного виробництва, має бути об'єктом підвищеного захисту.

Документальні, промислові й виробничі відходи як джерело конфіденційної інформації можуть містити дані про матеріали, їхній склад, особливості виробництва, технології, фінансові розрахунки тощо.

Фахівці у сфері інформаційної безпеки виділяють такі основні канали витоку інформації, що призводить до несанкціонованого отримання і/або модифікації інформації суб'єкта підприємництва [136, с.193–194]:

- канал несанкціонованого доступу (порушник використовує штатні засоби доступу до інформаційних ресурсів, порушує правила розмежування доступу з метою реалізації будь-яких з основних видів загроз для інформації);

- канал спеціального недопустимого регламентом впливу на параметри середовища функціонування з метою порушення доступності в комп'ютерній мережі;

- канал спеціального впливу нештатними програмними і/або програмно-технічними засобами на елементи обладнання, програми, дані та процеси в комп'ютерній мережі, які встановлюють у процесі її експлуатації, з метою реалізації будь-яких з основних видів загроз для інформації;

- канал спеціального впливу на компоненти комп'ютерної мережі за допомогою закладних пристроїв і/або програмних закладок, впроваджених у середовище її функціонування на передексплуатаційних

стадіях її життєвого циклу, з метою реалізації будь-яких з основних видів загроз для інформації;

- канал витоку інформації, утворений за допомогою використання інформативних параметрів побічного електромагнітного випромінювання та наведень з метою порушення конфіденційності;

- канал витоку інформації, утворений за допомогою використання побічних акустoeлектронних перетворень інформативних сигналів у кінцевому обладнанні з метою порушень конфіденційності;

- канал спеціального впливу на компоненти комп'ютерної мережі за допомогою впровадження комп'ютерних вірусів.

Канали поширення інформації можна розділити за формальністю:

- формальні канали (обмін офіційними діловими, науковими й технічними документами за допомогою засобів передавання офіційної інформації (пошта, телефон, інтернет, факс тощо));

- неформальні канали (особисте спілкування, зокрема, зустрічі, переписування, телефонні переговори тощо).

Різноманіття каналів витоку конфіденційної інформації ділових одиниць та значна кількість учасників ринку, з якими в них є конфлікт фінансових інтересів, зумовлює виникнення й поширення загроз інформаційній складовій фінансової безпеки суб'єктів підприємництва. Вважаємо необхідним систематизувати їх за такими ознаками [136, с.187-189]:

1. За природою виникнення:

- об'єктивні (природні), тобто вплив на об'єкт захисту фізичних процесів або стихійних природних явищ, які не залежать від людини;

- суб'єктивні, пов'язані з діяльністю людини. Серед них можна виділити ненавмисні, зумовлені помилковими діями працівників, та навмисні, що є наслідком навмисних дій порушників. Навмисні загрози можуть виникати як зі середини системи (з боку учасників процесу опрацювання інформації), так і ззовні (з боку сторонніх осіб).

2. За метою реалізації:

- загрози, пов'язані з порушенням конфіденційності фінансової інформації;

- загрози, пов'язані з порушенням цілісності фінансової інформації;

- загрози, пов'язані з порушенням (частковим чи повним) працездатності автоматизованих систем опрацювання інформації.

3. За принципом впливу на автоматизовані системи опрацювання інформації (АСОІ) виділяють такі загрози:

- з використанням доступу суб'єкта (користувача, процесу) до об'єкта (файлу даних, каналу зв'язку тощо);

- з використанням прихованих каналів (під прихованим каналом розуміють шлях передавання інформації, який дає змогу двом взаємодіючим процесам обмінюватись інформацією таким способом, що порушує системну політику безпеки).

4. За характером впливу на автоматизовані системи опрацювання інформації (АСОІ):

- активні загрози (призводять до зміни стану системи і можуть здійснюватись або з використанням доступу або як з використанням доступу, так і з використанням прихованих каналів);

- пасивні загрози (здійснюються шляхом спостереження користувачем будь-яких побічних ефектів. Пасивний вплив не веде до зміни стану системи, а пов'язаний лише з порушенням конфіденційності).

5. За способом впливу на об'єкт:

- загрози, що безпосередньо впливають на об'єкт атаки;

- загрози, що впливають на систему дозволів;

- загрози, що мають опосередкований вплив (через інших користувачів) на об'єкт атаки.

6. За об'єктом атаки:

- загрози автоматизованій системі опрацювання інформації (АСОІ) загалом;

- загрози даним або програмам, пристроям, каналам передавання даних;

- загрози процесам і підпроцесам користувачів;

- загрози каналам передавання даних.

7. За використовуваними засобами атаки:

- стандартне програмне забезпечення;

- спеціально розроблені програми.

Компоненти автоматизованих систем оброблення інформації поділяють на такі категорії:

- устаткування;

- програмне забезпечення;

- вихідна інформація;

- співробітники.

Приклади видів загроз безпеці автоматизованих систем опрацювання інформації (АСОІ) наведено в табл. 4.2

Таблиця 4.2

**Приклади видів загроз безпеці автоматизованих систем
опрацювання інформації (АСОІ) [83, с. 242]**

Загрози інформаційній безпеці				
Вид загрози	Об'єкти дій			
	Устаткування	Програми	Дані	Працівники
Розкриття інформації	Крадіжка носіїв, підключення, несанкціоноване використання ресурсів	Несанкціоноване копіювання, перехоплення	Крадіжка, копіювання, перехоплення	Передавання відомостей про захист, розголошення, халатність
Порушення цілісності інформації	Підключення, модифікація, спеціальні вкладення, зміна режимів	Впровадження "троянських коней" та "жучків"	Спотворення, модифікація	Вербування, підкуп працівників
Порушення функціонування інформаційної системи	Зміна режимів, виведення з ладу, руйнування	Спотворення, вилучення, підміна	Видалення, спотворення	Звільнення з посади, фізичне усунення

Від початку здобуття Україною Незалежності в діяльності суб'єктів підприємництва було виявлено значну кількість різноманітних загроз конфіденційній фінансовій інформації. Їх характеристику подано в табл. 4.3.

Таблиця 4.3

**Характеристика типових загроз конфіденційній фінансовій інформації
суб'єктів підприємництва в комп'ютерній мережі**

ЗАГРОЗА КОНФІДЕНЦІЙНІЙ ІНФОРМАЦІЇ	ХАРАКТЕРИСТИКА
НЕСАНКЦІОНОВАНИЙ ДОСТУП	Отримання користувачем несанкціонованого доступу до конфіденційної інформації через неефективний вибір засобів захисту конфіденційних даних, некоректну їхню установку й налагодження
"ЗЛАМ СИСТЕМИ"	Вплив на інформаційну систему, що передбачає проникнення з несанкціонованими параметрами входу

Продовження таблиці 4.3

“МАСКАРАД”	Спосіб порушення захисту інформаційної системи, якому може передувати перехоплення паролів безпеки, виконання будь-яких дій користувачем від імені іншого користувача, якому ці дії дозволені
“ЗБИРАННЯ СМІТТЯ”	Розкриття конфіденційної фінансової інформації через неповне знищення інформації після використання. Дані залишаються в пам’яті і, за умови застосування спеціальних програм, можуть бути відновлені
“ШКІДЛИВІ ПРОГРАМИ”	Програми, які прямо чи опосередковано дезорганізують процес оброблення інформації чи сприяють її розголошенню або спотворенню
“ТРОЯНСЬКИЙ КІНЬ”	Програма, яка виконує не описані в документах додаткові дії в доповнення до основних
“ВІРУС”	Програма, яка може заражати інші програми, включаючи до них модифіковані копії
“ХРОБАК”	Програма, яка поширюється через мережу і не залишає копії на магнітному носії. Найвідоміший представник цього класу – вірус “Morrisa”, який зруйнував мережу Internet у 1988 р.
“ЖАДІБНІ ПРОГРАМИ”	Програми, які під час виконання намагаються монополізувати певний ресурс системи, не даючи змоги іншим програмам використовувати його. Використання такими програмами ресурсів системи, зазвичай, призводить до порушення її доступності
“ЗАГАРБНИКИ ПАРОЛІВ”	Спеціальні програми, призначені для викрадення паролів

Джерело: сформувала автор на основі [83, с. 242]

Основними причинами, що призводять до порушень інформаційної безпеки суб’єктів підприємництва, на нашу думку, є такі: безвідповідальність, самоствердження і корисливий інтерес користувачів. Втрати від кожного виду порушень обернено пропорційні до їхньої частоти. Від порушень, зумовлених недбалістю, потрібний мінімальний захист, від зондування системи – жорсткіший, від проникнень – найбільш жорсткий, поєднаний із постійним контролем.

4.2. Оцінювання впливу персоналу на інформаційну складову фінансової безпеки суб’єктів підприємництва в Україні в умовах гібридних загроз

В епоху цифровізації усіх фінансових процесів, використання формату віддаленого доступу при виконанні працівниками своїх посадових обов’язків, що актуалізувався під час пандемії Covid-19, поширення

гібридних фінансових конфліктів важливим для керівників суб'єктів підприємства є усвідомлення, що загроза витоку конфіденційної інформації найчастіше пов'язана з їхнім власним персоналом, тобто з інсайдерами. Відтак, вивчення типів інсайдерів дає змогу розробити методи протидії їхній деструктивній діяльності, враховуючи індивідуальну специфіку кожного з них. Так, згідно з класифікацією міжнародної науково-дослідної компанії IDC, система інсайдерів має чотири рівні (рис. 4.2).

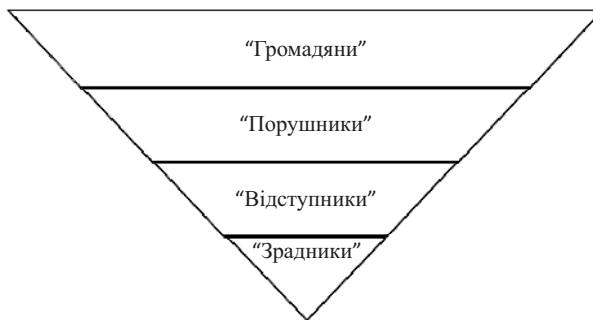


Рис. 4.2. Класифікація інсайдерів згідно з дослідженнями IDC [303, с. 37]

Категорія "громадяни" характеризує службовців, які зрідка порушують корпоративну політику і загалом не загрожують інформаційній безпеці суб'єктів підприємства. Натомість "порушники" становлять значну частку усіх працівників ділової одиниці. Вони здебільшого дозволяють собі в робочий час відволікатися на особисті справи, зокрема, працюють з персональною веб-поштою, комунікують у соціальних мережах тощо. Представники цього рівня інсайдерів генерують загрозу інформаційній безпеці підприємства, проте ці інциденти можна кваліфікувати як випадкові і ненавмисні.

Категорія "відступники" охоплює співробітників, які зловживають своїми привілеями з доступу до Інтернету і можуть передавати конфіденційну інформацію суб'єкта підприємства зовнішнім зловмисникам. Відтак, "відступники" становлять вагомую загрозу інформаційній безпеці суб'єкта підприємства. Однак найвищий рівень інформаційної загрози можуть генерувати співробітники, яких віднесено до категорії "зрадники". Це службовці, які умисно і регулярно чинять

зловживання з конфіденційною інформацією з корисливою метою, зазвичай, за фінансову винагороду від зацікавленої сторони. Існують також й інші підходи до класифікації інсайдерів (табл. 4.4).

Таблиця 4.4

Характеристика інсайдерів компанії, загроз та способів захисту від них [303, с. 39]

Вид інсайдера	Характеристика інсайдера	Деструктивні наслідки	Спосіб захисту
“Недбалий інсайдер”	Найбільш поширений тип внутрішніх порушників. Його порушення щодо конфіденційної інформації мають немотивований характер, не мають конкретних цілей, наміру, користі	Втрата інформації, її розголошення	Централізація роботи Пристроїв управління введенням/виведенням інформації
“Інсайдер, яким маніпулюють”	Співробітники, яких обманним способом залучають до порушень визначених норм. Такі працівники не підозрюють про те, що їхні дії призводять до втрати конфіденційних даних	Ненавмисна передача інсайдерської інформації стороннім особам під впливом “соціальної інженерії”	Централізація роботи Пристроїв управління введенням/виведенням інформації
“Скривджені інсайтери” або саботажники	Співробітники, які прагнуть завдати шкоди компанії з особистих причин	Поширення інформації у ЗМІ, кримінальних структурах, її псування або пошкодження	Централізація роботи Пристроїв управління введенням/виведенням інформації
“Нелояльні інсайтери”	Співробітники, що вирішили змінити місце роботи	Заволодіння інформацією, шантаж керівництва	
“Інсайтери, що вирішили підзаробити”	Працівники, що вирішили продати інсайдерську інформацію замовнику	Передача інформації конкурентам, особам, що готують рейдерське захоплення	Підвищення ефективності роботи служби економічної безпеки
“Впроваджені інсайтери”	Співробітники, які влаштувалися на роботу в компанію з метою здобуття та передавання інформації замовнику		

Згідно з виокремленими в таблиці 4.4 характеристиками інсайдерів, до категорії “недбалий інсайдер”, належать рядові співробітники, які можуть порушити вимоги про конфіденційність інформації через

неуважність. У їхніх діях зазвичай немає корисливого наміру. Для захисту від таких інсайдерів достатньо простих технічних засобів щодо запобігання каналам витоку: централізація роботи пристроїв управління введенням/виведенням інформації і контентна фільтрація вихідного трафіку.

Співробітники, яких віднесено до категорії “інсайдер, яким маніпулюють”, зазвичай чинять порушення під впливом “соціальної інженерії”.

Мотивом розголошення конфіденційної інформації для “скривдженого інсайдера” є особиста помста, наприклад, через образу на директора з огляду на непідвищення по службовій сходіні. Водночас, виділяють також категорію “нелояльний інсайдер”, яка передбачає працівників, незацікавлених у подальшій співпраці, зокрема, тих, що мають намір звільнитися, відкрити власний бізнес або є тимчасовими стажерами. Відмінністю таких інсайдерів від “скривджених” є те, що нелояльні співробітники не приховують факту викрадення інформації, а навпаки використовують його з метою забезпечення вигідного звільнення: з наданням компенсацій, рекомендацій тощо.

Окремо необхідно виділити категорію працівників “інсайдер, що вирішив підзаробити”. Такі співробітники спричиняють витік конфіденційної інформації на замовлення. Мотиви цих інсайдерів можуть бути різними: від бажання заробити значну суму грошей до дій з примусу, коли таких співробітників шантажують ті чи інші структури.

Розглянувши найпоширеніші категорії інсайдерів та їхні мотиви, вважаємо, що найбільшу загрозу становлять працівники “впроваджені інсайдери”. Оскільки такі співробітники зазвичай працюють на замовлення рейдерів та недобросовісних конкурентів, вони, як правило, забезпечені необхідними технічними засобами й навиками, що дає їм змогу подолати всі бар’єри на шляху до отримання конфіденційної інформації ділових одиниць.

Окрім встановлених мотиваційних чинників працівників до зради інтересів суб’єктів підприємництва, корисним є врахування факторів розголошення конфіденційної інформації працівниками суб’єктів підприємництва, що запропонувала І. Шульга (табл. 4.5)

Фактори розголошення співробітниками інформації [303, с.40]

ЧИННИКИ	%
Надмірна балакучість співробітників	32
Прагнення співробітників заробляти гроші будь-якими способами	24
Відсутність на підприємстві служби безпеки	14
Звички співробітників підприємства ділитися інформацією	12
Безконтрольне використання інформаційних систем	10
Наявність можливостей виникнення серед працівників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів, відсутність на підприємстві роботи щодо згуртованості колективу тощо	8

Окрім того, важливо акцентувати, що однією зі суттєвих загроз витоку конфіденційної фінансової інформації та інших супутніх даних, що становлять комерційну таємницю, становлять безпосередньо ІТ-працівники суб'єктів підприємництва, функціональним обов'язком яких є власне забезпечення інформаційної безпеки. На сьогодні існує чимало таких випадків як у вітчизняній, так і в світовій практиці функціонування ділових одиниць. Для прикладу, перед звільненням із Waymo в Uber Е. Левандовські скопіював на особистий ноутбук понад 14 тис. файлів Google, включно із графіками розробки і проектами продуктів. Левандовські частково визнав провину в крадіжці конфіденційної інформації та свою заборгованість перед потерпілим від шахрайства працедавцем у сумі \$179 млн [131].

Згідно з даними компанії Tesla, інженер із автоматизації програмного забезпечення впродовж трьох днів після прийому на роботу почав перехоплювати конфіденційні файли програмного забезпечення із захищеної внутрішньої мережі Tesla й переносити їх у свій особистий обліковий запис хмарного сховища в Dropbox [131].

Враховуючи рівень впливу інформаційної складової на фінансову безпеку в умовах цифровізації фінансових процесів, вважаємо необхідним застосування винятково ретельного й відповідального підходу при прийманні на роботу таких фахівців. Розглянемо характеристику сучасного ІТ-персоналу, який працює на підприємствах, й найпоширеніші ризикові дії зі сторони ІТ-фахівців [69]:

- медіанний вік спеціаліста в сфері ІТ: середній – 28 років;
- стать: 24,9 % – жінки, 75,1 % – чоловіки;
- найпоширеніші ризикові дії зі сторони ІТ-фахівців – загальні службові порушення (55 %); 49 % – причетність до крадіжок; 30 % – дотичність до витоку та розголошення конфіденційної інформації; 39 % – приховування справжніх причин звільнення з попередніх місць роботи; 29 % – контакти із представниками силових структур, органами прокуратури, спецслужб; 32 % – причетність до фальсифікації фінансових звітів.

На сьогодні є безліч каналів передавання секретних даних [136, с. 200]: електронна пошта, соціальні мережі, форуми, блоги, служби миттєвого обміну повідомленнями, зовнішні носії інформації, мобільні пристрої тощо. Так, одним із найпростіших способів розкрадання інформації є переписування даних з локальної мережі суб'єкта підприємництва на зовнішні пристрої. Впровадження в корпоративні ІТ-системи мобільних пристроїв (планшети, смартфони та ін.) завдяки своїм можливостям та компактності значною мірою спрощують вирішення широкого спектра бізнес-завдань. Однак безконтрольність діяльності співробітників на мобільних пристроях у сучасних умовах є неприпустимою через те, що за їхньою допомогою недобросовісні співробітники можуть організувати регулярний витік конфіденційних даних.

Складно контролювати також витік конфіденційної інформації у глобальну мережу Інтернет за допомогою електронних листів, програм для миттєвого обміну текстовими та голосовими повідомленнями, соціальних мереж та блогів, які набули значного поширення в останні роки. У практиці функціонування суб'єктів підприємництва вони допомагають пошуку необхідних кадрових ресурсів, вивченню потенційних партнерів з бізнесу і набору персоналу тощо. Водночас, використання нових способів комунікації призводить до зростання інформаційної вразливості, оскільки працівники можуть використовувати соціальні мережі, блоги, чати для незаконних дій, здатних завдати шкоду репутації та фінансовій діяльності компанії.

Питання моніторингу соціальних мереж працівників є на сьогодні дискусійним, оскільки, з одного боку, це легальний спосіб перевірки інформації, якою діляться працівники суб'єкта підприємництва на

наявність у ній службових даних, з іншого боку, в такий спосіб дещо порушуються етичні принципи та приватність особистого життя співробітників.

З метою аналізу рішення щодо цього дискусійного питання ми проаналізували результати опитування, проведені міжнародною мережею компаній, що пропонує професійні послуги у сфері консалтингу та аудиту “Pricewaterhouse”, які засвідчили, що 58 % респондентів у їхніх організаціях не здійснюють моніторинг відвідування соціальних мереж [41].

Окрім зловживань з порушенням цілісності та конфіденційності фінансової інформації, працівники суб’єктів підприємництва можуть вчиняти такі злочини з використанням інформаційних технологій:

- підроблення звітів;
- фальсифікація платіжних документів;
- крадіжки грошових коштів;
- перерахування грошових коштів на фіктивні рахунки;
- здійснення покупок з фіктивною оплатою;
- повторне отримання уже зроблених виплат.

Аналіз загроз інформаційного середовища, пов’язаних із персоналом, засвідчує, що ігнорування цього вагомого чинника фінансової безпеки призводить до деструктивних наслідків для суб’єктів підприємництва. Несанкціоноване втручання в роботу інформаційних систем, протиправне знищення, спотворення чи оприлюднення конфіденційної інформації, а також різні види фінансового шахрайства, вчинені з використанням інформаційних технологій можуть завдати значних матеріальних збитків діловим одиницям. Окрім того, йдеться не лише про фінансові втрати компаній, а й про різке погіршення іміджу з огляду на неможливість захисту власних конфіденційних даних. Ці проблеми потребують ухвалення ефективних стратегічних рішень у сфері забезпечення інформаційної безпеки та розроблення відповідних заходів з боку менеджменту бізнес-структур.

4.3. Чинник кіберзлочинності в гібридних фінансових конфліктах

Динамічні процеси діджиталізації суспільства характеризуються глибинним проникненням інформаційних технологій у всі сфери глобальної економіки та фінансово-господарські взаємозв’язки окремих

суб'єктів підприємництва. Прискоренню цифрової трансформації сприяла також пандемія COVID-19, оскільки стрімко зріс попит на фінансові операції у режимі онлайн та виникла необхідність здійснення значного обсягу роботи віддалено. Це значною мірою спростило ділову співпрацю учасників ринку, водночас зумовивши зростання ролі кібербезпеки в світі. Враховуючи те, що в глобалізованому бізнес-середовищі одним із основних активів є довіра, неспроможність протидіяти кіберзагрозам може нівелювати інновації у фінансовій сфері. Відповідно до застережень Ради фінансової стабільності МВФ “великий кіберінцидент, якщо він не буде належно стриманий, здатний порушити функціонування фінансових систем, у тому числі критично важливої фінансової інфраструктури, та спричинити масштабні наслідки для фінансової стабільності” [378, с. 25].

Окрім того, в умовах гібридних загроз зловмисники різного рівня, використовуючи інформаційні технології, дестабілізують як фінансові системи країн, так і знижують рівень фінансової безпеки окремих ділових одиниць. Підтвердженням факту, що кіберпростір на сьогодні є середовищем проявів гібридних агресій, є визнання у 2012 році НАТО кіберпростору новим театром воєнних дій [48, с. 44]. Адже гібридні загрози не мають територіального характеру і можуть бути здійснені миттєво з віддалених місць із використанням інформаційних технологій, що ускладнює можливість доведення причетності до них їхніх організаторів. Тому забезпечення кібербезпеки є одним із пріоритетних питань, що розглядається міжнародною спільнотою, про що свідчить прийняття у 2001 р. Конвенції про кіберзлочинність, яку Україна ратифікувала у 2005 р. [118]. У преамбулі цієї Конвенції вказано, що вона “є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва”. Окрім того, виділено такі кіберзлочини [118]:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані, втручання у систему, зловживання пристроями);

- правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами);

- правопорушення, пов'язані зі змістом інформації;

- правопорушення, пов'язані з порушенням авторських і суміжних прав.

В умовах гібридних загроз питання кібербезпеки та кіберзахисту стають пріоритетними цілями державної політики України й політики управління суб'єктів підприємництва, оскільки кіберзлочини стали одним із інструментів боротьби в гібридних фінансових конфліктах як на міждержавному рівні, так і між діловими одиницями.

Відтак, на національному рівні Законом України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 № 2163-VIII визначено такі ключові поняття кіберзлочинності [247]:

- кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

- кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави та кіберзахист її об'єктів;

- кіберзлочин (комп'ютерний злочин) – суспільно небезпечне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена Законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

- кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;
- кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Законодавчо визначено також сутність кібербезпеки та кіберзахисту. Відповідно під кібербезпекою необхідно розуміти захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Кіберзахист передбачає сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Виявлено, що до найпоширеніших кіберзлочинів належали такі: крадіжка особистих даних, вимагання, маніпуляції з персональними даними, неоплата (недоставка), фішинг/вішинг/смішинг/фармінг. Динаміку зміни кількості цих злочинів впродовж 2016–2020 років подано на рис. 4.3.

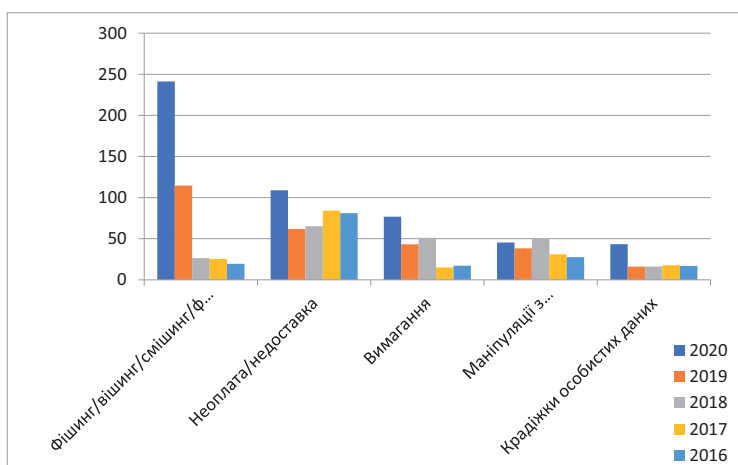


Рис. 4.3. Найбільш поширені кіберзлочини впродовж 2016–2020 рр.

Джерело: сформовано на основі даних [372]

Кіберзлочинність у всьому світі щороку завдає значних фінансових та репутаційних втрат як державам, так і окремим суб'єктам підприємництва. Водночас найбільшу загрозу на сьогодні, на нашу думку, становить використання кібератак у політичних цілях та в гібридних агресіях. Зокрема, росія в гібридній війні використовувала й продовжує використовувати кіберзлочини як вагомий важіль впливу на фінансову безпеку України, намагаючись дестабілізувати інформаційно-технічну інфраструктуру держави та фінансово-економічні процеси в країні. У 2013–2017 рр. кібератаки проти України відбувалися з використанням APT-атак (Snake, Uroboros, Sofacy/APT28, Epic Turla, Black Energy 2 і 3, Armageddon та інші). Перші системні кібератаки були зафіксовані у травні 2014 року на об'єкти української залізниці та сервер ЦВК під час проведення президентських виборів. Тоді ж було здійснено масштабну DDoS-атаку на Дарницьку ТЕЦ [140].

Окрім того, починаючи з 2015 р. відбувалися кібератаки на енергетичний сектор України: у грудні 2015 р. – на ПАТ “Прикарпаттяобленерго” і ПАТ “Київобленерго”; у грудні 2016 року – на ПАТ “Укренерго”. У 2017 р. чимало вітчизняних суб'єктів підприємництва та державних установ зазнала масштабної атаки комп'ютерного вірусу-шифрувальника Petya-A, до якої були причетні спецслужби росії [266; 267].

Деструктивних наслідків хакерської атаки вірусом Petya зазнали такі структури, як: “Київенерго”, “Укртелеком”, “Ощадбанк”, “Нова пошта”, “Укрпошта”, “Приватбанк”, “Укрзалізниця”, аеропорт “Бориспіль”, “Епіцентр”, “Укренерго”, мережа заправок ТНК, ПСГ “Ковальська”, ТРК “Люкс” (24 канал, радіо “Люкс” і ін.), “Антонов”, Київводоканал, Київський метрополітен, Кіберполіція, Нацполіція, Міністерство внутрішніх справ, Міністерство культури, Нацбанк, “Укргазбанк”, “Південний”, “Таскомбанк”, “ОТР банк”, “Кредобанк”, Радіо “Ера-FM”, “КП в Україні”, “Корреспондент.нет”, “Дніпроенерго”, клініка “Борис”, лікарня “Феофанія”, корпорація “Артеріум”. Основною метою цієї кібератаки був збір даних росією про підприємства України.

За результатами аналізу, який був проведений у 2018 р. консорціумом організацій на чолі з Радою зовнішньої політики “Українська призма”,

було розроблено Індекс стійкості до дезінформації. Метою цього дослідження стала оцінка рівня стійкості до іноземних, насамперед російських, дезінформаційних кампаній в 14 країнах Східної та Центральної Європи. Індекс охоплює такі показники [100]:

- схильність і сприйняття контенту проросійських ЗМІ;
- якість системної реакції;
- вразливість до прихованої дезінформації.

Результати аналізу дали змогу виявити, що у групу ризику входили такі країни: Латвія, Білорусь, Україна. Окрім того, з'ясовано, що майже у всіх країнах Центральної та Східної Європи відсутні якісні системні відповіді на інформаційні атаки, як і довгострокові національні стратегії боротьби з іноземними дезінформаційними кампаніями [289].

Аналіз інформаційних інструментів російської гібридної війни від здобуття Україною незалежності до повномасштабного вторгнення дав нам змогу встановити, що перед його початком росією було активізовано кібероперації за допомогою фінансованих нею хакерських угруповань. Суттєво зросла кількість кібератак в інформаційному просторі України від початку війни, зокрема через три дні після початку військової інтервенції росії кібератаки на державно-військовий сектор України зросли на 196 % порівняно з довоєнним періодом [140].

Проведений нами аналіз випадків кібератак українського інформаційного простору впродовж 2022 р. російськими АРТ-групами-хакерськими угрупованнями дав змогу виявити такі [140]:

- кібератака на офіційні web-сторінки уряду та міністерств України (січень 2022 року);
- DDoS-атаки на ЗСУ, сайти міністерств, громадського радіо та банків (лютий 2022 року);
- кібератака об'єктів критичної інфраструктури (березень 2022 року);
- кібератака на українські електромережі (квітень 2022 року);
- кібератака місцевих органів влади, імовірно, з метою шпигунства та викрадення тактичних та стратегічних даних (травень 2022 року);
- кібератака на сайт Державного підприємства “Національна атомна енергогенеруюча компанія “Енергоатом” (серпень 2022 р.).

Згідно з квартальним звітом Державної служби спеціального зв'язку та захисту інформації України у третьому кварталі 2022 р. за

допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій інформаційної безпеки. При цьому кількість зареєстрованих та опрацьованих кіберінцидентів зросла – від 64 до 115 порівняно з попереднім кварталом [89].

Виявлені кіберзлочини передбачали кібершпигунство, порушення доступності державних інформаційних сервісів та знищення даних інформаційних систем. З'ясовано, що кількість подій інформаційної безпеки з високим рівнем критичності зросла у 3,8 раза, кількість зареєстрованих кіберінцидентів із високим рівнем критичності підвищилась на 128 %. Кількість критичних подій інформаційної безпеки, джерелом яких були IP-адреси росії, збільшилась у 35 разів, порівняно з першим та другим кварталами 2022 р. Також порівняно з другим кварталом 2022 р., майже вдвічі зросла кількість детектованих подій інформаційної безпеки, пов'язаних із активним скануванням, джерелом яких є IP-адреси росії, з яких здійснювали кібератаки на українські інформаційні ресурси, розповсюджували дезінформацію, спрямовану на дискредитацію державних органів України [89].

Необхідним у контексті забезпечення фінансової безпеки є врахування основних цілей вчинюваних росією кібератак – фінансовий та комерційний сектори України, що підтверджує значущість та зв'язок фінансово-економічних й інформаційних інструментів гібридної війни й доводить актуальність врахування в гібридних фінансових конфліктах інформаційної складової.

Дослідження вчинюваних кібератак, проведене нами на основі даних Державної служби спеціального зв'язку та захисту інформації України, дало змогу встановити, що більшість кіберінцидентів пов'язана з хакерськими угрупованнями, що фінансуються урядом росії, зокрема, це UAC-0010 (Gamaredon) та інші [89].

Окрім того, виділимо хакерські угруповання, які організують кібератаки на установи України та НАТО – FrozenLake, Coldrive, Summit, FrozenBarentz і FrozenVista. Серед найпоширеніших інструментів кібератак, здійснюваних цими групами зловмисників – фішинг, зокрема атакують пошту Gmail, поштові сервіси різних урядових установ – Міноборони, МЗС та інших державних установ з метою шпигунства, дезінформації, руйнування інформаційних систем. Низка хакерських угруповань, зокрема

проросійська група Killnet, яка поширює політичні ідеї через незаконне використання мереж, постійно атакує об'єкти критичної інфраструктури країн НАТО за допомогою складних DDoS-атак [140].

Аналіз різних категорій зловмисників, що діють в інформаційному просторі України на основі експертних оцінок фахівців у сфері інформаційної безпеки дав нам змогу виокремити серед російських хакерів, які атакують українські державні інформаційні ресурси та критичну інформаційну інфраструктуру, такі групи [22]:

- політично мотивовані кіберзлочинці та військові хакери (кіберзлочинці, які об'єднуються з іншими угрупованнями для здійснення кібератак проти України);

- хакери, яких фінансує уряд росії, більшість із яких є військовослужбовцями, що працюють у спецслужбах країни-агресора.

Попри зростання кіберзлочинності в Україні в умовах війни, можемо констатувати, що кількість кібератак у світі в 2022 р. також зростає майже вдвічі. Перша половина 2022 р. засвідчила значне зростання атак проти всіх галузей економіки – у середньому 605 на день. Найчастіше цілями хакерів ставали державний, фінансовий сектори та медіа – близько 2 600 атак щотижня, що на 44 % більше, ніж у 2021 р. [90].

Важливою характерною рисою сучасної кіберзлочинності є широке використання кіберзлочинців замовниками у відповідних ІТ-фахівців. Відтак, послуги кіберзлочинців є затребуваними в гібридних фінансових конфліктах. Зокрема кіберпростір використовують як середовище для недобросовісної конкуренції. Як інструменти нечесної конкурентної боротьби зловмисники застосовують замовні статті в мережі Інтернет з метою поширення неправдивої інформації про суб'єкт підприємництва-жертву, негативні відгуки або коментарі щодо його діяльності, зокрема за допомогою чат-ботів, фішингові атаки з метою отримання доступу до персональних даних клієнтів.

Ще одним гібридним фінансовим конфліктом, у якому активно використовуються кіберзлочинні інструменти, є рейдерство. Це зумовлено тим, що сучасним протиправним захопленням ділових одиниць в Україні притаманні такі ознаки, як швидкість (через втручання до державних реєстрів), прихованість (труднощі щодо встановлення особи виконавця, що діє через інформаційний простір) та можливість дистанційного впливу на суб'єкт підприємництва-об'єкт агресії без необхідності фізичного

контакту з активами. Зокрема набули поширення випадки несанкціонованого проникнення до баз даних із нелегальним використанням кодів доступу нотаріуса чи реєстратора без їх відома та нелегального доступу до реєстрів шляхом хакерських атак.

Проведений нами аналіз підходів вчених та практиків до протидії загрозам фінансовій безпеці держави і суб'єктів підприємництва в умовах діджиталізації та гібридної війни [78; 128; 145; 169; 295; 367; 375; 377; 378; 383; 384; 385; 394], а також вивчення типів кіберзлочинців (реальних та найманих замовниками), їхніх мотивів і використовуваних інструментів агресії обґрунтовує необхідність групування кіберзлочинців за суб'єктами зловмисних дій, відтак, пропонуємо таку їхню класифікацію (рис. 4.4).

З метою протидії кіберзлочинності та удосконалення процесуальних механізмів притягнення до кримінальної відповідальності за вчинення таких злочинів у 2022 р. було внесено зміни до законів: “Про внесення змін до Кримінального процесуального кодексу України”, Закону України “Про електронні комунікації” з питання підвищення ефективності протидії кібератакам” № 2137-IX від 15 березня 2022 р. та “Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану” № 2149-IX від 24 березня 2022 р. [218, 224]. Внесені зміни до законодавчих актів спрямовані на оптимізацію національної системи кібербезпеки для протидії кіберзагрозам, формування дієвих кримінально-правових механізмів протидії кіберзлочинності, забезпечення безпеки використання цифрових послуг в умовах діджиталізації. Зокрема посилено санкції за такі злочини в інформаційній сфері: [132]: несанкціоноване втручання (ч. 1 ст. 361 ККУ); дії, вчинені повторно або за попередньою змовою групою осіб (ч. 2 ст. 361 ККУ); дії, передбачені ч. ч. 1 або 2 ст. 361 ККУ, якщо вони призвели до витоку, втрати, блокування інформації (ч. 3 ст. 361 ККУ); дії, передбачені ч. ч. 1 або 2 ст. 361 ККУ, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 ККУ); дії, передбачені ч. ч. 3 або 4 ст. 361 ККУ, вчинені під час дії воєнного стану (ч. 5 ст. 361 ККУ); створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ч. 1 ст. 361-1 ККУ).

КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ ЗА ЗЛОВМИСНИКАМИ			
ЗЛОВМИСНИКИ	НАМРИ	ЦІЛІ	ПРОЯВИ
Держави та підконтрольні їм угруповання	Геополітичні, історико-ідеологічні, фінансово-економічні, військово-терористичні	Порушення безпеки інформаційно-технічної інфраструктури держави	кібер-атаки на сервери державних інституцій та об'єкти фінансово-економічної інфраструктури
		Дезінформування населення, а також світової спільноти з метою зниження авторитету держави	викрадення та маніпуляції персональними даними тощо
Суб'єкти підприємництва та наймані ними кіберзлочинці	Фінансово-економічні	Створення небезпеки і завдання суттєвої майнової шкоди державі	дезінформування населення щодо роботи державних органів влади з метою зниження їх авторитету та дискредитації дій, поширення пропагандистської інформації
		Порушення територіальної цілісності держави, окупація її територій	викрадення цифрової інформації
		Фінансова вигода	використання шкідливих комп'ютерних програм для викрадення чи спотворення конфіденційної інформації
Терористичні групи, хактивісти	Фінансово-економічні, ідеологічні	Усунення конкурента з ринку	незаконне стеження за допомогою комп'ютерної техніки
		Протиправне встановлення контролю над фінансово-господарською діяльністю суб'єкта підприємництва тощо	несанкціоноване використання комп'ютерної техніки, зокрема для відключення сигналізації або проведення платежів через інтернет-банкінг
			використання Інтернету та електронної пошти з метою поширення неправдивої інформації про суб'єкт підприємництва-жертву й дискредитації його діяльності
Фінансова вигода; дестабілізація в соціумі	фінансові атаки з метою отримання доступу до конфіденційної фінансової інформації суб'єкта підприємництва, персональних даних клієнтів	викрадення цифрової інформації	
			використання шкідливих комп'ютерних програм для викрадення чи спотворення конфіденційної інформації

Рис. 4.4. Класифікація кіберзлочинів за суб'єктами зловмисних дій

Джерело: розробила автор

Водночас, окрім законодавчого забезпечення протидії кіберзлочинам та роботи відповідних державних органів, у діяльності суб'єктів підприємництва необхідно також розробляти й впроваджувати заходи щодо кіберзахисту. Передусім це стосується розроблення інструкцій для працівників щодо максимально безпечного користування ресурсами кіберпростору, відтак, рекомендуємо такі заходи убезпечення від кіберзагроз в інформаційному просторі (рис. 4.5).

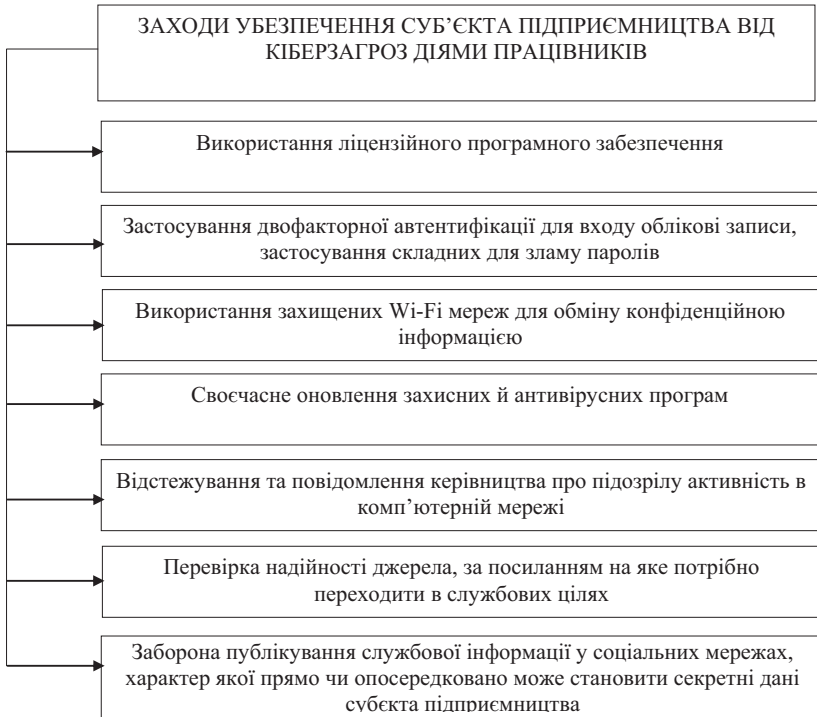


Рис. 4.5. Заходи убезпечення суб'єктів підприємництва від кіберзагроз діями працівників

Джерело: розробила автор

Аналіз злочинів з використанням сучасних інформаційних технологій, що знижує рівень фінансової безпеки суб'єктів підприємництва, зокрема шляхом використання зловживань з інформацією як інструменту в гібридних фінансових конфліктах, дав можливість виявити, що значна їхня частка пов'язана з людським фактором. Це можуть бути зумисні чи помилкові дії працівників, які спричиняють витік конфіденційної

фінансової інформації з внутрішнього середовища підприємства, а також зовнішні кібератаки, які стають можливими через недобросовісність та безвідповідальне поведіння персоналу в інформаційній мережі. Відтак, реалізуючи сукупність заходів із убезпечення працівників від необережних дій у кіберпросторі, можна перетворити вразливості людського ресурсу на ділову перевагу й таким способом підвищити рівень кіберзахисту як необхідної умови забезпечення фінансової безпеки суб'єктів підприємництва.

4.4. Військові агресії як багатомірна криза забезпечення фінансової безпеки суб'єктів підприємництва в Україні

Військова агресія росії спричинила деструктивні наслідки для кожного бізнес-сегменту в країні, спричинивши державні втрати в рекордних обсягах так і втрати потенціалу економіки до зростання в середньостроковій перспективі. Повномасштабний напад росії призвів до різкого зниження економічної активності в Україні, частина суб'єктів підприємництва, що розташовані у зонах активних бойових дій, тимчасово або повністю втрачені, їхня діяльність заблокована, майно розкрадено. Серед основних причин – фізичні руйнування виробничих потужностей та інфраструктури внаслідок масштабних ракетних атак та артилерійських обстрілів, тимчасова окупація низки територій кількох областей, втрата логістичних і виробничих зв'язків, скорочення пропозиції окремих товарів, вимушена масова міграція працівників суб'єктів підприємництва.

За оцінкою аналітиків Міністерства економіки (з використанням непрямих методів розрахунку та інструментів моделювання), зробленою з урахуванням оперативної оцінки Державної служби статистики України реального ВВП за 3 квартали 2022 р. у I кварталі 2022 р. встановлено зменшення порівняно з I кварталом 2021 р. на 15,1 %, у II кварталі 2022 р. – на 37,2 %, у III кварталі 2022 р. – на 30,8 % відповідно [184].

Аналіз характеристики життєдіяльності вітчизняних суб'єктів підприємництва в умовах значного психологічного шоку в перші тижні війни здійснено на основі результатів оперативного опитування 245 власників і керівників підприємств, проведеного Advanter Group та Лігою ділових клубів України станом на 13 березня 2022 р. [183]. Це анкетування було виконано в регіональному розрізі: (Вінниця, Дніпро,

Житомир, Закарпаття, Запоріжжя, Івано-Франківськ, Київ, Львів, Миколаїв, Одеса, Полтава, Ужгород, Харків, Херсон та Чернівці). Характеристику життєдіяльності вітчизняного бізнесу на початку війни подано на рис. 4.6.

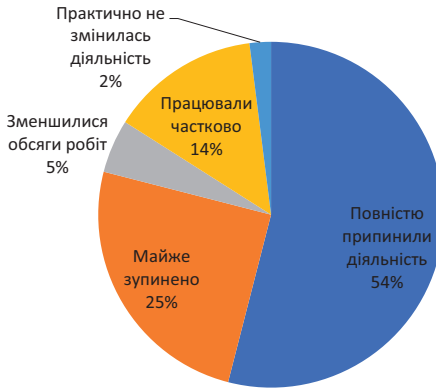


Рис. 4.6. Характеристика життєдіяльності українського бізнесу в умовах війни станом на 13.03.2022 р. від початку війни [183]

Як видно з рис. 4.6, 54 % повністю припинили функціонування, діяльність 25 % ділових одиниць майже зупинено, й лише 2 % підприємств майже не зазнали змін.

Середні втрати суб'єктів підприємництва внаслідок перших тижнів війни подано на рис. 4.7.



Рис. 4.7. Оцінка прямих втрат українського бізнесу з 24.02.2022 р. станом на 13.03.2022 р. [183]

Відтак було виявлено, що для 20 % ділових одиниць втрати становили від 50 тис. дол до 200 тис. дол.; 12 % опитаних підприємств зазнали втрат в діапазоні 10 тис. дол.–50 тис. дол.; розмір втрат 9 % становив від 200 тис. до 1 млн дол.

Згідно з іншими даними опитування, проведеного Європейською Бізнес-Асоціацією після 100 днів від початку повномасштабного вторгнення росії (опитано 101 директорів членських компаній), виявлено такі зміни в підприємницькому середовищі (див. рис. 4.8):



Рис. 4.8. Характеристика життєдіяльності українського бізнесу в умовах війни станом на 26.05.2022–02.06.2022 р. [182]

Дані опитування засвідчили, що лише 47 % підприємств продовжували працювати в повному обсязі, тоді як 50 % функціонували з певними обмеженнями. Окрім того, виявлено, що з 50 % тих суб'єктів підприємництва, які працювали з певними обмеженнями або частково, 37 % – обмежили географію присутності, 17 % – продовжили працювати онлайн, а 16 % були вимушені закрити частину офісів, торговельних точок чи відділень [182].

Щодо оцінки суб'єктами підприємництва своїх фінансових резервів, то згідно з даними опитування (див. рис. 4.9), 34 % оцінювали свою фінансову стійкість у 6 місяців, 20 % вважали, що протримаються кілька місяців, інші 20 % – рік, і ще 19 % зазначали, що фінансових резервів вистачить на період більше року. Водночас, 92 % опитаних компаній не користувалися державними чи міжнародними програмами для підтримки свого бізнесу.

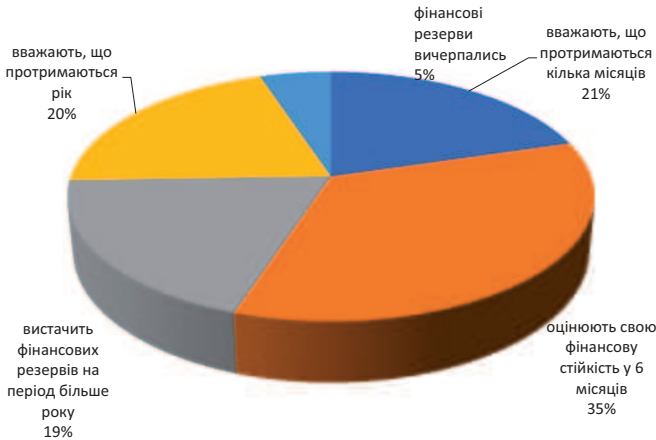


Рис. 4.9. Оцінка фінансових резервів українського бізнесу в умовах війни станом на 26.05.2022–02.06.2022 р. [182]

Унаслідок перших 100 днів активної фази війни 48 % ділових одиниць зазнали до 1 млн доларів втрат, 37 % – у діапазоні 1–10 млн доларів, 12 % – понад 10 млн доларів. Лише 2 % суб'єктів підприємництва не зазнали жодних втрат. Окрім того, встановлено, що 42 % підприємств зазнали втрат майна чи інших активів безпосередньо в результаті бойових дій [182].

Відповідно до даних опитування, на початку війни програмою релокації скористалися 2 % суб'єктів підприємництва, 7 % – перебували в процесі релокації, частково провели – 12 %, не встигли провести – 31 %; близько 48 % ділових одиниць не вбачали вирішення проблеми в релокації. Щодо релокації за кордон, то встановлено, що її здійснили 8 % підприємств від усіх опитаних, 5 % ділових одиниць – планували провести таку релокацію, 31 % на момент дослідження не визначилися з місцем релокації, залишитися в Україні вирішили 41 % підприємств. Втрати ВВП через релокацію підприємств в Україні було оцінено у 9 % [183].

На сьогодні не виявлено єдиної офіційної оцінки впливу воєнних дій на конкретні сектори економіки, водночас ми дослідили певні критичні наслідки для фінансової безпеки підприємств окремих галузей (див. рис. 4.10).

Сектор національної економіки	Основні інфраструктурні деформації галузі та наслідки військової агресії росії	Фінансові наслідки військової агресії росії
Аграрний бізнес	<ul style="list-style-type: none"> окупація та замінування значних площ с/г призначення та їх недосів; закриття морських портів та заблокований експорт продукції; знищення окупантами техніки та вилучення агропродукції в районах активних бойових дій; дефіцит робочої сили в зв'язку з мобілізацією працівників. 	<ul style="list-style-type: none"> дефіцит обігових коштів для закупівлі сировини; зростання цін на сировину та паливе; труднощі зі сплатою орендної плати власникам ділянок, які не були засіяні
Паливний бізнес	<ul style="list-style-type: none"> зупинка поставок з країн-учасників військової агресії; вичерпання внутрішніх резервів через ракетні обстріли та руйнування 20 нафтобаз та Кременчуцького НПЗ 	<ul style="list-style-type: none"> критичне зниження рентабельності через втрату поставок та державне регулювання (до 17.05.2022); дефіцит фінансових ресурсів.
Енергетика	<ul style="list-style-type: none"> залежність країни, крім західних областей від поставок електроенергії з країни-агресора та Білорусі (впродовж перших 3-х тижнів війни); зупинка генерації низки державних та приватних ТЕС та ТЕЦ; знищення чи окупація частини потужностей відновлювальної електроенергії, скорочення кількості її отримання 	<ul style="list-style-type: none"> фінансові втрати від інвестицій в потужності відновлювальної енергії; недоотримання прибутку
Гірничо-металургійний комплекс	<ul style="list-style-type: none"> руйнування чи консервація понад 30–40 % металургійних потужностей України; розкрадання окупантами металу та чавуну; втрата спеціалістів 	<ul style="list-style-type: none"> фінансові втрати від інвестицій в металургійні потужності; зниження продажів продукції, підвищення витрат на альтернативні логістичні схеми постачання сировини
Страховий бізнес	<ul style="list-style-type: none"> суттєві пошкодження офісів та неможливість відновити роботу; зупинення морського та авіа-страхування; ускладнення страхування вантажів; зупинення туристичного страхування та авто страхування. 	<ul style="list-style-type: none"> 2/3 компаній мають скорочення надходжень на 50–90 %, у 80 % – обсяг фінансових надходжень знизився на 50 %; наявність резервів у депозитах та державних облігаціях, що не дозволяє швидко їх конвертувати у кошти; збільшення страхових випадків
Хімічна промисловість	<ul style="list-style-type: none"> призупинення роботи більшості підприємств, втрата виробника сірчаної кислоти у м. Рубіжному, скорочення на 75 % виробничих потужностей у секторі виробництва добрив; знищення внаслідок ракетних обстрілів великих гуртових складів хімічних товарів 	<ul style="list-style-type: none"> втрати від скорочення виробництва та продажів становлять 5–6 млрд дол.; втрати прибутку – майже 600 млн дол.; вартість знищених потужностей – 2 млрд дол (дані Союзу хіміків України, станом на 15.05.22)
Фармацевт. бізнес	<ul style="list-style-type: none"> знищення окремих об'єктів, зокрема складу АТ “Фармак” у Київській області; труднощі з відкриттям аптек у регіонах, де відбуваються бойові дії; міграція співробітників аптечних мереж 	<ul style="list-style-type: none"> прямі втрати галузі невідомі, водночас за даними АТ “Фармак” втрати від знищення складу становили 1,5 млрд грн; зростання витрат на сировину та вартості логістичних послуг
Ритейл	<ul style="list-style-type: none"> руйнування торгових об'єктів внаслідок обстрілів (щонайменше 2 910 торгових точок), втрати у зв'язку з пограбами та мародерством об'єктів на окупованих територіях; збій логістики, дефіцит деяких товарів у виробників, нестача водіїв; складна процедура оформлення імпортованих продуктів, обмежений перелік товарів критичного імпорту. 	<ul style="list-style-type: none"> сумарні збитки від руйнування торгових точок – 1,4 млрд дол., втрати складів – 2 млрд грн, втрати товарів на складах – 3 млрд грн; збій логістики та її подорожчання через відсутність транспорту; зростання вартості доставки продуктів через високу ціну пального; скорочення оборотних коштів, інвестування лише для відновлення пошкоджених активів.

Рис. 4.10. Критичні наслідки війни для фінансової безпеки суб'єктів підприємництва за окремими секторами національної економіки

Джерело: розробила автор

Ми виявили, що суттєвих наслідків унаслідок військової агресії росії в Україні зазнали суб'єкти підприємництва аграрної сфери, передусім, у зв'язку із блокуванням експорту продукції через закриті українські порти. Оскільки сухопутний та річковий експорт у країни ЄС становить менше 20 % спроможності українських портів і менше 35 % від мінімально необхідного темпу місячного експорту в українських сховищах тривалий час залишалися значні обсяги пшениці та кукурудзи. Також на окупованих територіях та в районах активних бойових дій агресором було знищено техніку сільськогосподарських підприємств, відібрано насильницьким шляхом агропромислової продукцію. За даними Мінагрополітики, украдено близько 500 тис. тон збіжжя. Значні площі сільськогосподарського призначення не були засіяні в зв'язку з окупацією чи замінуванням територій. До 09.05.2022 р. в Україні було засіяно 8,6 млн га землі, що на 24 % менше, ніж у 2021 р. [189]. За даними Українського клубу аграрного бізнесу, недосів становив до 4 млн га [188].

Основними причинами критичних наслідків військової агресії росії для фінансової безпеки підприємств аграрної сфери стали, передусім, особливості їхньої діяльності:

- фермерські та польові роботи відбуваються на конкретних територіях, що могли зазнати бойових дій;
- сезонність аграрного бізнесу, що унеможливорює відкладення на невизначений термін або перенесення фермерських та польових робіт; дефіцит робочої сили, в зв'язку з мобілізацією працівників до ЗСУ чи залученням до штабу зон територіальної оборони.

Щодо енергетичній галузі країни, то внаслідок війни було суттєво скорочено кількість електроенергії, отриманої з відновлювальних джерел (сонячна генерація – на 40 %, вітрова – на 70 %, біогазова – на 20 %), оскільки основні потужності відновлювальної енергії розташовані у південних та південно-східних областях України, де відбуваються активні військові дії. До 40 % цих потужностей уже зруйновані чи пошкоджені, знаходяться на непідконтрольній території [46].

Більшість підприємств гірничо-металургійного комплексу зазнало катастрофічних наслідків для їх фінансової безпеки через розташування у південно-східній частині України, де тривають активні бойові дії. Відтак, їх законсервовано чи зруйновано, в окупації перебувають 30–40 %

металургійних потужностей України, зокрема ПАТ Металургійний комбінат “Азовсталь” та ММК ім. Ілліча, дочірнє підприємство АТ “АрселорМіттал Берислав”. Підприємства не можуть відвантажувати готову продукцію через заблоковані порти і морські шляхи (експорт реалізується тільки до ЄС залізницею, пропускна здатність якої не може покрити відсутність морської логістики, та через річкові порти). Окрім того, виявлено значні проблеми з постачанням сировини для окремих підприємств, зокрема, раніше ПАТ “Арселор Міттал Кривий Ріг” отримувало 30 % вугілля з Казахстану, яке відвантажували залізницею через росію. Відтак, в умовах війни підприємство обмежене в спроможності виробництва коксу для металургійного виробництва. Внаслідок військової агресії скоротився попит на металопродукцію на українському ринку [104].

Виявлено, що суттєвих втрат унаслідок військової агресії росії зазнав страховий бізнес в Україні через відсутність в умовах війни морського та авіастрахування в зв'язку із блокуванням морських портів та закриттям авіапростору.

Більшість підприємств хімічної промисловості зупинили виробництво, здебільшого в зоні активних бойових дій і на тимчасово окупованих територіях. Згідно з даними ДП “Черкаський НДІТЕХІМ”, суттєвих руйнувань зазнали близько семи великих та середніх хімічних підприємств. Жоден завод не відновив роботу в повному обсязі, зупинили діяльність 40–50 % суб'єктів підприємництва цієї галузі. Зруйновано виробника сірчаної кислоти у м. Рубіжному, зазнали значних пошкоджень ПрАТ “Северодонецький азот” та ПАТ “Сумихімпром”. У секторі виробництва добрив використовуються лише близько 25 % виробничих потужностей [104].

Можемо констатувати, що єдина галузь, яка виявилася найменш чутливою до кризових трансформацій, спричинених як пандемією Covid-19, так і воєнним станом в Україні – це ІТ-сфера. Так, за даними асоціації ІТ Ukraine, 52 % суб'єктів підприємництва зберегли 100 % укладених контрактів, 32 % – 90–99 % контрактів, 16 % – втратили понад 10 % контрактів. Здебільшого серед підприємств цієї галузі, що зазнали втрат – ті, програмні продукти яких були спрямовані на український ринок [104].

Потребує аналізу сфера паливного бізнесу, окремі суб'єкти підприємництва якої нами досліджено шляхом анкетування на предмет

наявності та протидії гібридним фінансовим конфліктам. Оскільки ця галузь в умовах війни набуває стратегічного значення внаслідок підвищення потреб у нафтопродуктах для ЗСУ, поліції, Державної служби з надзвичайних ситуацій та інших пріоритетних в умовах воєнного стану напрямів роботи. Окрім того, в перші місяці війни попит на паливо почав стрімко зростати з боку аграріїв через початок посівної.

Водночас саме цей вид діяльності зазнав значних кризових явищ на початку війни. Оскільки до повномасштабного вторгнення росії більша частина нафтопродуктів в Україну надходила з країни-агресора та Білорусі. За даними Нафтогазової асоціації України, на зазначені напрями припадало 60 % бензину та 85 % дизпалива. З початком російської військової інтервенції галузь почала переорієнтовуватися на внутрішні джерела, зокрема на Кременчуцький нафтопереробний завод. Водночас упродовж зростання військової агресії росії та потужних ракетних атак інфраструктуру цього нафтопереробного заводу було зруйновано. Окрім того, в перші місяці війни було знищено значну кількість українських нафтобаз. Це своєю чергою призвело до повного вичерпання внутрішніх резервів у країні та гострого дефіциту пального на АЗС. Окрім того, заблокований окупантами морський шлях унеможливив компенсування нестачі пального з інших країн.

Ми проаналізували особливості забезпечення фінансової безпеки суб'єктів підприємництва цієї сфери в перші місяці війни та розробили структурно-логічну схему періодизації організаційно-економічних заходів виходу їх з кризи (рис. 4.11).

На початку війни власники та керівництво досліджуваних суб'єктів підприємства зосередили увагу на забезпеченні фізичного захисту працівників, збереженні товарно-матеріальних цінностей та грошових коштів. Внаслідок панічних настроїв населення було встановлено обмеження добової реалізації продукції та її відпуску на одного споживача. Наступний етап передбачав організаційно-економічну мобілізацію, зокрема акумуляцію фінансових ресурсів шляхом тимчасового замороження всіх виплат грошових коштів суб'єктів підприємства та активізації роботи щодо повернення дебіторської заборгованості. Основні зусилля керівництва були спрямовані на

розроблення варіантів кризової фінансової стратегії відповідно до можливих сценаріїв подальшого розвитку війни.

КРИЗОВІ ЕТАПИ ВІЙНИ	АНТИКРИЗОВІ ЗАХОДИ ОПЕРАТИВНО-ТАКТИЧНОГО РЕАГУВАННЯ		
Початок війни (24.02.2022– 28.02.2022)	Забезпечення безпеки працівників суб'єктів підприємництва		
	Реалізація заходів зі збереження товарно-матеріальних цінностей та грошових коштів суб'єктів підприємництва		
	Лімітування добової реалізації продукції та відпуску на одного споживача в зв'язку з обмеженістю постачання		
Організаційно-економічна мобілізація суб'єкта підприємництва (01.03.2022– 15.03.2022)	Акумуляція фінансових ресурсів шляхом тимчасового замороження всіх виплат грошових коштів суб'єктів підприємництва та активізації роботи щодо повернення дебіторської заборгованості		
	Інвентаризація вцілених активів та оцінювання зобов'язань суб'єкта підприємництва щодо пріоритетності погашення		
	Формування кризового балансу		
	Розроблення варіантів кризової фінансової стратегії відповідно до можливих сценаріїв подальшого розвитку війни		
Переналаштування роботи суб'єкта підприємництва в умовах воєнного стану (01.03.2022– 20.04.2022)	Багаторазова зміна цінової політики		
	Зростання цін унаслідок зміни параметрів формули граничної роздрібною ціни (біржовий курс нафтопродуктів та курс гривні)	Зниження цін внаслідок скасування акцизного податку на продукцію й зниження ставок ПДВ та встановлення нової формули граничної роздрібною ціни	Зростання цін унаслідок зміни параметрів формули граничної роздрібною ціни (біржовий курс нафтопродуктів та курс гривні)
	Переорієнтація на нові джерела постачання		
	Зупинка реалізації для роздрібних споживачів за невігідними регульованими цінами та відпуск переважно корпоративному сектору за договірними цінами		
Гостра криза (20.04.2022– 17.05.2022)	Низька активність нафтотрейдерів-імпортерів через невігідні ціни реалізації		
	Зростання дефіциту палива		
	Лібералізація імпорту продукції з інших країн		
	Зростання маржинального доходу на одиницю реалізованого продукту		
Лібералізація ціноутворення (17.05.2022– 30.06.2022)	Активізація імпорту продукції з інших країн		
	Зростання маржинального доходу на одиницю реалізованого продукту		

Рис. 4.11. Структурно-логічна схема періодизації організаційно-економічних заходів виходу з кризи внаслідок військової агресії досліджуваних суб'єктів підприємства

Джерело: розробила автор

Значним ускладненням для функціонування ділових одиниць були умови державного регулювання, сформовані на методичних засадах

мирного часу, що під час війни втратили свою ефективність. Відтак, цей період часу характеризувався багаторазовою зміною цінової політики, що в поєднанні з дефіцитом запасів пального в країні спричинило гостру кризу. Оскільки відсутність нових налагоджених зв'язків із європейськими партнерами щодо постачання пального, наявність проблем з логістикою та не вигідні регульовані ціни призвели до зупинки реалізації продукції для роздрібних споживачів.

Унаслідок лібералізації ціноутворення 17.05.2022 р. й оперативного реагування на кризу власниками та керівництвом досліджуваних підприємств шляхом налагодження нового партнерства та активізації імпорту продукції з європейських країн, потребу пального на ринку України вдалося швидко забезпечити. Відтак, можемо констатувати, що сукупність антикризових заходів, спільно реалізованих суб'єктами підприємництва та державними органами влади на початку військової агресії значною мірою стабілізували економічну ситуацію.

РОЗДІЛ 5.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА СТРАТЕГІЧНІ ОРІЄНТИРИ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

5.1. Стратегічне оцінювання рівня фінансової безпеки суб'єктів підприємництва в Україні

Попри те, що під час війни засоби оперативно-тактичного реагування стали пріоритетними, власники й керівництво суб'єктів підприємництва, здобувши кількамісячний досвід здійснення фінансово-господарської діяльності в умовах воєнного стану, зіштовхнулись із потребою розроблення й вживання випереджувальних заходів щодо забезпечення фінансової безпеки, спрямованих на збереження їх життєздатності. Це обґрунтовує необхідність формування стратегії розвитку ділових одиниць у складних умовах і розроблення напрямів стратегічного оцінювання рівня їх фінансової безпеки.

Загалом оцінювання фінансової безпеки суб'єкта підприємництва, на нашу думку, передбачає сукупність послідовних дій, тісно взаємопов'язаних між собою з метою аналізу його зовнішнього та внутрішнього середовища щодо виявлення загроз реалізації визначених фінансових інтересів. Якісно виконане оцінювання рівня фінансової безпеки суб'єкта підприємництва дає змогу забезпечити його динамічну фінансову рівновагу та рівновагу в гібридних фінансових конфліктах. Також систематичне виконання такого оцінювання допомагає діловим одиницям протистояти загрозам, здатним завдати матеріальної та моральної шкоди, відтак, сприяє гнучкішому й більш обґрунтованому ухваленню фінансових рішень.

Відтак, вважаємо, що кожен суб'єкт господарювання, враховуючи масштаб й особливості своєї діяльності, повинен розробляти систему оцінювання рівня фінансової безпеки. Водночас, задля того, щоб забезпечити уніфікований підхід до її формування пропонуємо організаційну модель такого оцінювання, що охоплює сукупність заходів на кожному із етапів (підготовчий етап, етап оцінювання, етап фіксування результатів) (рис. 5.1).



Рис. 5.1. Організаційна модель оцінювання рівня фінансової безпеки суб'єктів підприємництва

Джерело: розробила автор

На підготовчому етапі необхідно визначити мету й ключові завдання, об'єкти, суб'єкти, методи, принципи, інформаційне забезпечення та часовий аспект оцінювання рівня фінансової безпеки суб'єктів підприємництва. Тож, метою такого оцінювання вважаємо виявлення деструктивного впливу різноманітних чинників внутрішнього та зовнішнього середовища на фінансову безпеку, встановлення спроможності протидії їм і розроблення та впровадження заходів захисту фінансових інтересів від виявлених загроз, у тому числі випереджувальної дії. Сформульована мета передбачає вирішення таких основних завдань:

- оцінювання фінансового стану і динаміки розвитку суб'єкта підприємництва;
- моніторинг наявності негативних тенденцій розвитку;

- з'ясування причин, джерел, характеру дії та впливу деструктивних чинників на фінансову безпеку суб'єкта підприємництва, в тому числі виявлених проявів гібридних фінансових конфліктів;
- прогнозування наслідків негативного впливу виявлених чинників внутрішнього та зовнішнього середовища на фінансово-господарську діяльність суб'єкта підприємництва;
- розроблення заходів протидії ідентифікованим загрозам та небезпекам.

Відповідно до масштабу та тривалості оцінювання необхідно встановити його вид. Оперативно-тактичне передбачає середньо- та короткострокове оцінювання чинників фінансової безпеки, встановлення їх відповідності стратегічним орієнтирам розвитку, виявлення відхилень досягнутих поточних показників від стратегічних.

Стратегічне оцінювання фінансової безпеки орієнтоване на триваліший період часу та визначення сукупності чинників фінансової безпеки, що характеризують як поточний стан фінансової безпеки суб'єкта підприємництва на основі досягнутих значень фінансових параметрів, так і концептуальних засад розвитку з урахуванням гібридних фінансових конфліктів.

Вагоме значення належить методам оцінювання рівня фінансової безпеки суб'єктів підприємництва, при виборі яких необхідно врахувати не лише визначені об'єкт, мету, завдання, індивідуальні особливості розвитку суб'єкта господарювання, а й ступінь узгодженості обраних методів між собою. Це важливо для підтвердження результатів, отриманих завдяки кільком методам, а також їх порівняння і на цій основі пошук причин розбіжностей та формування узагальнених висновків. Відповідно до сукупності обраних методів дослідження потрібно визначити джерела необхідної інформації, виконати її збирання та опрацювання з подальшим перетворенням у загальний масив даних для оцінювання фінансової безпеки ділової одиниці.

Наступні етапи оцінювання рівня фінансової безпеки суб'єкта підприємництва охоплюють виконання розрахунків, формування на підставі отриманих значень відповідних висновків та відображення результатів у документальній формі. Окрім того, формалізація організаційних процедур оцінювання дасть змогу підвищити ефективність управління фінансовою безпекою суб'єктів підприємництва, зменшити

трудо́ві та часо́ві затрати на його реалізацію, що своєю чергою допоможе зміцнити їхній фінансовий стан, мінімізувати фінансові втрати внаслідок деструктивного впливу чинників внутрішнього та зовнішнього середовища, запобігти протиправним захопленням, випадкам недобросовісної конкуренції чи іншим проявам гібридних фінансових конфліктів.

На основі синтезу наукових поглядів в сфері фінансового менеджменту, стратегічного аналізу, поведінкових фінансів [20; 31; 138; 149] пропонуємо стратегічне оцінювання фінансової безпеки суб'єктів підприємництва здійснювати із врахуванням фінансового та соціально-психологічного підходів, візуальну інтерпретацію чого подано в організаційній моделі (рис. 5.2).

На першому етапі оцінювання необхідно встановити перелік фінансових показників і їхніх оптимальних значень, за яких забезпечується фінансова безпека суб'єкта підприємництва. Також необхідно визначити тенденції зміни значень фінансових показників, за яких забезпечується фінансова безпека суб'єкта підприємництва.

Наступний етап передбачає аналіз виконання визначених вимог фінансової безпеки та бальну інтерпретацію отриманих оцінок фінансових параметрів. Тобто, якщо результуючий фінансовий показник відповідає умові, за якої забезпечується фінансова безпека, його значення трансформується в певну кількість балів, визначену експертами. Якщо досліджуваний показник не відповідає визначеній умові, то його значення трансформується в 0 балів.

Відповідно до встановленого сукупного результативного балу, що відображає значення показника фінансової рівноваги суб'єктів підприємництва (*ПФРСп*) та встановленої шкали значень цього показника можемо присвоїти відповідний рівень фінансової безпеки ділової одиниці.

Разом із оцінкою кількісних фінансових показників на основі фінансового підходу необхідно врахувати й якісні параметри – ефективність протидії гібридним фінансовим конфліктам (соціально-психологічний підхід). Вибір цих показників необхідно проводити відповідно до визначеного переліку найактуальніших для підприємства гібридних фінансових конфліктів. Відтак, наступний етап оцінювання передбачає визначення гібридних фінансових конфліктів, що становлять

загрозу фінансовій безпеці суб'єкта підприємництва та формування експертної групи для оцінювання вагомості та досягнутого значення показників ефективності протидії гібридним фінансовим конфліктам.

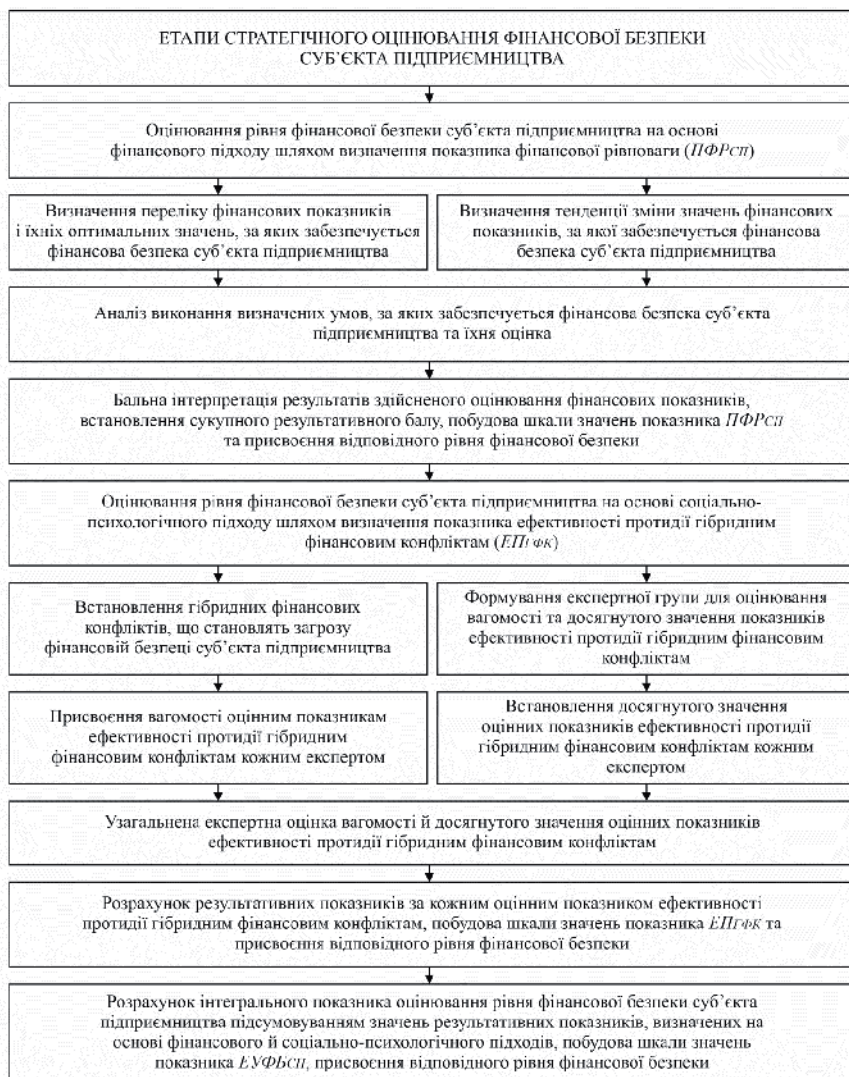


Рис. 5.2. Структурно-логічна схема організаційної моделі стратегічного оцінювання рівня фінансової безпеки суб'єкта підприємництва

Джерело: розробила автор

Узагальнена експертна оцінка вагомості й досягнутого значення оцінних показників ефективності протидії гібридним фінансовим конфліктам дасть нам змогу розрахувати результативні показники за кожним оцінним параметром ефективності протидії гібридним фінансовим конфліктам. На основі встановленої шкали значень показника *ЕПГФК* можна присвоїти відповідний рівень фінансової безпеки суб'єкта підприємництва.

Завершальним етапом стратегічного оцінювання рівня фінансової безпеки суб'єкта підприємництва є визначення загального рівня фінансової безпеки підсумуванням сукупних бальних оцінок кількісних та якісних індикаторів з формуванням шкали значень інтегрального показника й присвоєння відповідного рівня фінансової безпеки – високий, середній, низький.

Отже, рекомендована нами методика стратегічного оцінювання рівня фінансової безпеки розроблена із врахуванням фінансового та соціально-психологічного підходів. Фінансовий підхід передбачає проведення діагностики фінансової рівноваги суб'єктів підприємництва, яка є індикатором забезпечення фінансової безпеки суб'єктів підприємництва. Показник фінансової рівноваги ділових одиниць пропонуємо визначати шляхом оцінювання фінансових показників, досягнуті значення яких упродовж аналізованого періоду часу, є критеріями забезпечення фінансової безпеки суб'єктів підприємництва (*ПФРСП*). Відповідно до соціально-психологічного підходу рівень фінансової безпеки ділових одиниць встановимо за допомогою визначення показника ефективності протидії гібридним фінансовим конфліктам (*ЕПГФК*) за допомогою експертної оцінки. Загальний рівень фінансової безпеки визначимо на основі розрахунку інтегрального показника ефективності управління фінансовою безпекою суб'єктів підприємництва (*ЕУФБСП*).

Відтак, ефективність управління фінансовою безпекою суб'єктів підприємництва (*ЕУФБСП*) визначено за формулами:

$$EУФБСП = \left(\frac{\sum_{i=1}^n c_i}{r} + \frac{\sum_{p=1}^l f_p}{d} \right) / 2; \quad (5.1)$$

$$EПГФК = \sum_{i=1}^n c_i; \quad (5.2)$$

$$ПФРСП = \sum_{p=1}^l f_p; \quad (5.3)$$

$$c_i = \frac{S_i}{m} * \sum_{j=1}^m k_{ij}; \quad (5.4)$$

$$S_i = \frac{1}{m} * \sum_{j=1}^m W_{ij}; \quad (5.5)$$

де c_i – середнє досягнуте значення i -го показника;

S_i – середня вагомість показників протидії гібридним фінансовим конфліктам;

k_{ij} – оцінка значення i -го показника, що дана j -м експертом;

W_{ij} – оцінка вагомості i -го показника, що дана j -м експертом;

$i = \overline{1, n}$, де n – кількість показників протидії гібридним фінансовим конфліктам;

$j = \overline{1, m}$, де m – кількість експертів;

f_p – досягнуте значення фінансового показника;

$p = \overline{1, l}$;

l – кількість фінансових показників;

$f_p = \begin{cases} 0, & \text{якщо умова фінансової безпеки не виконана} \\ 1, & \text{якщо перша умова фінансової безпеки виконана або якщо друга умова виконана,} \end{cases}$

r – кількість поділок у шкалі оцінювання показників протидії гібридним фінансовим конфліктам;

d – кількість поділок у шкалі оцінювання фінансових показників.

За такого підходу найвищий рівень фінансової безпеки суб'єкта підприємництва досяжний за умови, що вся або переважна більшість індикаторів відповідає умові, за якої гарантована фінансова безпека.

Для визначення показника фінансової рівноваги (ПФРСп) ми відібрали показники групи ліквідності (коефіцієнт загальної ліквідності, коефіцієнт критичної ліквідності, коефіцієнт абсолютної ліквідності), фінансової стійкості (коефіцієнт загальної заборгованості, коефіцієнт співвідношення позикового і власного капіталу, коефіцієнт фінансової незалежності), ділової активності (коефіцієнт оборотності дебіторської заборгованості, коефіцієнт оборотності кредиторської заборгованості, коефіцієнт оборотності активів), прибутковості (коефіцієнт рентабельності продаж, коефіцієнт рентабельності активів,

коефіцієнт рентабельності власного капіталу). В умовах мінливості та динамічності чинників ринкового середовища важливим, на нашу думку, є не лише статична оцінка фінансових показників, а й урахування при визначенні фінансової безпеки ділових одиниць тенденції їх зміни впродовж кількох періодів часу. Відтак, у підсумку ми визначили дві умови, за яких забезпечується фінансова безпека – відповідність оцінних показників оптимальним значенням та виявлена тенденція зміни.

Пропоновану методику стратегічного оцінювання ми апробували на суб'єктах підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні. Результати оцінювання фінансових показників кожного із підприємств подано в додатках – МПП “Ірена” (додаток Ж), ТОВ “Західнафтозбут” (додаток И), АТ “Концерн Галнафтогаз” (додаток К), ТОВ “Поділлянафтозбут” (додаток Л), ТОВ “Вест Ойл Трейдинг” (додаток М), ТОВ “ОККО-Бізнес Партнер” (додаток Н).

Показник ефективності протидії гібридним фінансовим конфліктам (ЕПГФК) пропонуємо розраховувати експертним шляхом із урахуванням таких гібридних фінансових конфліктів: протидія корупції, запобігання недобросовісній конкуренції, попередження та ліквідація фінансового шахрайства працівників, запобігання відмиванню доходів, одержаних злочинним шляхом, протидія конфліктам із державними органами, запобігання конфліктам з інститутами фінансово-кредитної сфери, протидія рейдерству, нейтралізація інформаційних загроз. Відтак, на досліджуваних підприємствах, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні, за результатами попередньо проведеного анкетування було здійснено експертну оцінку.

До проведення експертної оцінки було залучено фахівців таких напрямів роботи:

- громадська активність щодо захисту інтересів суб'єктів підприємництва (підхід з позиції громадського моніторингу наявності проявів гібридних фінансових конфліктів у діяльності суб'єктів підприємництва);

- професійні журналістські розслідування проявів гібридних фінансових конфліктів у підприємницькому середовищі (підхід з позиції моніторингу ситуації ЗМІ);

- виявлення та розкриття проявів гібридних фінансових конфліктів державними органами (підхід з позиції державного контролю);
- дослідження стану фінансової безпеки інститутами фінансово-кредитної сфери (підхід з позиції оцінки можливості ділової співпраці).

Результати оцінювання вагомості значення показників ефективності протидії гібридним фінансовим конфліктам у забезпеченні фінансової безпеки суб'єктів підприємництва, встановлені кожним учасником експертної групи, подано в додатку В. Відповідно до узагальненої експертної оцінки встановлено такі значення вагомості для кожного із гібридних фінансових конфліктів (у %):

- протидія корупції – 13 %;
- запобігання недобросовісній конкуренції – 9 %;
- попередження та ліквідація фінансового шахрайства працівників – 17 %;
- запобігання відмиванню доходів, одержаних злочинним шляхом – 19 %;
- протидія конфліктам з державними органами – 14 %;
- запобігання конфліктам з інститутами фінансово-кредитної сфери – 10 %;
- протидія рейдерству – 12 %;
- нейтралізація інформаційних загроз – 6 %.

На наступному етапі експертною групою було проведено оцінювання досягнутого значення показників ефективності протидії гібридним фінансовим конфліктам у діяльності ТОВ “Вест Ойл Трейдинг”, МПП “Ірена”, АТ “Концерн Галнафтогаз”, ТОВ “Поділлянафтозбут”, ТОВ “Західнафтозбут”, ПП “ОККО Бізнес Партнер”. Узагальнені результати оцінювання підприємств подано в додатку Г.

Обчислення результативних показників за кожним оцінним показником на основі соціально-психологічного підходу дало нам змогу розрахувати показник ефективності протидії гібридним фінансовим конфліктам на кожному з досліджуваних підприємств (*ЕПГФК*). Відтак, отримуємо дві складові для визначення загального рівня фінансової безпеки суб'єктів підприємництва – показник фінансової рівноваги (*ПФРсп*), розрахований на основі фінансового підходу, та показник ефективності протидії гібридним фінансовим конфліктам (*ЕПГФК*), визначений експертним шляхом на основі соціально-психологічного підходу. Підсумовуванням значень цих результативних показників розрахуємо інтегральний показник ефективності управління фінансовою безпекою суб'єктів підприємництва (*ЕУФБсп*).

Для присвоєння рівня фінансової безпеки діловим одиницям ми побудували оцінну шкалу отриманих показників *ПФРсп*, *ЕПГфк ЕУФБсп* (табл. 5.1) та визначили рівні фінансової безпеки суб'єктів підприємництва відповідно до запропонованих підходів (табл. 5.2).

Таблиця 5.1

Визначення шкали оцінювання рівня фінансової безпеки суб'єктів підприємництва

Рівень фінансової безпеки суб'єктів підприємництва	Шкала експертної оцінки <i>ЕПГфк</i> , бали	Шкала оцінки <i>ПФРсп</i> на основі аналізу фінансових показників, бали	Шкала визначення <i>ЕУФБсп</i> на основі інтегральної оцінки, %
Низький рівень	0–3	0–4	0%-33%
Середній рівень	4–6	5–8	34%-66%
Високий рівень	7–10	9–12	67%-100%

Джерело: сформувала автор

Таблиця 5.2

Визначення рівня фінансової безпеки суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні

Суб'єкт підприємництва	Оцінка рівня фінансової безпеки					
	На основі експертної оцінки ефективності протидії гібридним фінансовим конфліктам (10-бальна шкала)		На основі аналізу динаміки фінансових показників (12-бальна шкала)		На основі інтегральної оцінки	
	<i>ЕПГфк</i> , бали	Рівень	<i>ПФРсп</i> , бали	Рівень	<i>ЕУФБсп</i> , %	Рівень
ТОВ “Вест Ойл Трейдінг”	7	Високий	3	Низький	48	Середній
МПП “Ірена”	4,7	Середній	9	Високий	61	Середній
АТ “Концерн Галнафтогаз”	8,7	Високий	7	Середній	73	Високий
ТОВ “Поділлянафтозбут”	6,4	Середній	4	Низький	49	Середній
ТОВ “Західнафтозбут”	7,4	Високий	1	Низький	41	Середній
ТОВ “ОККО-Бізнес Партнер”	8,3	Високий	6	Середній	67	Високий

Джерело: сформувала автор

Згідно з отриманими результатами на основі фінансового підходу встановлено високий рівень фінансової безпеки лише в МПП “Ірена”. На підприємствах АТ “Концерн Галнафтогаз” та ТОВ “ОККО-Бізнес Партнер” виявлено середній рівень фінансової безпеки. Результативні фінансові показники ТОВ “Поділлянафтозбут”, ТОВ “Західнафтозбут” та ТОВ “Вест Ойл Трейдінг” дали підстави для висновку про низький рівень їх фінансової безпеки. На основі експертної оцінки ефективності протидії гібридним фінансовим конфліктам ТОВ “Вест Ойл Трейдінг”, АТ “Концерн Галнафтогаз”, ПП “ОККО Бізнес Партнер”, ТОВ “Західнафтозбут” присвоєно високий рівень фінансової безпеки, на МПП “Ірена”, ТОВ “Поділлянафтозбут” встановлено середній рівень фінансової безпеки.

Виявлено, що результати, отримані згідно з фінансовим й соціально-психологічним підходами різняться між собою, що підтверджує відсутність збалансованості між фінансовою та безпековою складовою політики управління на досліджуваних підприємствах та потребує їх узгодження. Відтак, методика стратегічного оцінювання фінансової безпеки ділових одиниць дає змогу вчасно виявити диспропорції в їхній господарській діяльності, що призводять до виникнення та розвитку загроз реалізації фінансових інтересів. Її перевагою порівняно з іншими методами є також те, що завдяки зведенню всіх оцінних показників до єдиного бального стандарту можна охопити й оцінити ступінь впливу як кількісних, так і якісних параметрів розвитку підприємств, виявити проблемні зони й розробити заходи щодо підвищення їх рівня.

5.2. Концептуальні аспекти формування механізму управління фінансовою безпекою суб’єктів підприємництва в Україні в умовах гібридних загроз

В умовах невизначеності ринкового середовища й викликів та загроз фінансовій безпеці ділових одиниць, зумовлених пандемією Covid-19 та війною в Україні, необхідним є розроблення сучасного відповідного новим обставинам функціонування суб’єктів підприємництва механізму управління їх фінансовою безпекою. Водночас управління фінансовою безпекою підприємницьких структур є складним комплексним процесом, що охоплює низку важливих ланок, визначення яких залежить від правильно ідентифікованих об’єктів і суб’єктів управління.

Об'єкти та суб'єкти управління фінансовою безпекою підприємницьких структур показано на рис. 5.3.



Рис. 5.3. Об'єкти та суб'єкти управління фінансовою безпекою ділової одиниці

Джерело: розробила автор

Фінансова безпека суб'єктів підприємництва залежить від належного рівня прибутковості, наявності власних та альтернативних джерел формування фінансових ресурсів, оптимального вибору структури капіталу, синхронності та збалансованості в часі грошових потоків, можливості фінансування реальних та фінансових інвестицій, фінансових інновацій, попередження та мінімізації фінансових ризиків і недопущення фінансових криз на підприємстві. Відтак, загальним об'єктом управління фінансовою безпекою ділових одиниць є фінансова діяльність загалом, а до конкретних об'єктів, залежно від сформульованого завдання, належать різні її параметри: прибуток, джерела формування фінансових ресурсів, структура капіталу, активів і грошових потоків, реальні та фінансові інвестиції, фінансові інновації тощо.

Окрім того, до об'єктів управління фінансовою безпекою суб'єкта підприємництва необхідно зачислити інформаційні та кадрові ресурси, а також компоненти (чинники) його внутрішнього середовища та

підконтрольні підприємству сфери зовнішнього мікросередовища. Адже, якщо це можливо, то підприємство ліквідує, нейтралізує чи мінімізує загрози фінансовій безпеці, реагуючи на дію або впливаючи на чинники свого внутрішнього та зовнішнього середовища. Безпека конфіденційної фінансової інформації полягає в дотриманні її санкціонованості. Водночас необхідною умовою є забезпечення прозорості цих даних для контрольних органів.

Досягнення належного рівня фінансової безпеки суб'єктів підприємництва значно залежить від відповідного рівня фінансової компетентності менеджерів, що виражається в наявності знань і досвіду у сфері фінансового управління та виявляється у здатності працівників фінансової служби виконувати професійні обов'язки, вмінні прогнозувати результати та можливі наслідки різних варіантів управлінських рішень, встановлювати причинно-наслідкові зв'язки. Значущою є також система контролю працівників з метою запобігання фінансовим зловживанням.

Важливими об'єктами опосередкованого впливу при здійсненні управління фінансовою безпекою ділових одиниць є учасники їхнього економічного середовища, що можуть становити загрозу виникнення та розвитку гібридних фінансових конфліктів.

Оскільки діяльність із забезпечення фінансової безпеки суб'єктів підприємництва складається з багатьох напрямів, то її завдання вирішують за допомогою суб'єктів, які функціонують на підприємствах та за їхніми межами. До першої групи належать суб'єкти, які входять до складу організаційної структури ділових одиниць. Це працівники фінансового управління, служби фінансової безпеки, служби безпеки, а також увесь інший персонал, що опосередковано впливає на забезпечення фінансової безпеки суб'єкта підприємництва. У сучасній практиці господарювання суб'єктами управління фінансовою безпекою інколи також є головний економіст та (або) бухгалтер підприємства, оскільки самостійного підрозділу чи спеціалістів з цього кола питань у них немає. Певною мірою виконання функцій фінансового менеджера й економіста чи бухгалтера однією особою можна виправдати на невеликих підприємствах з незначними масштабами господарської діяльності. Однак в інших випадках це свідчить про те, що вітчизняні власники та керівники суб'єктів підприємництва на сьогодні ще не до кінця усвідомили важливість управління їх фінансовою безпекою, що в умовах нових викликів і загроз може мати значні деструктивні наслідки для діяльності.

Друга група – це суб’єкти, які перебувають за межами суб’єктів підприємництва і не підпорядковані їхньому керівництву. Це перш за все державні органи, які створюють умови гарантування фінансової безпеки ділових одиниць. Серед суб’єктів недержавних структур, діяльність яких стосується гарантування фінансової безпеки підприємництва, необхідно виділити Антирейдерський союз підприємців України, основні завдання якого такі: збереження вітчизняного промислового потенціалу; протидія незаконному переділу власності, моніторинг та аналіз практики протидії протиправним поглинанням, забезпечення допомоги підприємствам, які їх зазнали. Крім того, у недержавному секторі функціонують приватні охоронні служби, детективні агентства, інформаційні центри, консультативні організації, які надають послуги з розроблення та реалізації заходів, спрямованих на досягнення належного рівня фінансової безпеки суб’єктів підприємництва.

Враховуючи те, що управління фінансовою безпекою суб’єктів підприємництва повинно реалізовуватися як на макро-, так і на мікроекономічному рівні, виокремимо такі його основні функції (рис. 5.4).

ФУНКЦІЇ УПРАВЛІННЯ ФІНАНСОВОЇ БЕЗПЕКИ СУБ’ЄКТІВ ПІДПРИЄМНИЦТВА			
ФУНКЦІЇ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ НА РІВНІ СУБ’ЄКТІВ ПІДПРИЄМНИЦТВА	Ідентифікація загроз фінансовій безпеці	Забезпечення добросовісної конкуренції і прозорого механізму ціноутворення	ФУНКЦІЇ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ НА РІВНІ ДЕРЖАВИ
	Формування системи заходів із запобігання загрозам фінансовій безпеці й управління ризиками	Протидія механізмам нелегального перерозподілу власності	
	Ліквідація негативних наслідків, спричинених ризиковими ситуаціями	Стимування формування фінансових пірамід	
	Забезпечення захищеності майна	Запобігання корупції	
	Захист конфіденційної фінансової інформації	Протидія зловживанням у сфері оподаткування	
	Забезпечення захищеності керівного апарату підприємства та всіх інших його працівників	Захист інтересів власників	
	Протидія гібридним фінансовим конфліктам	Мінімізація фінансового шахрайства	

Рис. 5.4. Функції управління фінансовою безпекою суб’єктів підприємництва

Основними вимогами до управління фінансовою безпекою суб'єктів підприємництва в Україні повинні стати: захищеність підприємницького середовища посиленням відповідальності держави, альтернативність політики сприяння й розвитку підприємництва, внутрішня збалансованість основних параметрів фінансової безпеки підприємництва.

На наш погляд, управління фінансовою безпекою на рівні суб'єктів підприємництва можна реалізувати, планомірно й системно здійснюючи усі необхідні організаційно-економічні заходи на кожному з таких етапів (рис. 5.5).

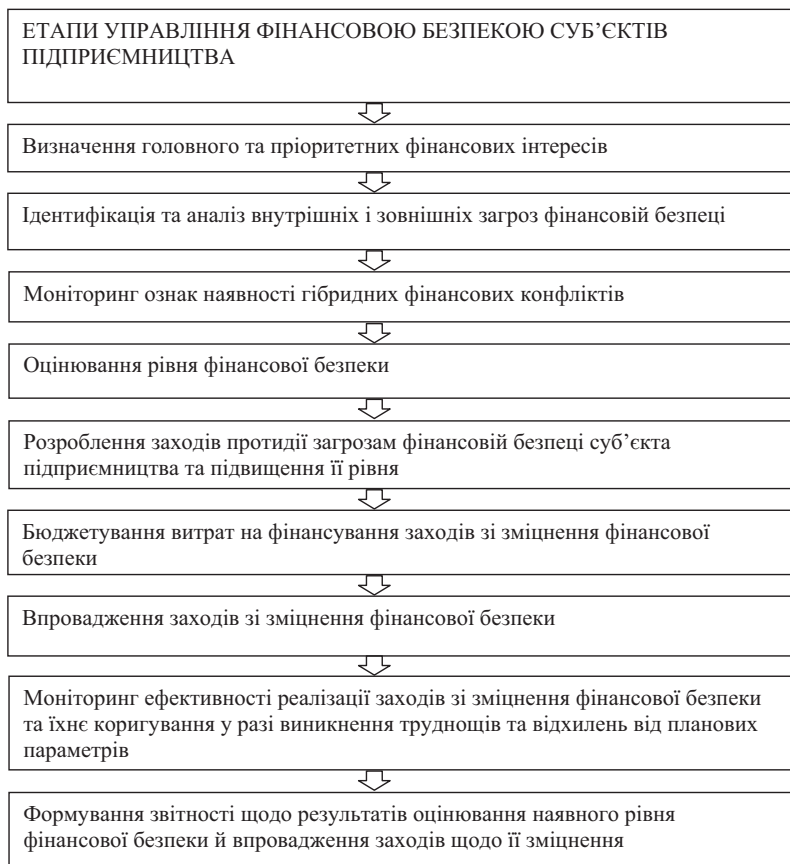


Рис. 5.5. Структурно-логічна схема управління фінансовою безпекою суб'єктів підприємництва

Джерело: розробила автор

Відтак, на першому етапі необхідно визначити головний та пріоритетні фінансові інтереси ділової одиниці та сформулювати завдання щодо реалізації стратегії й тактики їхнього захисту.

Другий етап передбачає визначення внутрішніх та зовнішніх загроз фінансовій безпеці суб'єктів підприємництва, їхнє ранжування за об'єктивним та суб'єктивним спрямуванням, сферою виникнення, ступенем значущості, способом виникнення, характером прояву та іншими важливими критеріями для кращого розуміння й розроблення заходів протидії кожній із них. Також цей етап охоплює визначення причин виникнення загроз та аналіз їхнього впливу на фінансову безпеку суб'єкта господарювання.

Важливим етапом управління фінансовою безпекою суб'єктів підприємництва є моніторинг проявів гібридних фінансових конфліктів. Така робота повинна відбуватися на постійній основі з розробленням сценаріїв впровадження організаційно-економічних заходів щодо ідентифікації кожного із таких конфліктів – фінансового шахрайства, рейдерства, недобросовісної конкуренції, корупції та ін.

Необхідним є також оцінювання рівня фінансової безпеки суб'єктів підприємництва та визначення регулярності його здійснення відповідно до масштабу та часового аспекту, відтак, має бути встановлена періодичність оперативного-тактичного та стратегічного оцінювання.

Наступний етап полягає в розробленні заходів протидії загрозам фінансовій безпеці суб'єкта підприємництва та способів підвищення її рівня. У цьому контексті необхідно визначити організаційне, інформаційне і технічне забезпечення їхньої реалізації, зокрема, підготовку професійних кадрів у сфері управління фінансовою безпекою, навчання працівників правил дотримання комерційної таємниці підприємства, правил роботи з документацією і технічними засобами; створення підрозділу управління фінансовою безпекою, встановлення технічних засобів захисту тощо. На цій стадії управління важливим є також пошук ресурсного забезпечення впровадження таких заходів й бюджетування відповідних витрат.

Після впровадження запланованих заходів зі зміцнення фінансової безпеки суб'єкта підприємництва, необхідним є постійний моніторинг їх реалізації та фіксування як результатів оцінювання наявного рівня фінансової безпеки, так і стану впровадження заходів щодо її зміцнення у відповідному управлінському звіті.

Вважаємо, що при здійсненні управління фінансовою безпекою суб'єктів господарювання на кожному із його етапів необхідно дотримуватися таких принципів (рис. 5.6).

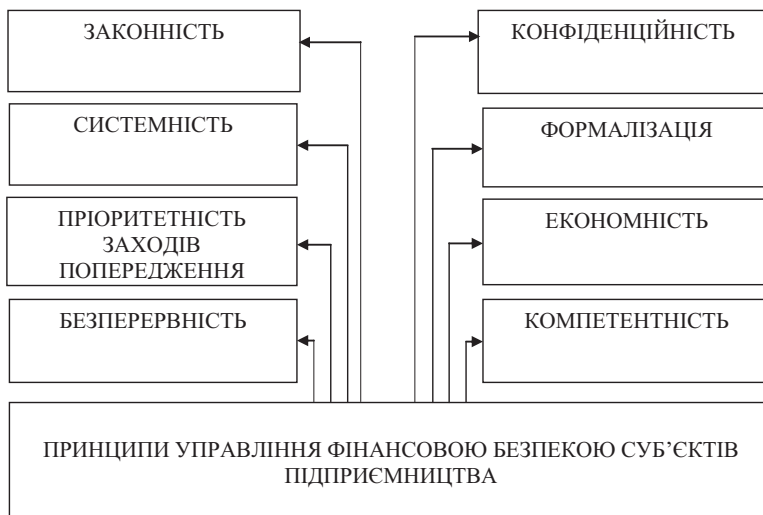


Рис. 5.6. Принципи управління фінансовою безпекою суб'єктів підприємництва

Джерело: розробила автор

1. Принцип законності. Усі дії з управління фінансовою безпекою суб'єктів підприємництва повинні відбуватися на підставі чинного законодавства й не суперечити йому. Внутрішні нормативні документи ділових одиниць повинні ґрунтуватися на чинних правових актах.

2. Принцип системності. Управління фінансовою безпекою повинно передбачати поєднання та взаємоузгодження кадрового потенціалу, інструментів, методів і заходів, що задіяні спеціальними службами суб'єкта підприємництва для забезпечення захисту його інтересів від зовнішніх і внутрішніх загроз. Ідейною основою такого системного використання різних ресурсів повинна стати Концепція зміцнення фінансової безпеки ділової одиниці та концептуальні документи в розрізі окремих важливих її складових, що регламентують політику із протидії фінансовому шахрайству, рейдерству, недобросовісній конкуренції, корупції тощо.

3. Принцип пріоритетності заходів попередження передбачає виявлення різних деструктивних чинників до того, як вони завдали шкоди суб'єкту підприємництва, вжиття заходів щодо запобігання їхньому негативному впливу.

4. Принцип безперервності означає, що заходи з управління фінансовою безпекою потрібно реалізовувати так, щоб забезпечувати постійний захист фінансових інтересів ділових одиниць в умовах ризиків.

5. Принцип формалізації передбачає організаційне й нормативне забезпечення управління фінансовою безпекою та дає змогу кожному учаснику процесу діяти послідовно, чітко виконуючи покладені на нього обов'язки та вирішуючи поставлені перед ним завдання. Діяльність із управління фінансовою безпекою потрібно вести на засадах єдиного підходу, визначеного в конкретних інструкціях та планах за окремими напрямками.

6. Принцип економності означає, що управління фінансовою безпекою має відбуватися так, щоб витрати на його реалізацію були економічно доцільними, а їхня сума не перевищувала того рівня, за якого втрачається їхнє економічне значення.

7. Принцип конфіденційності передбачає, що усі заходи з управління фінансовою безпекою суб'єктів підприємництва повинні бути секретними.

8. Принцип компетентності полягає в тому, що управлінням фінансовою безпекою ділових одиниць повинні займатися професіонали, які знають та розуміють суть проблеми повною мірою, уміють своєчасно оцінити ситуацію й ухвалити правильне рішення. До уваги потрібно брати рівень фінансової компетентності всього управлінського персоналу, а також зовнішніх консультантів, які впливають на діяльність суб'єктів господарювання.

Врахування такої сукупності принципів управління фінансовою безпекою суб'єктів підприємництва дасть змогу забезпечити реалізацію їхніх стратегічних й оперативно-тактичних цілей і визначених завдань функціонування.

Управління фінансовою безпекою суб'єктів підприємництва є динамічним багатоаспектним процесом, що передбачає багатоваріантність фінансово-господарських рішень, які коректують відповідно до мінливих умов ринкового середовища. Рішення та заходи з управління фінансовою безпекою, що розроблені та є ефективними для однієї ділової одиниці, можуть бути абсолютно недоцільними – для іншої. Попри те, необхідним є формування своєрідного “кістяка” управління, який визначає головні

аспекти управління – механізм управління фінансовою безпекою суб'єктів підприємства.

Вивчення підходів вчених щодо формування системи забезпечення фінансової безпеки суб'єктів підприємства, в тому числі методів антикризового фінансового управління та заходів попередження загроз функціонуванню ділових одиниць [5; 29; 66; 114; 174], дало змогу визначити механізм управління фінансовою безпекою суб'єктів підприємства як систему взаємопов'язаних між собою елементів, яка визначає і забезпечує реалізацію комплексу заходів на кожному з етапів управління фінансовою безпекою. Оскільки таке управління є підсистемою фінансового механізму суб'єкта господарювання, то механізм його забезпечення, на нашу думку, повинен формуватися через систему управління фінансовими відносинами з використанням певних фінансових методів і важелів, організаційно-правового, інформаційного й програмно-технічного забезпечення (рис. 5.7).

Суб'єкти управління фінансовою безпекою ділових одиниць впливають на об'єкти управлінського впливу за допомогою певних методів. Виділяють правові, економічні, організаційно-технічні та соціально-психологічні методи.

У межах правових методів забезпечення фінансової безпеки суб'єктів підприємства передбачається створення інструкцій про матеріальну відповідальність і захист комерційної таємниці, моніторинг законодавства та захист від протиправних дій і рішень органів державного управління. Методи правового регулювання полягають також в укладенні безпечних договорів із контрагентами, належній реєстрації документів, прав власності тощо. Забезпечення фінансової безпеки економічними методами повинно бути спрямоване на підвищення ефективності використання фінансових ресурсів ділових одиниць, зокрема, управління його активами, грошовими потоками, інвестиціями, прогнозування банкрутства тощо.

За допомогою організаційно-технічних методів відбувається формування організаційної структури управління фінансовою безпекою суб'єктів підприємства, визначення повноважень та відповідальності посадових осіб, розпорядку роботи, порядку дій у тій чи іншій ситуації.

Відтак, до чинників, які визначають таку організаційну структуру, відносимо такі: вид і масштаби економічної діяльності, організаційно-правова форма, специфіка ринку, притаманна здійснюваній діяльності

суб'єкта підприємництва, досягнутий рівень його фінансової безпеки, кількість і професійно-кваліфікаційний рівень працівників, можливість фінансового та іншого ресурсного забезпечення управління його фінансовою безпекою.

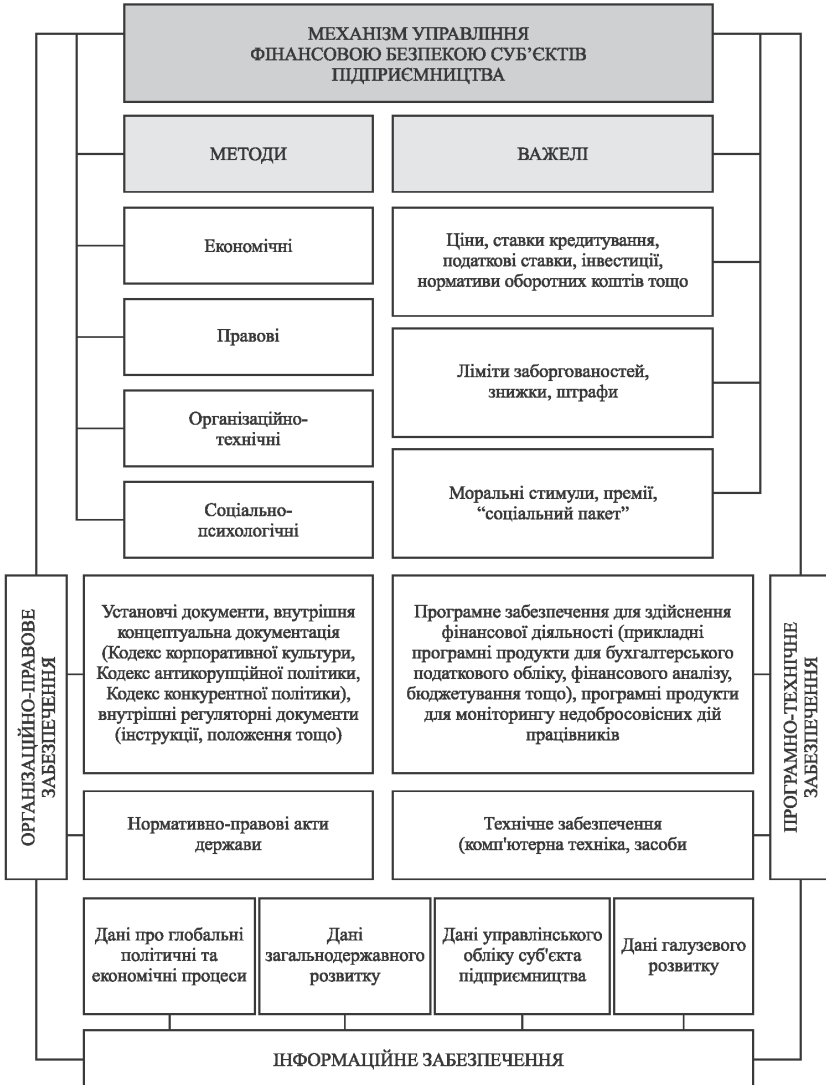


Рис. 5.7. Механізм управління фінансовою безпекою суб'єктів підприємництва

Джерело: розробила автор

Організаційно-технічні методи повинні охоплювати уведення в діяльності суб'єктів підприємництва режимів входу/виходу персоналу та відвідувачів; створення перешкод для доступу до майна, захист конфіденційної фінансової інформації тощо. Ці методи передбачають створення механізму оперативного реагування на загрози інформаційній безпеці та поширення негативної інформації в ЗМІ. Група цих методів така: аналіз, облік комерційної інформації; створення надійної системи захисту інформації та каналів її проходження; використання сучасних технологій захисту інформації (систем кодування і шифрування).

Використання соціально-психологічних методів передбачає вжиття заходів матеріального стимулювання, створення ефективної системи морального заохочення працівників, підбір кадрів з урахуванням їхніх психологічних характеристик, забезпечення соціального й професійного зростання, укладання договорів, створення атмосфери корпоративного духу, формування сприятливого морально-психологічного клімату в колективі.

В управлінні фінансовою безпекою ділових одиниць необхідно застосовування всіх зазначених груп методів управлінського впливу, які важливо реалізувати комплексно, безперервно й, за необхідності, ситуативно.

Кожному економічному методу відповідають певні економічні важелі (ціни, кредитні ставки, валютний курс, ставки податків, нормативи оборотних коштів, ліміт залишку грошових коштів тощо). Крім того, виділяють такі важелі управлінського впливу, як сукупність стимулів та заохочень для менеджерів за ухвалення ефективних управлінських рішень і штрафних санкцій за негативні наслідки їхніх дій у сфері фінансової безпеки.

Організаційно-правове забезпечення управління фінансовою безпекою суб'єктів підприємництва передусім охоплює організаційне забезпечення, що становить сукупність взаємопов'язаних обов'язків та повноважень внутрішніх структурних служб і підрозділів підприємства, які розробляють та ухвалюють рішення з управління їх фінансовою безпекою.

З метою документального затвердження організаційних аспектів у діяльності ділових одиниць доцільно формувати відповідні регуляторні документи, зокрема Положення про політику управління фінансовою безпекою, Положення про службу фінансової безпеки тощо, Кодекс

корпоративної культури, Кодекс антикорупційної політики, Кодекс конкурентної політики тощо.

Правове забезпечення управління фінансовою безпекою суб'єктів підприємництва повинно охоплювати нормативно-правові акти України, що регулюють їхню фінансово-господарську діяльність загалом (започаткування діяльності, кредитування, оподаткування, інвестування та ін.) та ті, які регламентують захист інтересів власників, конфіденційної фінансової інформації, захист від недобросовісної конкуренції, регулюють механізм банкрутства, визначають відповідальність за фінансове шахрайство тощо.

Інформаційне забезпечення в механізмі управління фінансовою безпекою ділових одиниць полягає у своєчасному формуванні й використанні повної та вірогідної інформації для ухвалення управлінських рішень. Зовнішні та внутрішні дані в системі управління фінансовою безпекою потрібно аналізувати й трансформувати у відповідні рекомендації, рішення, звіти.

Інформаційне забезпечення має містити якісні та кількісні параметри формування й використання фінансових ресурсів, операційні та фінансові бюджети, індикатори фінансової безпеки тощо. Воно формується на основі даних бухгалтерського, управлінського та статистичного обліку і звітності, світових, загальнодержавних, та галузевих показників.

Фінансово-господарська діяльність суб'єктів підприємництва є складним та трудомістким процесом, під час якого відбувається збирання та опрацювання великої кількості даних. Необхідність упорядкованості цих інформаційних потоків зумовлює потребу в якісному програмно-технічному забезпеченні. Відтак, у діяльності суб'єктів підприємництва з метою забезпечення їх фінансової безпеки необхідним є застосування прикладних програмних продуктів для здійснення бухгалтерського і податкового обліку, фінансового аналізу, бюджетування, моніторингу недобросовісних дій працівників тощо.

Застосування в діяльності суб'єктів підприємництва як основи управління їхньою фінансовою безпекою пропонованого механізму взаємопов'язаних між собою методів, важелів, організаційно-правового, програмно-технічного й інформаційного забезпечення дасть змогу забезпечити захист їх фінансових інтересів від внутрішніх і зовнішніх викликів і загроз, у тому числі проявів гібридних фінансових конфліктів.

5.3. Типові сценарії впровадження організаційно-економічних заходів протидії гібридним фінансовим конфліктам в діяльності суб'єктів підприємництва в Україні

Значне поширення гібридних фінансових конфліктів у практиці функціонування суб'єктів підприємництва та встановлені нами фактори впливу на їх виникнення, ознаки за якими можна їх ідентифікувати та вивчені тенденції розвитку дали змогу розробити організаційні моделі реалізації політики протидії кожному із досліджуваних конфліктів. Відтак, передусім, схарактеризуємо організаційні засади вирішення завдання протидії такому гібридному фінансовому конфлікту, як фінансове шахрайство. З цією метою пропонуємо використовувати розроблену нами організаційну модель (рис. 5.8).

Перший етап запропонованої моделі – підготовчий, на якому необхідно визначити мету, завдання, об'єкти, суб'єкти та принципи протидії фінансову шахрайству в діяльності ділових одиниць. Метою протидії фінансовому шахрайству в діяльності кожного суб'єкта підприємництва є зниження рівня злочинності, досягнення позитивних змін у її динаміці і структурі шляхом нейтралізації чинників, що зумовлюють її виникнення, розвиток і поширення.

Сформульована мета передбачає вирішення таких завдань: виявлення причин фінансового шахрайства й умов, що їм сприяють; вжиття заходів з їх усунення або нейтралізації; встановлення осіб з деструктивною поведінкою, схильних до фінансового шахрайства; застосування заходів організаційного та психологічного впливу на працівників з деструктивною поведінкою; обмеження дії негативних явищ і процесів, супутніх фінансовій злочинності на підприємстві; усунення виявлених недоліків у роботі суб'єктів протидії фінансовому шахрайству з метою підвищення її ефективності.

Загальним об'єктом протидії фінансовому шахрайству в діяльності ділових одиниць є фінансова діяльність загалом, а до конкретних об'єктів, залежно від сформульованого завдання, належать різні її параметри: фінансові ресурси, фінансова інформація, активи підприємства. Суб'єктами протидії фінансовому шахрайству є власники, керівництво, Служба фінансової безпеки та усі інші служби й кожен працівник суб'єкта підприємництва.



Рис. 5.8. Організаційна модель реалізації політики протидії фінансовому шахрайству

Джерело: розробила автор

На наш погляд, робота з протидії фінансовому шахрайству в підприємницькій діяльності повинна організовуватись із врахуванням таких принципів (рис. 5.9):

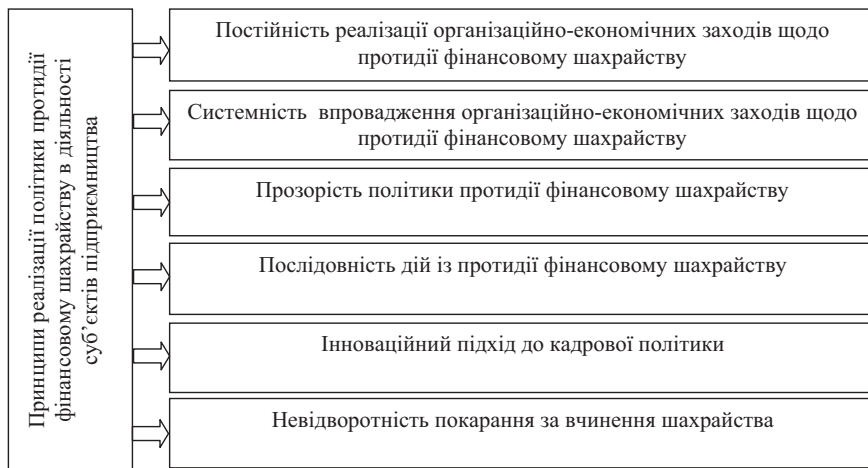


Рис. 5. 9. Принципи реалізації політики протидії фінансовому шахрайству в діяльності суб'єктів підприємництва

Джерело: розробила автор

Серед перелічених принципів особливу увагу хочемо звернути на застосування інноваційного підходу при здійсненні кадрової політики, яка повинна передбачати використання новітніх методик відбору працівників при їхньому прийнятті на роботу. Одним із важливих принципів реалізації політики із протидії фінансовому шахрайству є незворотність покарання працівників за вчинення злочинів. Водночас трапляються ситуації, коли менеджера, який вчинив шахрайство, залишають працювати, враховуючи його цінність як фахівця у відповідній сфері або з міркувань загрози розголошення ним конфіденційної інформації. Однак безкарність породжує всюдозволеність, що підтверджує і теорія розбитих вікон Дж. Вілсона і Дж. Келлінга, котру ми описали в попередніх розділах. Учені експериментальним шляхом довели, що, порушення існуючих правил частіше відбувається, коли є приклади безкарного вчинення правопорушень у минулому.

Для попередження загроз фінансовій безпеці, генерованих персоналом ділових одиниць, потрібно постійно проводити моніторинг його кадрової безпеки. Тому на наступному етапі необхідно розробити

методику оцінки кадрової безпеки, під якою розуміємо стан суб'єкта підприємництва, який дає змогу визначати загрози зі сторони персоналу та запобігати негативним впливам на його фінансову безпеку. Аналіз наукових підходів до вивчення проблематики забезпечення кадрової безпеки підприємств [80; 97; 146; 277; 387] дав нам змогу виокремити такі інструменти оцінки кадрової безпеки:

- тести компанії Midot – оцінка благонадійності кандидата на посаду й оцінка лояльності персоналу;
- перевірка на детекторі неправди (поліграфі);
- тести компанії Profiles International – SOS (початкова оцінка претендента), PMF (оцінка управлінських якостей), EBC (перевірка відомостей про співробітника), CSP (оцінка роботи з клієнтами), PXT (оцінка відповідності посаді), WES (оцінка командної роботи), PPI (оцінка ефективності праці), PLP (оцінка лояльності), JSA (оцінка професійних якостей), PSA (оцінка ефективності продаж), CP360 (оцінка 360);
- тести Extended System – комп'ютерна програма, яка визначає індивідуальні особливості співробітника для спроможності виконання тієї чи іншої роботи.

Впровадження таких інноваційних рішень та новітніх програмних продуктів із забезпечення кадрової складової фінансової безпеки суб'єктів підприємництва потребує додаткових витрат. Зокрема, на думку О. Підхомного, атмосфера шахрайства та недовіри зумовлює додаткові витрати на функціонування різноманітних систем моніторингу та контролю. Однак такі системи в деяких випадках можуть бути дорожчими, ніж втрати від зловживань [196, с. 18]. Не погоджуємося з такою позицією, оскільки деструктивні наслідки від фінансових зловживань в умовах цифровізації економічних процесів й гібридних агресій вимірюються не лише значними економічними збитками й нематеріальними втратами у формі зниження морального духу ділової одиниці й рівня її ділової репутації, а й можуть спричинити гостру кризу їх функціонування та загрозу втрати бізнесу загалом унаслідок рейдерства.

Підготовчий етап організаційної моделі протидії фінансовому шахрайству передбачає визначення методів його виявлення й розслідування. Відтак, до основних із них, на наш погляд, варто віднести такі:

- внутрішній і зовнішній аудит. За результатами опитування, яке проведене компанією “Ernst & Young”, присвяченого питанням шахрайства, внутрішні аудитори допомагають виявити до 44 % та розкрити до 26 % фактів шахрайства [179];

- система повідомлень у різних формах, зокрема функціонування “гарячої лінії”;

- ротація кадрів;

- постійний контроль з боку власників роботи найманого керівництва, а зі сторони керівництва – персоналу;

- обмеження одноосібного ухвалення рішень щодо значних за сумами фінансових операцій, отримання великих обсягів кредитування тощо;

- використання власниками різних джерел інформації про стан функціонування суб’єкта підприємництва з метою їх порівняння та встановлення достовірності (результати перевірок державними органами, дані, отримані під час неформальних контактів з працівниками, аудиторські висновки, інформація, отримана від ділових партнерів тощо);

- встановлення випробувального терміну праці працівників керівної ланки;

- моніторинг ділової активності власниками найманого керівництва після завершення випробувального терміну праці (близько двох–п’яти років роботи на посаді у сфері виробництва і великого бізнесу; півтора–два роки у сфері послуг і гуртової торгівлі);

- здійснення IT-контролю активності працівників у комп’ютерній мережі в робочий час за допомогою спеціальних прикладних програм;

- використання поліграфа (детектора брехні) у разі підозри у фінансовому шахрайстві.

Також необхідно розробити стандарти і процедури протидії фінансовому шахрайству в підприємницькій діяльності, які найефективніше допомагали б виявляти зловживання у сфері фінансів та забезпечували б найменші втрати від шахрайства. Необхідно враховувати ризики шахрайства в підприємстві за галузями, регіонами та масштабами діяльності і здійснювати порівняльний аналіз методів боротьби з шахрайством, що використовуються діловою одиницею зі способами протидії фінансовим злочинам, які застосовують інші суб’єкти господарювання.

Оцінювання наявного стану захищеності від фінансового шахрайства в підприємницькій діяльності повинно передбачати аналіз кадрової безпеки,

усіх чинників організаційного характеру, негативних явищ і процесів, які є супутніми фінансовій злочинності. Також цей етап передбачає розслідування фінансового шахрайства, вчиненого працівниками суб'єкта підприємництва, зокрема виявлення фінансових злочинів, способів та причин їх вчинення з метою встановлення проблем ефективності використання наявних методів протидії фінансовому шахрайству. Відповідно до проведеного оцінювання наявного стану захищеності від фінансового шахрайства необхідно розробити та впровадити фінансово-економічні, організаційно-технічні та етико-моральні заходи протидії.

До фінансово-економічних необхідно віднести засоби, які передбачають співпрацю із контрагентами з належним рівнем платоспроможності та надійною репутацією, що допоможе запобігти можливій змові між ними й співробітниками ділової одиниці.

Організаційно-технічні засоби протидії фінансовому шахрайству повинні охоплювати такі:

- професійна підготовка внутрішніх аудиторів з долученням додаткових інструментів контролю фінансового шахрайства;
- покарання винних у фінансовому шахрайстві осіб та захист інформаторів про його випадки;
- колегіальне ухвалення управлінських рішень з високим рівнем ризику шахрайства;
- участь профільних працівників в семінарах щодо протидії фінансовому шахрайству з метою обміну досвідом;
- інформування партнерів та контрагентів щодо основних засад Кодексу корпоративної культури, зокрема неприйнятності шахрайства та зловживань і наслідків у випадку його вчинення, що забезпечить формування чіткого розуміння у партнерів і контрагентів негативних результатів співпраці у разі виявлення фактів змови зі співробітниками ділової одиниці;
- забезпечення прозорості бізнес-процесів під час реалізації і закупівлі товарів (робіт, послуг);
- перевірка працівників на наявність ознак фінансового шахрайства, наприклад, здійснення ними витрат, які не збігаються з доходами;
- застосування для інформування про шахрайства “гарячих ліній”.

Водночас унаслідок пандемії Covid-19 виявлено, що значну кількість фінансових угод укладено без здійснення ретельного аналізу контрагентів, а віддалена робота працівників була мало контрольованою, оскільки в

складних економічних умовах для багатьох ділових одиниць пріоритетним стало збереження своєї ринкової позиції.

Етико-моральні засоби, що необхідно впроваджувати в діяльності суб'єктів підприємництва з метою запобігання й протидії фінансовому шахрайству, повинні охоплювати формування сприятливого психологічного клімату, наявність високого рівня корпоративної культури, створення програми допомоги працівникам у кризових фінансових ситуаціях, що значною мірою допоможе знизити рівень мотиваційного чинника працівників до скоєння фінансових злочинів.

У системі етико-моральних засобів протидії фінансовому шахрайству вважаємо необхідним акцентувати на чиннику корпоративної культури, оскільки функціонування суб'єкта підприємництва характеризується взаємодією значної кількості працівників, що перебувають у безперервній комунікації для реалізації поставлених службових завдань. Відтак, важливим у цьому контексті є підвищення рівня їхньої мотивації та спрямування на досягнення стратегічних цілей ділової одиниці спільними зусиллями кожного працівника.

Під корпоративною культурою розуміємо взаємопов'язану систему цінностей і переконань, які повинен усвідомлювати й схвалювати кожен працівник суб'єкта підприємництва. Відтак, серед її основних елементів, на наш погляд, варто виокремити такі:

- система комунікацій;
- усвідомлення кожним співробітником своєї ролі в забезпеченні реалізації стратегічних чи/або оперативно-тактичних цілей;
- наявність спеціального одягу, який характеризує приналежність до певного суб'єкта підприємництва й дає змогу відчувати себе в такий спосіб членом єдиної команди;
- розпорядок дня, в тому числі організація короткотривалого відпочинку працівників;
- взаємовідносини з діловими партнерами;
- система мотивування та трудова етика (відповідальність за виконану роботу, якість роботи, оцінка роботи та винагорода за неї, просування по кар'єрних сходах);
- віра в успіх;
- символіка суб'єкта підприємництва (логотипи, бренди, гасла, кредо тощо).

Загалом учені виділяють різні типи корпоративної культури й відповідні механізми її реалізації. Зокрема, Г. Чайка [297] виокремлює такі:

- “культура влади”. У діяльності таких суб’єктів підприємництва передбачене ефективне використання і перерозподіл ресурсів керівництвом. Цей тип культури ґрунтується на принципах ієрархії, просування по сходинках якої відбувається за критеріями відданості загальній меті. У цьому разі провідну роль відіграє керівник, його якості та здібності, які дають змогу оперативно реагувати на динамічні зміни зовнішнього середовища, ухвалювати та реалізовувати складні рішення;

- “рольова культура”. Для ділових одиниць з таким видом культури характерний суворий функціональний розподіл ролей та спеціалізації підрозділів. Цей тип організацій функціонує на засадах правил і стандартів діяльності, дотримання яких гарантує їхнє виконання. Джерелом влади тут є не особисті якості керівника, а його становище в ієрархічній структурі. Така організація здатна успішно працювати тільки в стабільному середовищі;

- “культура завдань”. У таких підприємствах культура зорієнтована на вирішення поставлених конкретних завдань і реалізацію проєктів. Ефективність діяльності ділової одиниці з такою культурою визначена професіоналізмом працівників, корпоративним груповим ефектом і повнотою інформації. Застосування цього типу культури доцільне в тих випадках, коли ситуативні вимоги ринку є визначальними для діяльності організації;

- “культура особистості”. Суб’єкти підприємництва з таким видом культури об’єднують людей не для вирішення завдань, а для того, щоб вони могли досягти власних цілей. Влада ґрунтується на професіоналізмі та вмінні спілкуватися і взаємодіяти.

Ми проаналізували результати проведених опитувань на предмет дієвості корпоративної культури в контексті забезпечення фінансової безпеки й виявлено таке:

- підприємства з високою лояльністю співробітниками за три роки дали своїм акціонерам 112 % прибутку, ділові одиниці зі середнім рівнем лояльності співробітників – 90 %, а з низьким – лише 76 % [146, с. 130];

- близько 65 % власників/керівників у розрізі різних секторів економіки вважають, що корпоративна культура впливає на фінансові результати діяльності [261, с. 127].

Для підтвердження висновків про важливість корпоративної культури

в забезпеченні фінансової безпеки ділових одиниць скористаємося дослідженнями вчених у сфері організації управління, зокрема Н. Ринкевич [261, с. 127] (табл. 5.3).

Таблиця 5.3

Результати анкетування впливу корпоративної культури на фінансові результати суб'єктів підприємництва

Види діяльності	Відповіді, % експертів		
	Так	Ні	Частково
Харчова промисловість	64,3	7,1	28,6
Будівництво	66,7	33,3	-
Сфера послуг	65,8	12,2	22
Оптова й роздрібна торгівля	38,5	15,4	46,1
Освіта й наука	76,2	4,8	19
Державне управління	80	-	20
Вугільна промисловість	100	-	-
У цілому	65,2	10,4	24,4

Встановивши важливість чинника корпоративної культури в протидії фінансовому шахрайству в діяльності ділових одиниць, визначимо її основні сутнісно-функціональні характеристики (рис. 5.10).

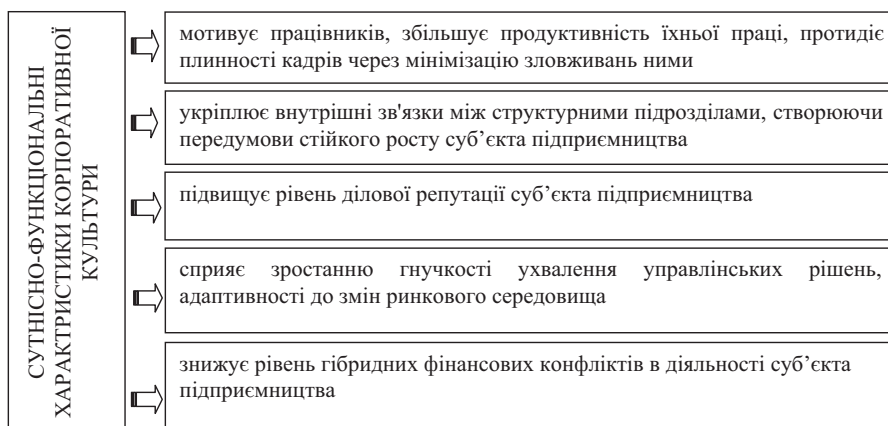


Рис. 5.10. Сутнісно-функціональні характеристики корпоративної культури

Джерело: розробила автор

Відтак, необхідним є окреслення послідовності етапів формування корпоративної культури в діяльності ділових одиниць, візуальну інтерпретацію яких подано на рис. 5.11.

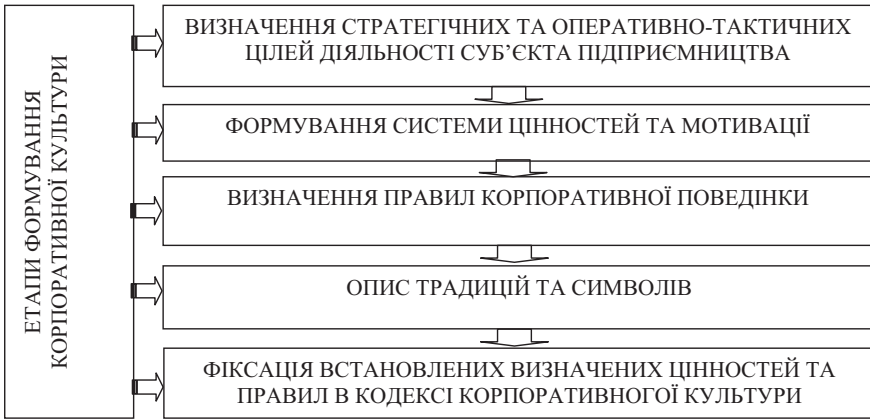


Рис. 5. 11. Структурно-логічна схема формування корпоративної культури

Джерело: розроблено автором

Для реалізації сукупності етапів з формування корпоративної культури необхідним є створення спеціального підрозділу на підприємствах, що відповідатиме за розроблення і впровадження програм корпоративної культури, створення сприятливої атмосфери для її сприйняття працівниками, укладення в їх свідомості системи цінностей і мотивації, необхідних для забезпечення успішної діяльності, розвитку у персоналу соціальної поведінки, необхідної для протидії фінансовому шахрайству.

Основні засади корпоративної культури необхідно фіксувати в Кодексі корпоративного управління (Кодексі корпоративної культури), що сприятиме орієнтації всіх підрозділів і працівників підприємницької структури на загальні цілі, дасть змогу підвищувати рівень ініціативності персоналу, забезпечувати відданість загальній справі. Такий кодекс повинен містити правила й норми поведінки, засновані на засадах фахової компетентності працівників і принципах загальнолюдської моралі.

Наступний досліджений нами гібридний фінансовий конфлікт – рейдерство, що потребує розроблення відповідних до його специфіки заходів протидії.

Корисним у цьому контексті є дослідження способів протидії рейдерству в зарубіжній практиці [67, с. 36]:

– спосіб захисту “відлякування акул” (уведення в статутні документи положень, які охоплюють обмежуючі умови переходу контролю над підприємством до агресора (норма про мажоритарну більшість, яка передбачає ухвалення певних рішень принаймні двома третинами голосів; норма про переобрання ради директорів тощо));

– спосіб захисту “коштовності корони” (створення окремих юридичних осіб, які становлять самостійну цінність (володіння торговельними марками суб’єкта підприємництва, контроль закупівлі сировини і матеріалів для виробництва, а також збут готової продукції));

– спосіб захисту “золотий парашут” (наявність спеціальних умов у статутних документах і трудових контрактах топ-менеджерів (у разі їхнього дострокового звільнення передбачена грошова компенсація));

– спосіб захисту “отруйна пігулка” полягає в тому, щоб зробити суб’єкт підприємництва непривабливим для загарбників укладанням не вигідних угод (закупівля сировини за завищеними цінами, продаж продукції за заниженими цінами, отримання довготермінових кредитів на умовах високих відсотків) через ймовірність отримання штрафів і неустойки за відмову від їхнього виконання;

– спосіб протидії агресивному захопленню “захист Пекмена” передбачає ситуацію, коли суб’єкт підприємництва, який потенційно намагаються поглинати, робить покупцеві зустрічну пропозицію про купівлю або починає приховане скуповування акцій і боргових зобов’язань загарбника;

– спосіб захисту “білий лицар” використовують у випадку, коли інші методи захисту від поглинання виявилися неефективними й передбачає вибір суб’єкта підприємництва, який більш прийнятний для злиття чи поглинання.

Функціонування ділових одиниць в Україні має свої відмінні особливості, виявлені в попередніх розділах схеми рейдерства, також не дають змоги повною мірою скористатися розглянутими способами протидії протиправному захопленню, що використовують у закордонній практиці. Водночас, враховуючи окремі аспекти закордонного досвіду, пропонуємо такі заходи протидії рейдерським атакам, що необхідно реалізувати на рівні держави та ділових одиниць (рис. 5.12).

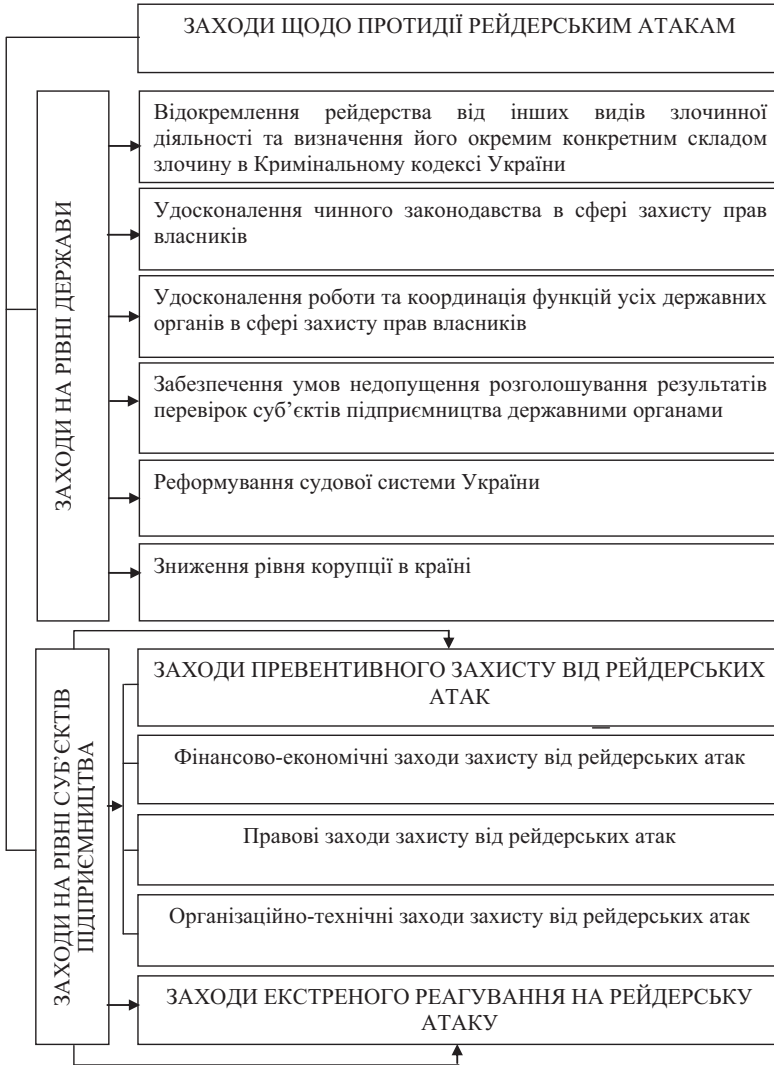


Рис. 5.12. Систематизація заходів щодо протидії рейдерським атакам в Україні

Джерело: розробила автор

На рівні суб'єктів підприємництва передусім необхідно концентрувати управлінські зусилля на способах попередження рейдерства та з цією метою реалізувати сукупність фінансово-економічних, правових та організаційно-технічних заходів. Попри те, що такі засоби захисту від

рейдерства необхідно розробляти індивідуально для кожного суб'єкта підприємництва з урахуванням особливостей його діяльності, можемо уніфікувати низку ключових із них, які рекомендуємо загалом. Відтак, основними фінансово-економічними заходами захисту від рейдерства вважаємо такі: формування захищеної корпоративної структури; моніторинг активів та зобов'язань; контроль за виконанням менеджерами операцій, що передбачають відчуження активів, розпорядження значними сумами коштів, залучення великих обсягів кредитів; застосування способів захисту, що різко знижують економічну привабливість захоплення ділової одиниці; консолідація в руках основних власників якомога більшого пакета акцій (часток); проведення ділової розвідки з метою отримання даних щодо розвитку ринкової інфраструктури, діяльності партнерів, клієнтів, конкурентів.

До організаційно-технічних заходів захисту від рейдерських атак пропонуємо включати такі:

- створення системи мотивації або обмеження повноважень менеджменту в частині одноосібного ухвалення важливих рішень;
- обов'язкова перевірка посвідчень і повноважень осіб державних контролюючих органів, а також підстав для витребування різних документів суб'єкта підприємництва з метою запобігання фактам перевищення ними своїх службових повноважень;
- реагування винятково на письмові запити представників державних органів, уникаючи надання інформації під час телефонних розмов, щоб не стати інформатором для рейдерів;
- впровадження надійної системи технічного захисту конфіденційної фінансової інформації;
- обмеження в обігу важливих документів усередині суб'єкта підприємництва;
- здійснення суворого контролю над вхідною та вихідною кореспонденцією, в тому числі засобами електронного зв'язку;
- забезпечення надійного місця зберігання печатки та важливої документації суб'єкта підприємництва (оригіналів установчих і реєстраційних документів, правоустановчих документів на активи й на придбання акціонерами їхніх пакетів акцій, оригіналів ліцензій, дозволів, договорів оренди тощо);
- захист печатки суб'єкта підприємництва від підроблення;

– долучення до смс-інформування про реєстраційні дії з нерухомістю та періодичний моніторинг державних реєстрів на предмет зміни реєстраційних даних.

Дослідження праць вчених в сфері юридичного захисту прав суб'єктів підприємницької діяльності [4; 14; 56; 66; 71; 160] дало змогу виділити такі основні правові заходи захисту від рейдерських атак:

- належний юридичний супровід діяльності суб'єкта підприємництва й розроблення досконалої структури усіх його важливих документів;
- створення правових умов, що перешкоджають маніпуляціям з акціями (для суб'єктів господарювання акціонерної форми власності);
- створення правових обмежень щодо неконтрольованого скуповування боргів ділової одиниці, зокрема, передбачення в договорах, за якими суб'єкт господарювання є стороною-боржником, умови, що уступка права вимоги за договором може бути тільки за згодою боржника;
- ухвалення Положення “Про конфіденційну фінансову інформацію суб'єкта господарювання”, де передбачено вимоги її нерозголошення та відповідальність за порушення цих вимог, а також доцільно обмежити можливість надання конфіденційної інформації третім особам тільки за рішенням загальних зборів (наглядової ради).

Реалізація таких превентивних заходів захисту від рейдерських атак дає змогу запобігти або суттєво знизити ймовірність їх реалізації.

Захист після активних агресивних дій рейдерів передбачає реалізацію таких екстрених заходів:

- створення кризової групи із протидії рейдерству;
- звернення зі скаргою про незаконне захоплення підприємства до Комісії з питань розгляду скарг у сфері державної реєстрації [220; 221];
- звернення зі скаргою про незаконні реєстраційні дії до Ради бізнес-омбудсмена;
- розроблення та реалізація стратегії судового захисту;
- реструктуризація основних активів суб'єкта підприємництва;
- захист реєстру акціонерів (для суб'єктів господарювання акціонерної форми власності);
- блокування пакета акцій “агресора” (для суб'єктів господарювання акціонерної форми власності);
- захист від масового скуповування акцій ділової одиниці (для суб'єктів господарювання акціонерної форми власності);

- контркуповування акцій агресора (для суб'єктів господарювання акціонерної форми власності);
- додаткова емісія акцій для товариств акціонерної форми власності чи збільшення статутного фонду для товариства з обмеженою відповідальністю;
- організація фізичного захисту об'єктів власності;
- забезпечення захисту конфіденційної інформації;
- обтяження майна суб'єкта підприємництва (довірче управління майном, оренда і застава);
- організація PR-підтримки заходів протидії рейдерству.

Окрім заходів протидії рейдерству, на рівні суб'єкта підприємництва важливим є розроблення та впровадження дієвих механізмів боротьби з протиправними захопленнями на рівні держави. Зокрема, виявлено потребу удосконалення правового механізму регулювання рейдерства в частині виокремлення його як окремого кримінально караного діяння. Оскільки відсутність чіткого та системного покарання за протиправні захоплення підприємств при можливості притягнення до відповідальності лише за низкою складових злочинів рейдерства значно ускладнює процес ефективної протидії незаконним захопленням підприємств в Україні. Тому серед основних заходів подолання рейдерства на рівні держави доцільно: удосконалити чинне законодавство, відокремивши рейдерство від інших видів злочинної діяльності та визначивши його як окремих конкретний склад злочину в Кримінальному кодексі України; забезпечити умови недопущення розголошування результатів перевірок ділових одиниць державними органами; реформувати судову систему України відповідно до принципів судочинства міжнародної практики; продовжувати державну роботу з мінімізації рівня корупції в країні.

Протидія рейдерству повинна об'єднувати роботу професіоналів, залучених до управління фінансовою безпекою ділової одиниці на внутрішньому рівні (працівники підприємства) та зовнішньому рівні (послуги аутсорсингу в сфері фінансової безпеки). До внутрішньої системи фінансової безпеки повинні бути залучені абсолютно всі співробітники (фахівці фінансово-аналітичного департаменту, юридичного департаменту, фахівці з кадрової безпеки, IT-безпеки, конкурентної розвідки та ін.).

Щодо зовнішніх фахівців в сфері управління фінансовою безпекою суб'єктів підприємництва, то, на наш погляд, щоб підвищити ефективність даної складної ланки управління можливим є залучення професіоналів із адвокатського супроводу, кіберзахисту, конкурентної розвідки, кризової комунікації тощо. Лише об'єднавши спільні зусилля внутрішніх та зовнішніх фахівців у сфері фінансової безпеки, можна ефективно протидіяти усім реальним та потенційним загрозам протиправного захоплення суб'єктів господарювання.

Окрім того, на сьогодні певні інструменти протидії рейдерству надають громадські організації, ЗМІ, приватні консалтингові компанії, що пропонують комплексні сервіси. Однак вони передбачають лише окремі аспекти боротьби з протиправним захопленням: адвокатські та охоронні послуги, послуги з PR, послуги із протидії кібератакам, формування корпоративної безпеки, розроблення конкурентних дій тощо.

Забезпечення фінансової безпеки суб'єктів підприємництва належить до сфери управління, винятково чутливої до зовнішніх деструктивних впливів. Залучення зовнішніх фахівців може бути як корисним, так і становити загрозу для фінансової безпеки ділових одиниць. Оскільки варто враховувати, що рейдери можуть використовувати таких спеціалістів у якості шпигунів, які впроваджуються у підприємство під прикриттям.

Відтак, ефективна протидія незаконному захопленню суб'єктів підприємництва вимагає комплексного підходу, поєднання різноманітних інструментів захисту, залучення різного рівня фахівців із внутрішнього та зовнішнього середовища з ретельною перевіркою їх доброчесності. Також важливим у цьому контексті є і постійний зв'язок суб'єктів підприємництва між собою. Адже на сьогодні, незважаючи на наявність значної кількості асоціацій та клубів, ділова спільнота не є згуртованою. Водночас співпраця з громадськими організаціями, членство в бізнес-асоціаціях може значною мірою запобігти протиправному захопленню бізнесу. Адже спільними зусиллями, в тому числі оприлюднюючи інформацію про кожне правопорушення в сфері захисту інтересів власників, легше їм протидіяти.

Боротьба з корупцією як гібридним фінансовим конфліктом, що виникає в підприємницькій діяльності, своєю чергою потребує розроблення організаційного інструментарію протидії їй. Пропонуємо вирішення цього завдання реалізувати за допомогою такої організаційної моделі (рис. 5.13).



Рис. 5.13. Організаційна модель реалізації антикорупційної політики в діяльності суб'єктів підприємництва

Джерело: розробила автор

Підготовчий етап передбачає встановлення мети, завдань, об'єктів, суб'єктів та принципів антикорупційної політики ділових одиниць. Потрібно визначити бізнес-процеси та перелік посад із корупційним ризиком, а також осіб, відповідальних за впровадження та дотримання антикорупційної політики.

Наступним кроком має стати розроблення і впровадження антикорупційних стандартів і процедур, спрямованих на забезпечення добросовісної роботи працівників та фіксація сформованих засад антикорупційної політики в Кодексі антикорупційної політики.

Оцінка антикорупційної позиції суб'єкта підприємництва передбачає перевірку бізнес-процесів з корупційним ризиком, генерованим його працівниками, контрагентами і державними службовцями, з якими є взаємодія при здійсненні діяльності.

Визначення корупційних ризиків, генерованих працівниками, має охоплювати такі напрями:

- дослідження особистісних характеристик працівників та їх фінансового становища, в т. ч., аналіз нетипових надходжень грошових коштів на їхні рахунки;
- перевірку наявності у працівників прямих чи опосередкованих зв'язків із контрагентами, державними службовцями;
- моніторинг підозрілих статей витрат та недоотримання доходів суб'єктом підприємництва;
- перевірку обґрунтованості надання пільгових умов контрагентам зі сторони працівників.

Визначення корупційних ризиків, генерованих контрагентами ділових одиниць, передбачає передусім формування команди щодо проведення такої оцінки з багатопрофільних фахівців, зокрема юристів, фінансових аналітиків, працівників Служби фінансової безпеки тощо. Для пошуку та збору інформації про контрагентів можна використовувати такі відкриті джерела, як сервіс моніторингу реєстраційних даних українських підприємств “Opendatabot”, а також програмні рішення для бізнесу, зокрема “YouControl”, “CONTR AGENT” тощо. Благонадійність контрагентів пропонуємо визначати шляхом аналізу отриманих даних за такими критеріями:

- реєстрація контрагентів, достовірність засновницьких документів;
- наявність фактів судових справ та кримінальних проваджень;

- фінансовий стан, досвід та наявність необхідних ресурсів для виконання умов контрактів, що укладаються;
- порядок дотримання усіх регламентних процедур при укладенні угод (тендерної документації, комерційних пропозицій тощо);
- наявність взаємозв'язків контрагентів з працівниками суб'єкта підприємництва;
- ділова репутація контрагентів, наявність у них антикорупційної системи;
- особистісні характеристики та діловий імідж власників та керівництва контрагентів;
- наявність фактів пов'язаності контрагентів із групами політичного впливу в країні.

Визначення корупційних ризиків, генерованих державними службовцями, передбачає дослідження державної політики в сфері діяльності суб'єкта підприємництва й з'ясування усіх необхідних процедур організаційного характеру, які необхідно здійснювати в процесі його функціонування.

Завершальним кроком на етапі оцінювання антикорупційної позиції ділових одиниць повинна бути оцінка ймовірних масштабів фінансових та репутаційних наслідків при виявленні корупційних ризиків. З цією метою необхідно встановити допустимий рівень корупційних ризиків та здійснити їх ранжування за вагомістю деструктивного впливу на фінансову безпеку суб'єктів господарювання.

Антикорупційна політика суб'єкта підприємництва передбачає розроблення та впровадження низки конкретних заходів із протидії корупції для кожної категорії ризику з метою її усунення. Водночас організаційними заходами універсального характеру є забезпечення інформованості уповноважених служб ділової одиниці про реальні та потенційні випадки корупції, а також інформування контрагентів про неприпустимість корупції. Необхідно проводити розслідування усіх корупційних дій, незворотне покарання винних осіб та захист інформаторів про випадки корупції в підприємницькій діяльності, підвищувати рівень компетентності фахівців служби фінансової безпеки шляхом участі профільних працівників в антикорупційних семінарах з метою обміну досвідом.

Основні принципи антикорупційної політики суб'єктів підприємництва нерозривно пов'язані з принципами протидії корупції на рівні держави. Відтак, вважаємо необхідним виокремити серед них такі (рис. 5.14):

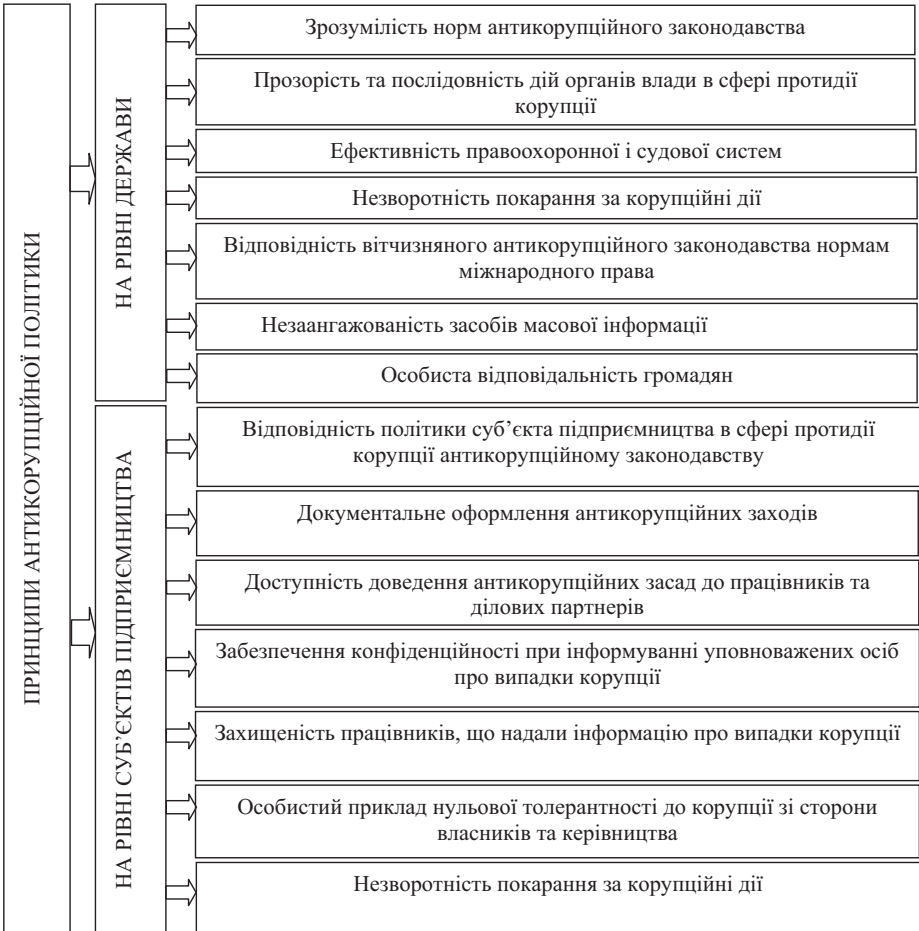


Рис. 5.14. Принципи реалізації антикорупційної політики на рівні держави та суб'єктів підприємництва

Джерело: розробила автор

До важливих завдань протидії гібридним фінансовим конфліктам належить розроблення конкурентної політики ділових одиниць в частині нівелювання впливу недобросовісної конкуренції на їх фінансову безпеку. Рекомендуємо використовувати організаційну модель конкурентної політики суб'єктів підприємництва в умовах недобросовісної конкуренції (рис. 5.15).

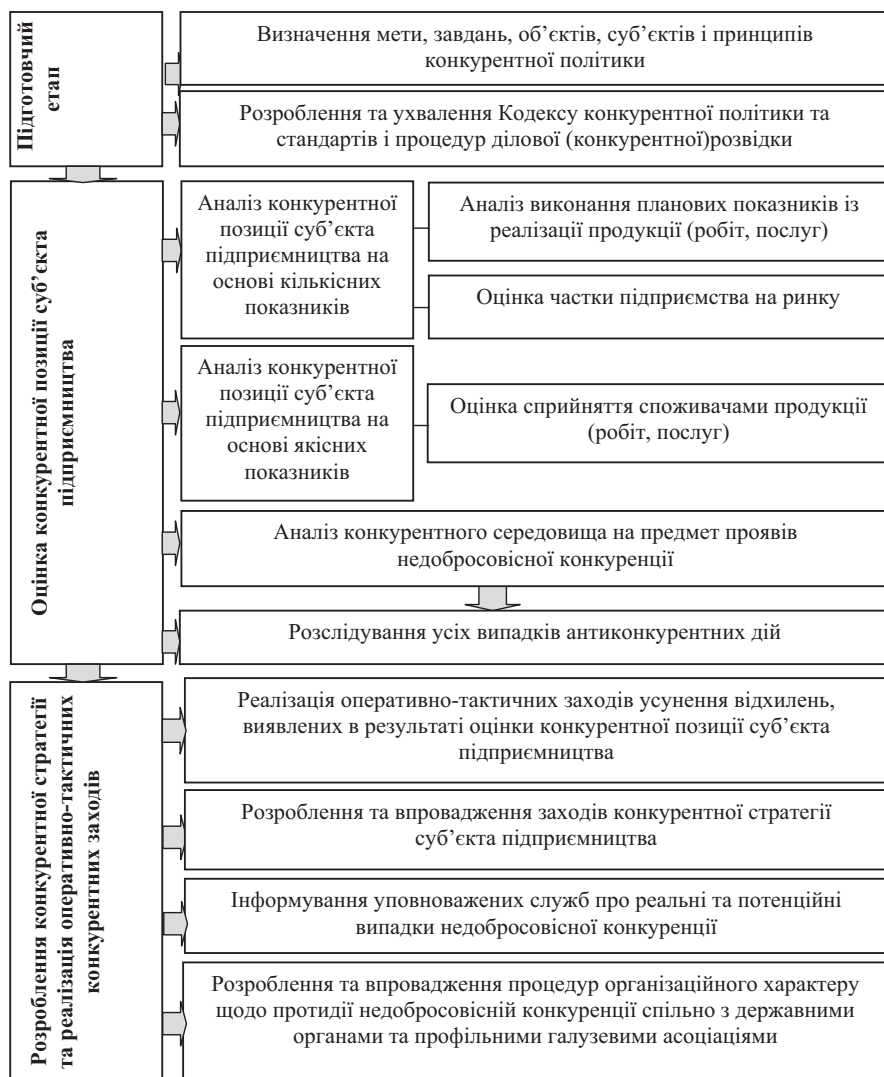


Рис. 5.15. Організаційна модель реалізації конкурентної політики суб'єкта підприємництва в умовах недобросовісної конкуренції

Джерело: розробила автор

Об'єктом конкурентної політики є фінансові інтереси суб'єкта підприємництва, а суб'єктами є власники, керівництво, Служба фінансової безпеки та усі інші відділи управління й кожен працівник зокрема.

Метою реалізації конкурентної політики є захист фінансових інтересів суб'єкта підприємництва шляхом здійснення ділової розвідки та реалізації конкурентної стратегії, а також виявлення та усунення антиконкурентних дій в спільному з конкурентами сегменті ринку. Сформульована мета передбачає вирішення таких основних завдань:

- проведення ділової розвідки;
- розроблення та реалізація конкурентної стратегії;
- фіксація антиконкурентних дій;
- розроблення методів протидії недобросовісній конкуренції (стратегії дій на ринку);
- залучення відповідних державних органів до протидії недобросовісній конкуренції.

Наступний етап передбачає розроблення та ухвалення Кодексу конкурентної політики та стандартів і процедур ділової розвідки суб'єкта підприємництва. Цей внутрішній документ покликаний описати напрями ділової розвідки, які здійснюватимуться діловою одиницею на ринку з окресленням правових та етико-моральних аспектів такої діяльності, методи реалізації конкурентної стратегії та способи виявлення та захисту від недобросовісної конкуренції.

Вважаємо, що кожен суб'єкт підприємництва повинен періодично проводити оцінювання своєї конкурентної позиції та конкурентного середовища на предмет проявів недобросовісної конкуренції. На основі отриманих результатів необхідно розробити стратегію та тактику дій з інформуванням відповідних уповноважених служб, а також із залученням державних та галузевих органів до впровадження заходів із протидії цьому виду гібридного фінансового конфлікту.

Аналіз особливостей розвитку гібридних фінансових конфліктів, які характеризуються спільними ознаками, та організаційні моделі протидії кожному із них, що передбачає схожість у реалізації окремих попереджуючих заходів, дав змогу зробити висновок про необхідність уніфікації підходу до управління ними й агрегування організаційно-економічного інструментарію протидії їм у діяльності суб'єктів підприємництва. Відтак, пропонуємо використовувати типові сценарії впровадження організаційно-економічних заходів протидії гібридним фінансовим конфліктам у практику ділових одиниць, візуальну інтерпретацію яких подано в додатку П.

Реалізація таких сценаріїв впровадження організаційно-економічних заходів протидії гібридним фінансовим конфліктам дасть змогу суб'єктам підприємництва підвищити ефективність боротьби з фінансовим шахрайством зі сторони працівників, рейдерством, проявам корупції та недобросовісної конкуренції.

Як було нами виявлено, унаслідок зростання залежності від інформаційних та комунікаційних систем суб'єкти підприємництва стають вразливішими до порушень режиму інформаційної, а в підсумку й фінансової безпеки внаслідок таких чинників:

- високі темпи зростання парку електронних гаджетів і можливостей зв'язку, розширення сфер їхнього використання;
- залучення в процес інформаційної взаємодії щораз більшої кількості людей і організацій;
- концентрація великих обсягів інформації різного призначення і належності на електронних носіях;
- наявність інтенсивного обміну інформацією між учасниками фінансових процесів;
- перехід більшості ділових одиниць на дистанційну форму роботи внаслідок впровадження карантинних заходів під час пандемії Covid-19.

Водночас фінансова інформація суб'єктів підприємництва в умовах гібридних фінансових конфліктів передбачає необхідність посиленого захисту її ключових властивостей:

- конфіденційність (доступність винятково для працівників з відповідними повноваженнями);
- цілісність (неможливість модифікації неавторизованими користувачами);
- доступність (своєчасний безперешкодний доступ до інформації уповноважених на це користувачів).

Вважаємо, що реалізувати захист конфіденційної фінансової інформації можна шляхом використання сукупності спеціальних служб та заходів адміністративно-правового, соціально-психологічного й організаційно-технічного характеру, що дадуть змогу забезпечити її збереження, цілісність та належний порядок доступу.

Відтак, у діяльності ділових одиниць необхідно розробляти й впроваджувати дієву систему захисту конфіденційної інформації, що

допоможе забезпечити надійну й ефективну протидію зловмисникам та вирішити сукупність таких завдань:

- захист законних прав та інтересів суб'єкта підприємництва;
- збирання, оцінювання та прогнозування даних, які характеризують ситуацію всередині та за межами ділової одиниці;
- вивчення партнерів, клієнтів і конкурентів суб'єкта підприємництва;
- своєчасне виявлення можливого інтересу до суб'єкта господарювання та його співробітників з боку осіб, які можуть стати джерелом загроз фінансовій безпеці;
- недопущення проникнення в діяльність суб'єкта підприємництва представників структур економічного шпигунства, організованої злочинності та окремих осіб з протиправними намірами;
- протидія технічному проникненню в комп'ютерну мережу ділової одиниці зі злочинними намірами.

Сьогодні в Україні порядок захисту інформації регламентує сукупність законодавчих актів щодо використання інформації, визначення прав й обов'язків учасників інформаційних відносин у процесі роботи з конфіденційною фінансовою інформацією, а також відповідальність за порушення цих правил (табл.5.4).

Таблиця 5.4

**Законодавчі акти України, що регламентують
порядок захисту інформації**

ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ АКТІВ УКРАЇНИ В СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ	АСПЕКТИ РЕГУЛЮВАННЯ
ЗУ "Про інформацію" від 02.10.1992 № 2657-ХІІ	відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації
ЗУ "Про електронні комунікації" від 16.12.2020 № 1089 - ІХ	визначення правових та організаційних основ державної політики у сферах електронних комунікацій
ЗУ "Про електронні довірчі послуги" від 05.10.2017 № 2155-VІІІ	визначення правових та організаційних засад надання електронних довірчих послуг і здійснення електронної ідентифікації
ЗУ "Про електронні документи та електронний документообіг" від 22.05.2003 № 851-ІV	визначення організаційно-правових засад електронного документообігу й використання електронних документів
ЗУ "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94	регулювання відносин у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

Продовження таблиці 5.4

ЗУ “Про захист від недобросовісної конкуренції” від 07.06.1996 № 236/96, зокрема ст. 8., ст.15-1, глава 4	встановлення дискредитаційних дій щодо суб’єкта підприємництва; поширення інформації, що вводить в оману; неправомірне збирання, розголошення та використання комерційної таємниці
Кодекс України про адміністративні правопорушення (ст. 163.9, 163.11, 164.3)	визначення відповідальності за незаконне використання інсайдерської інформації, умисне поширення неправдивих або неточних відомостей, а також отримання, використання, розголошення комерційної таємниці, що може завдати шкоди діловій репутації або майновим інтересам суб’єкта підприємництва
Кримінальний кодекс України (ст. 163, 200, 231, 232, 330, 359, 360, 361, 362, 363)	визначення відповідальності за протиправні дії з інформацією та незаконне втручання в роботу комп’ютерів, систем та комп’ютерних мереж

Джерело: склала автор на основі [112; 132; 239; 222; 223; 224; 236; 237; 238; 239]

Відтак, згідно зі Законом України “Про інформацію” громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, отриманою на власні кошти, або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного чи іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, у тім числі належність її до категорії конфіденційної, і визначають для неї систему (способи) захисту. Для цього, крім Наказу про комерційну таємницю, ділові одиниці можуть затверджувати посадові інструкції із зазначенням порядку і системи обміну інформацією між співробітниками та зовнішніми користувачами, устанавлювати деталізований графік документообігу з призначенням відповідальних осіб, фіксувати спеціальні умови в трудових угодах і контрактах.

Суб’єкти підприємництва зобов’язані надавати конфіденційні відомості лише відповідним органам державної виконавчої влади і правоохоронним органам, і лише відповідно до чинного законодавства. Порядок надання інформації цим органам регламентований законами України: “Про оперативно-розшукову діяльність” від 18 лютого 1992 р. № 2135-XII, “Про прокуратуру” від 14 жовтня 2014 р. № 1697-VII, “Про Національну поліцію” від 02 липня 2015 р. № 580-VIII, “Про Національне антикорупційне бюро України” від 14 жовтня 2014 р. № 1698-VII, “Про Службу безпеки України” від 25 березня 1992 р. № 2229-XII, “Про основні засади здійснення державного фінансового контролю в Україні” від 26 січня 1993 р. № 2939-XII та іншими нормативними актами.

Положення щодо захисту конфіденційної інформації визначено також Законом України “Про захист від недобросовісної конкуренції”, зокрема такими статтями: ст. 15-1 “Поширення інформації, що вводить в оману”; ст. 17 “Розголошення комерційної таємниці”; ст. 18 “Схилення до розголошення комерційної таємниці”; ст. 19 “Неправомірне використання комерційної таємниці”.

Відповідальність за злочинні дії, пов’язані з одержанням інформації незаконним способом чи її зміною, знищенням, розголошенням регламентується Кримінальним кодексом України, зокрема такими статтями: ст. 163; ст. 200, ст. 231; ст. 232; ст. 232-1; ст. 330; ст. 359. ст. 360; ст. 361; ст. 361-1; ст. 361-2; ст. 362; ст. 363; ст. 363-1.

Високий рівень безпеки фінансової інформації неможливий без належної організації цього процесу на рівні суб’єктів підприємництва. З цією метою пропонуємо організаційну модель побудови та функціонування системи захисту конфіденційної фінансової інформації (рис. 5.16).

На першому етапі необхідно визначити перелік конфіденційної фінансової інформації та осіб, що повинні мати доступ до неї. Наступний етап передбачає оцінку наявного рівня захищеності конфіденційної фінансової інформації. Враховуючи знання та досвід фахівців у сфері захисту інформації [78; 81; 83], пропонуємо таку оцінку виконувати із використанням сукупності індикаторів інформаційної безпеки (додаток Р).

Після оцінювання наявного рівня захищеності фінансової інформації необхідно дослідити чинники, що впливають на порушення її конфіденційності чи цілісності. До них належать фактори, які не залежать від керівництва та персоналу ділової одиниці, та ті, які безпосередньо залежать від їхніх дій. Отже, до чинників, що виникають через помилки та упущення керівників суб’єкта підприємництва та їхніх співробітників, належать такі: застосування несертифікованих технічних засобів опрацювання фінансової інформації; низький рівень роз’яснювальної роботи щодо правил її захисту й безконтрольність за їх дотриманням; наявність працівників з психологічною готовністю до зловживань з фінансовою інформацією; низький рівень мотивації працівників; висока плінність кадрів у діяльності суб’єкта підприємництва.



Рис. 5.16. Теоретико-організаційна модель побудови та функціонування системи захисту конфіденційної фінансової інформації суб'єктів підприємництва

Джерело: розробила автор

Зовнішніми чинниками є: стихійні лиха (шторм, ураган, смерч, землетрус, повінь); катастрофи (пожежі, вибухи); несправності, аварії технічних засобів і устаткування; дії зловмисників.

Вважаємо, що система заходів щодо захисту конфіденційної фінансової інформації в діяльності суб'єктів підприємництва повинна охоплювати адміністративні, соціально-психологічні та технічні заходи захисту (рис. 5.17).

ЗАХОДИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ФІНАНСОВОЇ ІНФОРМАЦІЇ НА РІВНІ СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА	АДМІНІСТРАТИВНО-ПРАВОВІ	Встановлення переліку конфіденційної фінансової інформації
		Встановлення осіб, що мають доступ до конфіденційної фінансової інформації
		Забезпечення конфіденційності та відповідного режиму роботи з фінансовою інформацією
		Внесення до трудового договору з працівниками вимоги щодо нерозголошення конфіденційної фінансової інформації
		Запровадження дисциплінарних стягнень з працівників, що порушують правила інформаційної безпеки
	СОЦІАЛЬНО-ПСИХОЛОГІЧНІ	Ретельний підбір персоналу та намагання протидіяти плинності кадрів
		Мотивація працівників
		Бесіди та навчання працівників щодо виконання правил інформаційної безпеки
	ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ	Застосування захищених технічних засобів, що створюють перешкоди несанкціонованого доступу до конфіденційної інформації
		Використання спеціальних програм з функціями захисту конфіденційної фінансової інформації

Рис. 5.17. Система заходів щодо захисту конфіденційної фінансової інформації на підприємстві

Джерело: розробила автор

До адміністративно-правових заходів належать заходи організаційного характеру, що регламентують порядок роботи персоналу з конфіденційною фінансовою інформацією. Перш за все це стосується визначення переліку конфіденційної фінансової інформації та посадових осіб, що матимуть доступ до неї, і закріплення цього порядку в письмовій формі у відповідних інструкціях підприємства.

Організаційно-технічні заходи захисту конфіденційної фінансової інформації ґрунтуються на застосуванні захищених технічних засобів і спеціальних програм, призначених для створення перешкод на

можливих шляхах проникнення і доступу потенційних порушників до конфіденційної фінансової інформації. Відтак, окрім базових правил безпеки, необхідно вживати такі заходи цифрової захищеності:

- створення резервних копій ключових файлів для мінімізації збитків від атак з вимогою викупу;
- встановлення та регулярне оновлення захисного програмного забезпечення для протидії відомим цифровим загрозам;
- регулярне сканування усіх пристроїв, під'єднаних до корпоративної мережі та заборона використання неперевіраних портативних пристроїв;
- проведення регулярних тренінгів та курсів для працівників з метою навчання їх базовим правилам кібербезпеки;
- контроль доступу до облікових записів та баз даних;
- проведення регулярних тестувань захищеності корпоративних продуктів.

Соціально-психологічними заходами є бесіди з персоналом щодо безпеки фінансової інформації. Працівники ділових одиниць повинні бути навчені процедур захисту і правильного поведження з конфіденційною фінансовою інформацією та ознайомлені з мірами відповідальності за розголошення конфіденційних даних і процедурою повідомлення про різні типи інцидентів, що можуть вплинути на безпеку фінансової інформації. Важливим є також створення позитивного робочого клімату в колективі та забезпечення належної мотивації персоналу з метою уникнення невдоволених своїм становищем, що можуть бути потенційними зрадниками інтересів суб'єкта підприємництва і передати інформацію конкурентам чи іншим недоброзичливцям.

На сьогодні для запобігання витоку конфіденційної інформації широко застосовують DLP-системи (з англ. data leak prevention – запобігання витоку даних), що засновані на аналізі потоків даних. У разі виявлення конфіденційної інформації спрацьовує захист, який відстежує повідомлення або блокує його надсилання. Сутність роботи подібних систем полягає не тільки у блокуванні різних способів передавання інформації, а й у ретельній фільтрації всього трафіку. Найкращі DLP-системи, наприклад, можуть стежити за інтернет-трафіком, а також за інформацією, яку записують з комп'ютерів на

зовнішні носії (USB-флеш, оптичні диски тощо), за документами, які роздруковують, та ін. У цьому разі в автоматичному режимі система визначає, чи є в потоці даних документи, що містять конфіденційну інформацію, або такі, які схожі на них за змістом. Виявляючи щось подібне, DLP-система відразу посилає попередження співробітнику, який відповідає за гарантування інформаційної безпеки, і той вирішує, яких треба вживати заходів [78].

Серед технічних засобів варто виділити також використання програмного комплексу SearchInform, який дає змогу контролювати всі канали витоку інформації, а багатокomпонентна структура – вибрати тільки необхідні модулі. До ключових функцій цього програмного комплексу належать такі:

- повний контроль інформації, яку передають через Skype (голосові, текстові, SMS-повідомлення і файли);

- контроль ноутбуків, що дає змогу виявити витік інформації через ноутбуки, використовувані співробітниками за межами корпоративної мережі;

- контроль корпоративних смартфонів і планшетів на базі iOS (HTTP(S), Skype, Mail, IM, FTP);

- виявлення відправника даних незалежно від використаних ним електронної поштової скриньки, номера ICQ, акаунта Skype;

- відстеження і візуалізація комунікаційних зв'язків між співробітниками, що дає змогу автоматично виявляти й аналізувати зв'язки співробітників один з одним та із зовнішніми адресатами для зручної роботи і проведення внутрішніх розслідувань;

- розмежування прав доступу до інформації, що дає змогу налаштувати права доступу до перехопленої інформації;

- контроль вмісту робочих станцій і загальнодоступних мережевих ресурсів, що дає змогу відстежувати появу конфіденційної інформації в місцях, для цього не призначених;

- створення архіву перехопленої інформації, що дає змогу проводити повноцінні службові розслідування, суттєво спрощуючи відновлення послідовності подій інциденту.

Становлення та функціонування системи захисту конфіденційної фінансової інформації передбачає, на нашу думку, врахування низки таких принципів (рис. 5.18).

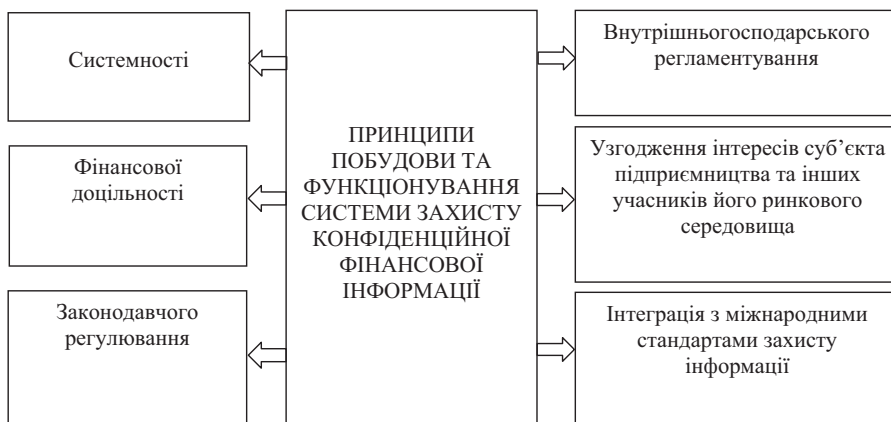


Рис. 5.18. Принципи побудови та функціонування системи захисту конфіденційної фінансової інформації на підприємстві

Джерело: розробила автор

1. Принцип системності (зумовлений необхідністю сприйняття системи захисту фінансової інформації нерозривно з іншими системами управління підприємством).

2. Принцип законодавчого регулювання (передбачає розроблення ефективної законодавчої бази, яка б забезпечувала захист інформації і створення на державному рівні дієвих механізмів та інституцій, які б забезпечували контроль за дотриманням захисту фінансової інформації ділових одиниць).

3. Принцип внутрішньогосподарського регламентування (передбачає затвердження основних правил захисту конфіденційної фінансової інформації на рівні суб'єктів підприємництва у відповідних інструкціях).

4. Принцип збалансування інтересів ділових одиниць та суб'єктів їхнього економічного оточення (зумовлений необхідністю пошуку компромісу між конфіденційністю фінансової інформації та необхідним обсягом даних, що підлягають оприлюдненню, зокрема, це стосується випадків, коли йдеться про виявлення антисоціальних проявів, корупційних дій, ухилення від оподаткування, отримання доходів, отриманих злочинним способом, неповернення позикових коштів тощо).

5. Принцип інтеграції з міжнародними стандартами захисту конфіденційної фінансової інформації та протидії кіберзлочинності

(передбачає врахування міжнародних базових правових основ з мінімізації загроз впливу кіберзлочинності).

6. Принцип фінансової доцільності (передбачає пошук оптимального співвідношення між ефективністю системи захисту інформації та витратами на її становлення і функціонування).

Взаємодія держави та приватного сектора в сфері кібербезпеки здійснюється шляхом [247]:

- створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

- підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, комплексних знань, навичок і вмій, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

- обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

- партнерства та координації команд реагування на комп'ютерні надзвичайні події;

- залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проєктів та нормативних документів у сфері кібербезпеки;

- надання консультативної та практичної допомоги з питань реагування на кібератаки;

- формування ініціатив та створення авторитетних консультативних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

- запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

- періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

- створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

– тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

Спільні дії державного і приватного сектора щодо формування ефективної політики з інформаційної безпеки та розроблення й упровадження відповідних заходів, вдосконалення міжнародного та національного законодавства, організація державних і міжнародних підрозділів та структур у боротьбі з кіберзлочинами дадуть змогу ліквідувати чи значно скоротити фінансові втрати суб'єктів підприємництва від інформаційних загроз. Це своєю чергою сприятиме кращій протидії гібридним фінансовим конфліктам у їхній діяльності та дасть змогу підвищити рівень їхньої фінансової безпеки.

5.4. Пріоритетні напрями трансформації інституційно-правового забезпечення фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних загроз

Забезпечення фінансової безпеки суб'єктів підприємництва шляхом державного регулювання основних засад цього складного процесу є невід'ємним елементом політики національної безпеки в мирний час та набуває підвищеного значення в умовах воєнного стану. Оскільки фінансова система держави, важливою складовою якої є фінанси суб'єктів підприємництва, повинна швидко й ефективно трансформуватися відповідно до потреб оборони держави з метою подальшої протидії агресору. Відтак, важливість зміцнення ділових одиниць шляхом раціонального й дієвого в умовах нових викликів і загроз державного регулювання суттєво зростає.

Державне регулювання фінансової безпеки суб'єктів підприємництва передбачає передусім законодавчо оформлену систему зовнішнього впливу на неї з використанням сукупності методів прямого й опосередкованого впливу. Методи прямого регулювання використовують для безпосереднього втручання держави в економічні процеси та фінансову діяльність ділових одиниць. Такий вплив передбачає вжиття заходів із застосуванням інструментів правового й адміністративного регулювання. Відтак, правове регулювання передбачає діяльність держави щодо запровадження обов'язкових норм поведінки суб'єктів підприємництва шляхом

застосування правових методів. Ці методи використовують з метою створення правової бази, що гарантує фінансову безпеку ділових одиниць через ухвалення законодавчих та нормативних актів. Тож, така нормативно-правова база повинна бути адаптованою до умов сучасних викликів і загроз та передбачати відповідні механізми реалізації впроваджених законодавчих ініціатив та контролю за їхнім виконанням. Адміністративні методи (ліміти, квотування, обмеження цін, рентабельності, санкції, штрафи, соціальні стандарти тощо), що поділяють на заходи заборони, дозволу і примусу, повинні бути економічно обґрунтованими й переглядатись відповідно до динамічної зміни ситуації в країні. Зокрема, як ми виявили в попередніх розділах роботи, своєчасна зміна державної політики ціноутворення на ринку нафтопродуктів дала змогу подолати паливну кризу в державі, що виникла на початку військової агресії росії.

Необхідними також є методи опосередкованого впливу, що використовують з метою формування економічного середовища, яке сприяє зміцненню належного рівня фінансової безпеки ділових одиниць. Опосередковане регулювання застосовують за допомогою інструментів цінової, фіскальної, грошово-кредитної, інвестиційної та іншої політики, що передбачає запровадження системи податків, пільг в оподаткуванні, диференціювання податків, надання пільг у кредитуванні, маніпулювання обліковою ставкою, регулювання валютного курсу національної грошової одиниці, митне регулювання експорту й імпорту, визначення валютних курсів та умов обміну валют тощо. Під час війни більшість методів прямого та опосередкованого регулювання потребують перегляду їхнього застосування й вибору найбільш оптимального в складних воєнних умовах застосування.

Важливим в умовах військової агресії є правове регулювання фінансової безпеки ділових одиниць у контексті гарантування національної безпеки загалом. Розглядаючи правову базу, що регламентує складові національної безпеки, необхідно зауважити, що в Основному документі, який визначає напрями гарантування національної безпеки – Конституції України, поняття фінансової безпеки безпосередньо не згадуване (табл. 5.5). Зокрема, в ньому йдеться лише про засади гарантування національної безпеки, державної безпеки, економічної безпеки, інформаційної безпеки, екологічної безпеки, особистої безпеки людини, громадської безпеки.

Конституційні основи окремих складових національної безпеки

Складова національної безпеки	Стаття	Сутність конституційного положення
Громадська безпека, економічна безпека	13	Захист прав усіх суб'єктів права власності і господарювання, соціальна спрямованість економіки
Державна безпека, економічна безпека, інформаційна безпека	17	Захист суверенітету і територіальної цілісності України, гарантування її економічної та інформаційної безпеки
Громадська безпека	41	Захист прав володіння, користування і розпорядження власністю, результатами своєї інтелектуальної, творчої діяльності
Громадська безпека, економічна безпека, продовольча безпека	42	Захист прав ведення підприємницької діяльності, яка не заборонена законом, захист конкуренції у підприємницькій діяльності, прав споживачів щодо якості і безпечності продукції та всіх видів послуг і робіт
Економічна безпека	56	Захист прав на відшкодування за кошт держави чи органів місцевого самоврядування матеріальної та моральної шкоди, завданої незаконними рішеннями, діями чи бездіяльністю органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб при здійсненні ними своїх повноважень.

Джерело: сформувала автор на основі [119]

Серед складових національної безпеки, визначених у Конституції, найтісніше пов'язані з фінансовою безпекою економічний та інформаційний аспекти безпеки.

У Законі України “Про національну безпеку України” від 21 червня 2018 р. №2469-VIII [243] визначено поняття воєнного конфлікту, збройного конфлікту, воєнної безпеки, державної безпеки, загроз національній безпеці, національних інтересів, окреслено принципи, що визначають порядок формування державної політики у сферах національної безпеки й оборони.

У Законі України “Про Раду національної безпеки і оборони України” від 05 березня 1998 р. № 183/98-ВР [252] окреслено функції цього координаційного органу, згідно з якими він вносить пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки й оборони; здійснює координацію та контроль за діяльністю органів виконавчої влади у сфері національної безпеки й оборони у мирний час; координує та здійснює контроль за діяльністю органів виконавчої влади у сфері національної безпеки й

оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Важливим нормативно-правовим актом у сфері зміцнення фінансової безпеки суб'єктів господарювання є Закон України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення” від 06 грудня 2019 р. № 361-IX [226]. Цей Закон спрямований на захист прав і законних інтересів громадян, суспільства й держави, гарантування національної безпеки визначенням правового механізму протидії легалізації (відмиванню) доходів, одержаних злочинним способом, фінансуванню тероризму та розповсюдження зброї масового знищення, а також формування загальнодержавної аналітичної бази даних для надання правоохоронним органам України й іноземних держав змоги виявляти, перевіряти та розслідувати злочини, пов'язані з відмиванням коштів та іншими незаконними фінансовими операціями.

Захист прав суб'єктів підприємництва в сфері конкурентної боротьби регламентують Закони України “Про захист економічної конкуренції” від 11 січня 2001 р. № 2210-III та “Про захист від недобросовісної конкуренції” від 07 червня 1996 р. № 236/96, що визначають правові засади захисту економічної конкуренції та обмеження монополізму в господарській діяльності.

Протидія гібридному фінансовому конфлікту – корупції регламентується в Україні такими нормативно-правовими актами:

- Законом України “Про запобігання корупції” № 1700-VII від 14 жовтня 2014 р. [225], що обумовлює правові та організаційні засади функціонування системи запобігання корупції в Україні, зміст та порядок застосування превентивних антикорупційних механізмів, правила щодо усунення наслідків корупційних правопорушень;

- Законом України “Про Національне антикорупційне бюро України” від 14 жовтня 2014 р. № 1698-VII [241], що визначає правові основи організації та діяльності Національного антикорупційного бюро України;

- Наказом Офісу Генерального прокурора “Про затвердження Положення про Спеціалізовану антикорупційну прокуратуру Офісу Генерального прокурора” № 125 від 05 березня 2020 р., що окреслює основні завдання, функції та напрями діяльності цього державного органу [232].

Важливі аспекти фінансової безпеки суб'єктів підприємництва висвітлені в Господарському, Податковому, Кримінальному кодексах України, Кодексі України про адміністративні правопорушення, зокрема в частині протидії рейдерству, шахрайству, нелегальному банкрутству. Інформаційну складову фінансової безпеки суб'єктів підприємництва в Україні, зокрема захист від кіберзлочинності регламентує Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII від 05.10.2017 р. [247].

Рівень обґрунтованості державного регулювання фінансової безпеки суб'єктів підприємництва та його відповідність реаліям сьогодення в частині забезпечення нормативно-правового поля їхнього функціонування значно впливає на стан їхньої фінансової безпеки. Адже якщо відповідне законодавство становить єдину систему за взаємною узгодженістю норм та повнотою законодавчого регулювання підприємницької діяльності загалом і фінансової безпеки зокрема, то це створює сприятливі умови для здійснення фінансово-господарської діяльності ділових одиниць. Водночас, прогалини в законодавчій базі та невідповідність нормативно-правових норм політичній, економічній та воєнній ситуації в країні, навпаки, є джерелами ризиків та загроз фінансовій безпеці суб'єктів підприємництва, нерідко посилюючи дію негативних чинників зовнішнього середовища.

Окрім створення правового поля функціонування суб'єктів господарювання та забезпечення їх фінансової безпеки, держава впливає на ці процеси за допомогою відповідних інституцій, виконуючи низку завдань, зокрема: реалізує грошово-кредитну, бюджетну, податкову, інвестиційну, та інші складові державної політики; забезпечує стійкість фінансової системи до впливу світових та національних фінансових криз; нейтралізує вплив тіньових структур на національну фінансову систему, протидіє злочинам та адміністративним правопорушенням у фінансовій сфері.

Державні органи на різних рівнях та в різний спосіб впливають на фінансову безпеку суб'єктів підприємництва, водночас їх функції переплітаються між собою і нерідко дублюються. Відтак, з метою їхньої систематизації ми розробили структурно-логічну схему державного регулювання фінансової безпеки ділових одиниць за напрямками такого впливу та гілками влади (див. рис. 5.19). Зазначимо, що такий поділ є досить умовним, адже окремі державні органи виконують кілька функцій управління.



Рис. 5.19. Структурно-логічна схема функцій державного регулювання фінансової безпеки суб'єктів підприємництва

Джерело: розробила автор

Президент України, реалізуючи функцію забезпечення фінансової безпеки держави і функціонуючих в ній ділових одиниць у контексті забезпечення національної безпеки України, визначає стратегічні напрями її зміцнення, бере участь у створенні та реорганізації органів виконавчої влади, які забезпечують фінансову безпеку.

Передусім роль державних органів у реалізації захисту суб'єктів підприємництва від різноманітних загроз їхній фінансовій безпеці полягає в удосконаленні законодавства в частині господарських правопорушень, охорони інтелектуальної власності, захисту комерційної таємниці; поліпшенні системи державного фінансового моніторингу, забезпеченні ефективного регулювання ринків фінансових послуг. Цю функцію виконує Верховна Рада України.

Конституційний суд України, суди загальної юрисдикції здійснюють правосуддя щодо гарантування економічної безпеки особи, суспільства, держави, в тому числі її фінансової складової.

Забезпечення фінансової безпеки ділових одиниць залежить від ефективності роботи Національного банку України [242] в частині виконання таких важливих функцій, як здійснення грошово-кредитної політики держави; організація готівкового грошового обігу; запровадження правил проведення банківських операцій, бухгалтерського обліку і звітності, захисту інформації, коштів та майна; регулювання діяльності платіжних систем і систем розрахунків в Україні; валютне регулювання, зокрема, визначення порядку проведення операцій в іноземній валюті, організація і здійснення валютного контролю за банками та іншими фінансовими установами, які отримали ліцензію Національного банку на виконання валютних операцій тощо.

Основними завданнями Міністерства фінансів України в сфері регулювання фінансової безпеки суб'єктів підприємництва [229] є реалізація державної політики у сфері боротьби з правопорушеннями під час застосування податкового та митного законодавства, у сфері контролю за трансфертним ціноутворенням, запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення тощо.

Міністерство економіки України [194] забезпечує захист економічних прав і законних інтересів України та функціонуючих у країні ділових одиниць шляхом виконання низки таких функцій: формування державної

політики у сфері розвитку підприємництва, державної політики з контролю за цінами, державної регуляторної політики та державної політики з питань ліцензування, дозвільної системи, нагляду (контролю) у сфері господарської діяльності; формування та реалізації державної політики у сфері промислової безпеки; державної політики у сфері публічних закупівель тощо.

Важливу роль у забезпеченні фінансової безпеки суб'єктів господарювання відіграє Міністерство юстиції України [231], яке забезпечує формування та реалізацію державної правової політики з питань банкрутства, уживає заходів із протидії рейдерству, запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (щодо адвокатських бюро, адвокатських об'єднань та адвокатів, які здійснюють адвокатську діяльність індивідуально; нотаріусів; суб'єктів господарювання, що надають юридичні послуги; осіб, які надають послуги щодо створення, забезпечення діяльності або управління юридичними особами) тощо.

Державним правоохоронним органом, на який покладено запобігання, виявлення, припинення, розслідування та розкриття корупційних правопорушень, що стосуються його підслідності, є Національне антикорупційне бюро України. Завдання цього державного органу влади – протидія кримінальним корупційним правопорушенням, які вчинені вищими посадовими особами, уповноваженими на виконання функцій держави або місцевого самоврядування, та становлять загрозу національній безпеці. Відтак, Національне антикорупційне бюро України виконує такі основні функції [241]: уживає оперативно-розшукових заходів з метою запобігання, виявлення, припинення та розкриття кримінальних правопорушень, віднесених законом до його підслідності; проводить досудове розслідування таких кримінальних правопорушень; уживає заходів щодо розшуку й арешту коштів та іншого майна, які можуть бути предметом конфіскації або спеціальної конфіскації у кримінальних правопорушеннях, віднесених до його підслідності тощо. Національне антикорупційне бюро України взаємодіє з іншими державними органами при реалізації своїх функцій, зокрема з Національним банком України, Фондом державного майна України, Антимонопольним комітетом України, Національним агентством з

питань запобігання корупції, органами Державної прикордонної служби, органами державної фіскальної і митної служби тощо. Національне агентство з питань запобігання корупції своєю чергою відповідальне перед Верховною Радою України і є підконтрольним їй та підзвітним Кабінету Міністрів України. До його повноважень належать: аналізування стану запобігання та протидії корупції в Україні, розроблення проектів Антикорупційної стратегії та державної програми з її виконання, формування та реалізація антикорупційної політики, розроблення проектів нормативно-правових актів з цих питань; організація досліджень з питань вивчення ситуації щодо корупції; проведення моніторингу та контролю за виконанням актів законодавства з питань етичної поведінки, запобігання та врегулювання конфлікту інтересів у діяльності осіб, уповноважених на виконання функцій держави або місцевого самоврядування, та прирівняних до них осіб тощо.

Національне агентство України з питань виявлення, розшуку та управління активами [240], одержаними від корупційних та інших злочинів формує та реалізує державну політику у сфері виявлення й розшуку активів, які можуть бути арештовані у кримінальному провадженні, а також управління активами, які арештовані у кримінальному провадженні.

З метою забезпечення прозорих умов роботи бізнесу та запобігання корупції в Україні було створено Раду бізнес-омбудсмена [186]. Цей незалежний консультативно-дорадчий орган Кабінету Міністрів України фінансується з Мультидонорського рахунку стабілізації та сталого розвитку України (МДР), розпорядником якого є ЄБРР. Країнами-донорами МДР є Данія, Фінляндія, Франція, Німеччина, Італія, Японія, Нідерланди, Норвегія, Польща, Швеція, Швейцарія, Великобританія, США. Основними функціями Ради бізнес-омбудсмена в контексті забезпечення фінансової безпеки суб'єктів підприємництва є представлення та захист їхніх інтересів у державних органах.

Державна податкова служба України реалізує політику в сфері оподаткування щодо контролю за надходженням до бюджетів та державних цільових фондів, податків, зборів, платежів; контролю за своєчасністю здійснення розрахунків в іноземній валюті, дотриманням порядку проведення готівкових розрахунків за товари (послуги), а також

за наявністю ліцензій на провадження видів господарської діяльності, що підлягають ліцензуванню, торгових патентів тощо [233].

Функції щодо протидії правопорушенням, які посягають на функціонування економіки держави та фінансову безпеку суб'єктів підприємництва виконує також Бюро економічної безпеки України. До його основних завдань належать [215]: оцінювання ризиків і загроз економічній безпеці держави і ділових одиниць, напрацювання способів їх мінімізації та усунення; запобігання, виявлення, припинення, розслідування кримінальних економічних правопорушень.

Координаційним органом з питань національної безпеки й оборони при Президентові України є Рада національної безпеки і оборони України, основними функціями якого є [252]: визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки й оборони у політичній, економічній, соціальній, воєнній, науково-технологічній, екологічній, інформаційній та інших сферах; внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки й оборони; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки й оборони у мирний час та в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Центральним органом виконавчої влади зі спеціальним статусом з питань фінансового моніторингу є Державна служба фінансового моніторингу України, на яку покладено такі завдання [228]: реалізація державної політики у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення; внесення на розгляд Міністра фінансів пропозицій щодо забезпечення формування державної політики у цій сфері; збирання, аналіз інформації про фінансові операції, що підлягають фінансовому моніторингу; проведення національної оцінки ризиків тощо. Державна служба фінансового моніторингу України співпрацює з іншими державними органами України та компетентними органами іноземних держав та міжнародними організаціями у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

Гарантування фінансової безпеки суб'єктів господарювання на ринку фінансових послуг покладено на Національну комісію з цінних паперів та фондового ринку [244], основними завданнями якої є реалізація державної політики щодо розвитку та функціонування ринку цінних паперів і похідних (деривативів) в Україні; здійснення державного регулювання та контролю за емісією та обігом цінних паперів і похідних (деривативів); захист прав інвесторів шляхом здійснення заходів щодо запобігання і припинення правопорушень на ринку цінних паперів тощо.

Протидія недобросовісній конкуренції як одному із поширених на сьогодні гібридних фінансових конфліктів реалізується Антимонопольним комітетом України, на який покладено такі функції [214]: здійснення державного контролю за дотриманням законодавства про захист економічної конкуренції на засадах рівності суб'єктів господарювання перед законом; контролю за концентрацією, узгодженими діями суб'єктів господарювання та дотриманням вимог законодавства про захист економічної конкуренції під час регулювання цін (тарифів) на товари, що виробляються (реалізуються) суб'єктами природних монополій; контролю щодо створення конкурентного середовища та захисту конкуренції у сфері публічних закупівель.

У частині протидії корупції реалізує відповідні функції також Спеціалізована антикорупційна прокуратура, зокрема здійснює нагляд за додержанням законів під час проведення оперативно-розшукової діяльності, досудового розслідування кримінальних правопорушень Національним антикорупційним бюро України [232].

Згідно з Законом України “Про розвідку” № 912-XI від 17.09.2020 р. Головне управління розвідки Міністерства оборони України виконує такі ключові завдання в сфері гарантування фінансової безпеки держави та суб'єктів підприємництва [253]: проводить збір, аналітичне опрацювання й надання розвідувальної інформації, реалізує заходи з метою сприяння реалізації національних інтересів України, забезпечення безпеки; виявляє і визначає ступінь зовнішніх загроз національній безпеці України, у тому числі у кіберпросторі; бере участь у боротьбі з тероризмом, протидії розвідувально-підривної діяльності проти України, транснаціональній організованій злочинності та іншій злочинній діяльності, що становлять зовнішню загрозу національній безпеці України. Головне управління розвідки співпрацює також із компетентними органами іноземних держав

та міжнародними організаціями з метою забезпечення національної безпеки України.

До розвідувальних органів у сфері забезпечення фінансової безпеки як складової національної безпеки належить також Служба зовнішньої розвідки України, що здійснює розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах [255].

Функції захисту інтересів держави, суб'єктів підприємництва та населення покладено на Міністерство цифрової трансформації України [230] і Кіберполіцію, яка функціонує як структурний підрозділ Національної поліції України й забезпечує захист прав і свобод громадян, інтересів суспільства й держави від кримінально протиправних посягань у кіберпросторі [245].

Важливим при розробленні стратегії забезпечення фінансової безпеки держави й ділових одиниць є її наукове обґрунтування, що повинно ґрунтуватися на аналізі викликів і загроз в умовах гібридних агресій та реалізується сукупністю вітчизняних науково-дослідних установ.

Аналіз наукових підходів до державного регулювання фінансової безпеки суб'єктів підприємництва [11; 21; 24; 30; 49; 58; 60; 61; 111; 115; 127; 157] та вивчення функцій, які виконує низка державних органів України в цій сфері дав змогу виявити тісний взаємозв'язок між ними, координацію та співпрацю, яку необхідно в окремих аспектах посилити й удосконалити механізм такої взаємодії з метою уникнення дублювання обов'язків.

Відтак, можемо констатувати, що фінансова безпека суб'єктів підприємництва є результатом комплексної дії їхніх внутрішніх управлінських служб та державного регулювання. Органи державної влади, формуючи ефективну законодавчу базу в сфері зміцнення фінансової безпеки держави та ділових одиниць й упроваджуючи дієві механізми захисту прав власників в Україні, позитивно впливають на їх фінансовий стан і фінансові результати, підвищують рівень довіри інвесторів до національних підприємств, що своєю чергою, сприяє збільшенню інвестиційних вкладень в економіку та її розвитку.

Водночас українське суспільство загалом й уся система інституційно-правового забезпечення його функціонування зазнали радикальних трансформацій з початком повномасштабного вторгнення росії в Україну.

Це зумовило не лише перебудову системи цивільного захисту України [142], а й реформатування політики реалізації її фінансових інтересів. Відтак, підхід до державного регулювання фінансової безпеки суб'єктів підприємництва, який був застосований у мирний час, також зазнав змін, оскільки не відповідає вимогам воєнного стану.

Від початку війни значна кількість ділових одиниць на Сході, Півдні та Півночі України опинились у зоні бойових дій, зазнали обстрілів й масштабних руйнувань. З метою збереження їх виробничих було впроваджено державну програму релокації (евакуації) підприємств у більш безпечні області [227.]. Згідно з програмами релокації передбачено такі види державної підтримки для постраждалих підприємств: підбір місця розташування для виробничих потужностей; допомогу з перевезенням на нову локацію; сприяння в розселенні працівників та пошуку нових співробітників; підтримку у відновленні логістики, закупівлі сировини та пошуку ринків збуту. Своєю чергою, обласні військові адміністрації вивчають та за можливості задовольняють потреби суб'єктів підприємництва у релокації. Відтак, до програми релокації бізнесу в Україні вже долучилася низка областей, а саме: Закарпатська, Івано-Франківська, Львівська, Тернопільська, Хмельницька, Чернівецька, Вінницька, Волинська, Рівненська, Київська, Дніпропетровська, Черкаська, Полтавська та Кіровоградська області.

За даними Міністерства економіки [92] станом на 24.10.2022 р. було зареєстровано 1 863 заявки підприємств на переміщення, 623 з цих підприємств відмовилися від релокації у зв'язку з деокупацією територій, на яких вони розташовані. За програмою релокації в більш безпечні регіони переміщено 761 підприємство, 80 % з яких відновили роботу на новому місці. Серед переміщених суб'єктів підприємництва, які відновили свою діяльність на новому місці, найбільшу частку становлять [92]: підприємства у сфері оптової та роздрібної торгівлі, ремонту автотранспортних засобів і мотоциклів (40,24 % від загальної кількості релокованих підприємств); переробної промисловості (31,71 %); інформації та телекомунікацій (6,34 %); професійної, наукової та технічної діяльності (5,85 %); будівництва (4,15 %).

Щодо оцінки релокованих ділових одиниць у регіональному розрізі, то найбільше підприємств релокувалося до Львівської (30 % релокованих підприємств), Закарпатської (17 %), Чернівецької (11 %), Івано-

Франківської (8 %), Хмельницької (7 %) та Тернопільської (7 %) областей [92].

Відповідно до Порядку надання фінансової державної підтримки суб'єктам підприємництва, затвердженого постановою Кабінету Міністрів України від 24.01.2020 р. № 28 [211] під час війни розширено можливості отримання діловими одиницями державної фінансової підтримки.

З метою дослідження особливостей державного регулювання в умовах воєнного стану діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні ми розробили логіко-історичну схему періодизації умов їх функціонування (рис. 5.20).

Відповідно до проведеного аналізу функціонування досліджуваних суб'єктів підприємництва виявлено, що в довоєнний час на ринку цього сектора економіки спостерігалися прояви недобросовісної конкуренції, він характеризувався різним ціновим позиціонуванням його учасників унаслідок використання окремими господарюючими суб'єктами схем ухилення від оподаткування та обманювання споживачів приховуванням дефектів якості. З початком війни припинилися поставки нафтопродуктів з росії і білорусі, відбулось різке спустошення запасів пального на АЗС, що спричинило його тривалий дефіцит у країні. Окрім того, початковий етап війни характеризувався проблемами логістики та нестачею транспорту для доставки пального.

Державне регулювання полягало, передусім, в урядовій лібералізації формули розрахунку максимально дозволених цін пального на початку війни та подальшого його скасування з метою наповнення ринку України нафтопродуктами, а також тимчасового встановлення нульової ставки акцизного податку на паливо та зниженні ставки ПДВ з 20 % до 7 %.

Окрім того, було спрощено отримання ліцензій на автоперевезення, а саме вдвічі скорочено обсяг необхідних для отримання ліцензії документів, скасовано необхідність підтвердження трирічного досвіду роботи, ліквідовано подання документів про наявність матеріально-технічної бази та наявність договорів, а термін розгляду заявки на отримання ліцензії за новою процедурою скорочено з 10 днів до 1–3 днів.

Довосний період	до 24.02.22 р.	<ul style="list-style-type: none"> висококонкурентний ринок з різним ціновим позиціонуванням учасників, верхня межа якого обмежена державним регулюванням; прояви недобросовісної конкуренції в частині демпінгування цін на пальне внаслідок використання схем ухилення від оподаткування та обманювання споживачів приховуванням дефектів якості (сурогатне паливо).
Шокові дії після вторгнення рф в Україну	26.02.–02.04.2022 р.	<ul style="list-style-type: none"> максимально можливі продажі на АЗС при обмеженні відпуску в одні руки; різке спустошення запасів пального на АЗС.
Вичерпування внутрішніх резервів пального в Україні	26.02.–02.04.2022 р.	<ul style="list-style-type: none"> переорієнтація з російських та білоруських джерел постачання на Кременчуцький нафтопереробний завод; зниження державних стандартів щодо якості пального в умовах його дефіциту до рівня евро-3; втрата окремих об'єктів (нафтобаз та АЗС) в зоні активних бойових дій (Київська, Чернігівська, Харківська, Херсонська, Сумська області); зростання цін на паливо; урядова лібералізація формули розрахунку максимально дозволеної ціни пального на АЗС для уможливлення імпорту з Європи (11.03.2022 р.) скасування акцизного податку на пальне та зниження ПДВ з 20% до 7% (15.03.2022 р.) з метою послаблення впливу зростання цін на пальне.
Налагодження європейських логістичних ланцюгів постачання пального	02.04–17.05.2022 р.	<p>повна зупинка функціонування Кременчуцького нафтопереробного заводу через масштабні ракетні обстріли та знищення його інфраструктури (02.04.2022 р.);</p> <p>штучне обмеження реалізації пального АЗС по невідгидним регулюванням державою цінам з одночасною появою “сірого” ринку пального по вищим цінам;</p> <p>переговори зі світовими компаніями щодо постачання пального в Україну;</p> <p>скасування дозволів на проїзд через територію Польщі для вантажівок, що здійснюють перевезення пального (06.05.2022 р.);</p> <p>створення режиму прискореного пропуску палива на пунктах перетину кордону з Україною.</p>
Державне сприяння імпорту пального та розширення логістичних можливостей і наповнення українського ринку паливом	17.05- червень 2022 р.	<ul style="list-style-type: none"> скасування державного регулювання цін на паливо (17.05.2022 р.); зростання цін на АЗС та мінімізація “сірого” ринку палива (легалізація економічно обритуваних цін на пальне внаслідок скасування державного регулювання цін); включення ембарго на постачання російської нафти до пакета санкцій ЄС проти росії, відповідно до якого дві третини імпорту (який надходить морським шляхом) припинено негайно і до 90% – до кінця 2022 р. (01.06.2022 р.). Послаблення отримали Угорщина, Словаччина та Чехія. Також окремий дозвіл на купівлю російської нафти до кінця 2024 р. отримала Болгарія через особливості роботи її нафтопереробного заводу. додолучення до схвалення шостого пакету санкцій Євросоюзом проти росії, що включає ембарго на російську нафту також Швейцарії (10.06.2022 р.); зростання кількості імпортерів пального та насичення українського ринку паливом.

Рис.5.20. Логіко-історична схема періодизації умов функціонування суб'єктів підприємництва що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні в умовах воєнного стану

Джерело: розробила автор

Водночас необхідно акцентувати на міжнародній підтримці європейських країн у подоланні паливної кризи в Україні на початку війни як на державному рівні у формі запроваджених проти агресора санкцій, так і на рівні європейських ділових одиниць, з якими вдалося в короткі терміни налагодити ділове партнерство. Відтак, на основі аналізу досліджуваних підприємств, можемо зробити висновок, що вітчизняні ділові одиниці, які займаються виробництвом та оптовою і роздрібною торгівлею паливом на сьогодні повністю перелаштувались на нові ринки постачання з європейських країн, таких як Литва, Польща, Румунія, Німеччина, Болгарія, Австрія та ін.

Тож, можемо констатувати, що спільними заходами на рівні держави та вітчизняних ділових одиниць, а також міжнародних партнерів суб'єкти підприємництва цієї галузі продовжують успішно функціонувати, генеруючи позитивний економічний ефект для подальшої протидії агресору.

ВИСНОВКИ

За результатами дослідження зроблено теоретичне узагальнення і запропоновано нове вирішення науково-прикладної проблеми, пов'язаної з поглибленням теоретико-методологічних і науково-прикладних засад забезпечення фінансової безпеки суб'єктів підприємництва в Україні.

1. Встановлено, що у кожному суспільстві складно переплетені різноманітні економічні інтереси, рівень урівноваження яких зумовлює подальший розвиток як окремих індивідів та суб'єктів господарювання, так і держави в цілому. З'ясовано, що в підприємницькій діяльності складовою частиною економічних інтересів ділових одиниць є фінансові інтереси, які є формою прояву об'єктивних потреб й спонукальним мотивом їхньої фінансово-господарської діяльності. Водночас у сучасних економічних умовах, ускладнених постпандемічним періодом й воєнним станом, фінансові інтереси суб'єктів підприємництва можуть бути суперечливими та незбалансованими з інтересами інших учасників ринку і їхнім персоналом. Неузгодження фінансових інтересів суб'єктів господарювання з фінансовими інтересами дотичних до їхньої діяльності структур може призвести до виникнення різного роду конфліктних ситуацій та зумовлювати проблеми фінансової безпеки.

2. Запропоновано під фінансовим конфліктом розуміти протистояння суб'єктів фінансових відносин, що виникає в процесі здійснення ними фінансово-господарської діяльності внаслідок несумісності інтересів та ціннісних орієнтирів. Фінансові конфлікти систематизовано за низкою ознак (суб'єктами, сферою й природою виникнення, рівнем взаємодії учасників, відношенням до суб'єкта підприємництва, тривалістю, організаційно-правовою формою ділової одиниці, рівнем впливу на фінансову безпеку) з виокремленням нових класифікаційних критеріїв – наслідками, результативністю й множинністю важелів впливу на фінансову безпеку суб'єктів підприємництва.

3. Доведено, що глобалізація, стрімка цифровізація усіх економічних процесів та радикальні зміни у сфері безпеки призвели до появи низки фінансових протистоянь, характерною ознакою яких є перехід до використання гібридних важелів впливу на досягнення бажаних результатів фінансового конфлікту. Тому в сучасних реаліях доцільним є виокремлення гібридних фінансових конфліктів у самостійну галузь

наукового пізнання та введення в її термінологічний апарат поняття “гібридний фінансовий конфлікт”, під яким запропоновано розуміти протистояння, що виникає у фінансових відносинах, має переважно прихований характер і передбачає скоординоване застосування множинності методів впливу з метою реалізації тіньових фінансових інтересів його учасників.

4. Визначено найпоширеніші гібридні фінансові конфлікти в сучасних умовах господарювання (рейдерство, недобросовісна конкуренція, фінансове шахрайство працівників, корупція, конфлікти з інститутами фінансово-кредитної сфери, державними органами, відмивання доходів, отриманих злочинним шляхом) та наголошено на важливості врахування в перелічених гібридних конфліктах впливу інформаційних загроз.

5. Сформульовано концептуальний підхід щодо структурно-компонентного аналізу гібридних фінансових конфліктів на основі методів експертної оцінки суб’єктів підприємництва, що дало можливість сформулювати їхню узагальнену характеристику за низкою спільних ознак (злочинна діяльність, спрямована на фінансову сферу; прихований характер; фальсифікація документів; наявність несанкціонованих операцій; використання фактора недобросовісного персоналу; зловживання з конфіденційною інформацією; психологічні маніпуляції) і деструктивних наслідків для фінансової безпеки ділових одиниць.

6. Акцентовано, що в умовах гібридних агресій та воєнного стану в Україні трансформується підхід до забезпечення фінансової безпеки суб’єктів підприємництва, що вимагає утримання їхньої динамічної фінансової рівноваги та постійного пошуку балансу власних фінансових інтересів з інтересами інших учасників конкурентного економічного середовища. В цьому контексті поглиблено розуміння сутності поняття “фінансова безпека суб’єктів підприємництва”, під яким запропоновано розуміти їхню спроможність зберігати динамічну фінансову рівновагу та рівновагу в гібридних фінансових конфліктах.

7. Констатовано, що оскільки забезпечення фінансової безпеки суб’єктів підприємництва передбачає одночасне досягнення двох незалежних цілей – динамічної фінансової рівноваги і рівноваги в гібридних фінансових конфліктах, методологія наукового дослідження проблем фінансової безпеки ділових одиниць повинна реалізовуватись із врахуванням фінансового та соціально-психологічного підходів. На цій

основі для аналізу стану фінансової безпеки суб'єктів господарювання запропоновано використовувати концептуальну модель “Колесо рівноваги суб'єктів підприємництва в гібридних фінансових конфліктах”, що побудована на основі найбільш поширених на сьогодні гібридних фінансових конфліктів. Модель дає можливість з'ясувати рівень досягнення поставлених цілей у протидії кожному із цих конфліктів, виявити негативний вплив на стан фінансової безпеки нераціональних рішень власників та керівництва внаслідок їхніх поведінкових упереджень та тіньових інтересів інших учасників ринку, а також відстежити динаміку розвитку ділових одиниць упродовж їхнього життєвого циклу.

8. Обґрунтовано, що при дослідженні гібридних фінансових конфліктів важливим є історичний аналіз взаємопов'язаної сукупності ознак та фактів за низку періодів. У цьому контексті як альтернативний метод наукового пізнання чинників фінансової безпеки суб'єктів підприємництва запропоновано використовувати метод історичної абдукції, сформований на двокомпонентному поєднанні фактора часу при вивченні умов виникнення, формування й розвитку чинників фінансової безпеки суб'єктів підприємництва та фактора встановлення абдуктивного висновку, що ґрунтується на здійсненні міркування від наявних даних до вибору однієї із альтернативних гіпотез, яка пояснює їх найоптимальніше.

9. Ідентифіковано типові види фінансового шахрайства в діяльності суб'єктів підприємництва, що дало можливість систематизувати причини його виникнення на ті, які пов'язані з неякісною кадровою перевіркою під час приймання на роботу, зумовлені проблемами формування корпоративної культури; спричинені прогалинами менеджменту. Встановлено, що до ранніх ознак фінансового шахрайства належать: наявність несанкціонованих операцій, відсутність первинних документів, використання підписаних незаповнених бланків документів, необґрунтоване коливання цін, значний немотивований обсяг наданих знижок, зокрема окремим контрагентам, співпраця з партнерами зі сумнівною діловою репутацією, відсутність прозорого механізму закупівель.

10. Встановлено, що рейдерство як гібридний фінансовий конфлікт щодо зміни контролю над фінансово-господарською діяльністю суб'єкта підприємництва й заволодіння його активами постійно змінює свою форму та еволюціонує разом із економічними і політичними процесами в

країні. Сучасне рейдерство є багатограним процесом, в якому використовуються різноманітні методи протиправного захоплення підприємств, зокрема корупційні технології взаємодії з державними органами, кіберзлочини, економічне шпигунство, кримінальні схеми тощо. На основі ретроспективного аналізу рівня захисту прав власності в Україні впродовж 2010–2022 рр. виявлено доволі низькі позиції держави в міжнародному рейтингу захисту прав власності. Попри те, що в 2020 р. оцінка міжнародного індексу захисту прав власності (IPRI) дещо зросла порівняно з 2019 р. до значення 4,466, що становило 22-ге місце в регіоні Центрально-Східної Європи та Центральної Азії та 105-те у світі, в останні два роки значення IPRI знизилося до 4,453 – у 2021 р. та 3,980 у 2022 р. Визначено, що низький рівень захисту прав власності в Україні пов'язаний передусім із тривалими складними стагнаційними процесами в правовому середовищі, відсутністю єдиного підходу до розслідування рейдерства (визначення цього терміна не закріплено на законодавчому рівні і не визначено у Кримінальному кодексі України як окреме кримінально-каране діяння, його розслідування провадиться за ознаками супутніх злочинів, передбачених іншими статтями Кримінального кодексу) та політичною й соціально-економічною нестабільністю, зумовленою військовою агресією росії.

11. Аргументовано, що в складних умовах мінливості та невизначеності ринкового середовища складно забезпечити баланс фінансових інтересів між діловими одиницями, що конкурують в одній галузі, особливо в умовах постпандемічного періоду й гібридних агресій. Досить часто суб'єкти підприємництва застосовують нелегальні або умовно легальні методи конкурентної боротьби, що дає можливість одному із учасників ринку одержати комерційної вигоди і забезпечити краще становище на ринку обманом споживачів, партнерів, державних органів. Тому серед вагомих загроз фінансовій безпеці суб'єктів підприємництва у сфері відносин власності, варто виокремлювати недобросовісну конкуренцію, під якою запропоновано розуміти гібридний фінансовий конфлікт між суб'єктом підприємництва та його конкурентами, що виникає внаслідок порушення чинного законодавства й норм ділового етикету останніми з метою одержання неправомірних конкурентних переваг, комерційної вигоди і забезпечення домінуючого (монопольного) становища на ринку.

12. Доведено, що в умовах гібридних загроз зловмисники різного рівня, використовуючи інформаційні технології, можуть використовувати кіберзлочини як важелі впливу в гібридних фінансових конфліктах й суттєво знижувати рівень фінансової безпеки як ділових одиниць, так і дестабілізувати фінансові системи окремих країн. З метою посилення фінансової стійкості держави та підвищення рівня фінансової безпеки суб'єктів підприємництва необхідно максимально нівелювати вплив інформаційних загроз на їх функціонування. Обґрунтовано необхідність розширення та доповнення підходів до систематизації кіберзлочинів відповідно до проявів гібридних агресій на міждержавному рівні й на рівні ділових одиниць й запропоновано їхню класифікацію шляхом уточнення суб'єктів таких злочинних дій (держави та підконтрольні їм угруповання, суб'єкти підприємництва і наймані ними кіберзлочинці, терористичні групи, хактивісти).

13. Визначено та розкрито етапи функціонування суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні від початку війни й розроблено логіко-історичну схему оперативного-тактичних заходів щодо їхнього виходу з кризи із виокремленням організаційно-економічних заходів на кожному із встановлених етапів (початок війни, організаційно-економічна мобілізація суб'єкта підприємництва, гостра криза, лібералізація ціноутворення). Встановлено дієвість сукупності заходів, реалізованих діловими одиницями та державними органами влади у стабілізованні економічної ситуації на початку військової агресії й обґрунтовано необхідність розроблення стратегічних орієнтирів забезпечення фінансової безпеки України та суб'єктів підприємництва в подальшій протидії агресору.

14. Запропоновано методикау стратегічного оцінювання рівня фінансової безпеки ділових одиниць із врахуванням фінансового та соціально-психологічного підходів. Згідно з цією методикою рівень фінансової безпеки рекомендовано визначати діагностуванням фінансової рівноваги суб'єктів підприємництва шляхом оцінки фінансових показників, визначенням показника ефективності протидії гібридним фінансовим конфліктам експертним методом, а також розрахунком інтегрального показника ефективності управління фінансовою безпекою суб'єктів підприємництва. Методика дає змогу здійснити комплексний аналіз рівня фінансової безпеки ділових одиниць, враховуючи не лише

фінансові параметри їхнього розвитку, але й поведінкові аспекти ухвалення управлінських рішень й деструктивні дії зловмисників. Окрім того, використання запропонованого аналітичного інструментарію дає змогу порівняти результати встановленого рівня фінансової безпеки, отримані згідно з двома концептуальними підходами, виявити збалансованість чи її відсутність між фінансовою та безпековою складовою політики управління на досліджуваних підприємствах, встановити причини можливої невідповідності й усунути їх.

15. Доведено взаємозв'язок між досліджуваними гібридними фінансовими конфліктами в підприємницькій діяльності й обґрунтовано необхідність агрегування організаційно-економічного інструментарію протидії фінансовим конфліктам в умовах сучасних викликів і загроз. З цією метою розроблено типові сценарії впровадження організаційно-економічних заходів протидії гібридним фінансовим конфліктам у діяльності суб'єктів підприємництва. Єдиний уніфікований підхід до стратегічного й оперативного-тактичного реагування на прояви фінансового шахрайства, рейдерства, корупції та недобросовісної конкуренції сприятиме їх своєчасному виявленню, запобіганню й нейтралізації деструктивного впливу на фінансову безпеку суб'єктів підприємництва в процесі євроінтеграції та глобалізаційних змін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абляев Е. А., Яструбецька Л. С. Систематизація фінансових конфліктів у корпоративних відносинах. *Інтегрований підхід до модернізації науки: методи, моделі та мультидисциплінарність* : матеріали Міжнар. наук.-практ. конференції. International scientific journal “Grail of Science”. 2022. № 23. Р. 50–54.
2. Абляев Е. А., Яструбецька Л. С. Сутність та причини фінансових конфліктів у діяльності компаній. *Наукова робота вчених-гуманітаріїв* : матеріали Міжнар. наук. конф. Видавництво “ACADEMCONF.COM”. № 12. 2022. С. 24–31.
3. Актуальні проблеми боротьби з корупцією в Україні: монографія / В. М. Гаращук, А. О. Мухатаєв ; Нац. акад. прав. наук України, Ін-т вивч. пробл. злочинності, Служба безпеки України, Ін-т дослідж. пробл. держ. безпеки. Харків : Право, 2010. 143 с.
4. Андреев Д. О. Адміністративно-правові засоби захисту прав власників цінних паперів : автореф. дис. ... канд. юрид. наук : спец. 12.0.07 “адміністративне право і процес; фінансове право; інформаційне право”. Київ, 2008. 20 с.
5. Антикризове фінансове управління в системі суб’єктів економічної діяльності : методи та інструменти оцінювання : [монографія] / В. В. Коваленко, М. В. Суганяка, В. І. Фучеджи. Одеса : Атлант, 2013. 458 с.
6. Антипов В. І. Тіньова економіка та економічна злочинність : світові тенденції, українські реалії та правові засоби контролю (теоретико-методологічне узагальнення). Вінниця : ДП ДКФ, 2006. 1040 с.
7. Баб’як Я. Б., Яструбецька Л. С. Аналіз особливостей залучення вітчизняними підприємствами банківських кредитів. *Молодий вчений*. 2015. № 12 (2). С. 195–198. URL : <http://surl.li/eptcq>
8. Базалук О. Теорія війни та миру. Геофілософія Європи. Київ : МФКО, 2016. 246 с.
9. Баконіна О. Огляд ринку компаній з конкурентної розвідки. ІТ-платформа для управління інформацією та мінімізації ризиків

- компаній. URL : https://jurliga.ligazakon.net/intervyu/196268_oglyad-rinku-kompany-z-konkurentno-rozvdki (дата звернення: 07.07.2020 р.).
10. Банківська система : [підручник] / М. І. Крупка, Є. М. Андрущак, Н. Г. Пайтра, Л. С. Яструбецька [та ін.] ; [за ред. д-ра екон. наук, проф. М. І. Крупки]. Львів : ЛНУ імені Івана Франка, 2013. 556 с.
 11. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : [монографія]. Київ : Київ. нац. торг.-екон. ун-т, 2004. 759 с.
 12. Безух О. В. Захист від недобросовісної конкуренції у сфері промислової власності : автореф. дис. ... канд. юрид. наук : 12.00.04. Донецьк, 2001.
 13. Бережний Я. В. Перспективи забезпечення прав власності як підґрунтя для розвитку підприємницької діяльності в Україні. *Аналітична записка*. Національний інститут стратегічних досліджень при Президентові України. 2014. URL : <http://www.niss.gov.ua/articles/1659/> (дата звернення 14.06.2018 р.).
 14. Берлач Ю. А. Адміністративно-правове забезпечення протидії рейдерству в Україні : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2014. 205 с.
 15. Білик М. Д. Фінансовий аналіз : навч. посібник. Київ : КНЕУ, 2005. 592с.
 16. Біляк Ю. В. Основні загрози фінансовій безпеці корпоративних фінансів. *Агросвіт*. 2017. № 12. С. 20–30.
 17. Біляк Ю. В. Специфіка корпоративного рейдерства як процес отримання юридичного та фізичного контролю над майном, бізнесом проти волі власника підприємства. *Ефективна економіка*. 2013. № 5. URL : http://nbuv.gov.ua/UJRN/efek_2013_5_41 (дата звернення: 10.09.2020 р.).
 18. Бланк І. О. Управління фінансовою безпекою підприємства. 2-ге вид. Київ : Ельга, 2009. 778 с.
 19. Бланк І. О. Управління фінансовою безпекою підприємства. Київ : Ніка-Центр; Ельга, 2004. 784 с.
 20. Бланк І. О. Фінансова стратегія підприємства : монографія. Київ : Ельга, Ніка-Центр, 2004. 720 с.

21. Бойко В. В. Пріоритети та інструменти розвитку сільських територій в системі забезпечення економічної безпеки України : монографія. Львів : Видавництво ННБК “АТБ”, 2017. 426 с.
22. Бойко І. Україну атакують дві групи російських хакерів. Офіційна сторінка інформаційного агентства UNIAN. URL : <https://www.unian.ua/war/kiberataki-na-ukrajinu-2022-ukrajinu-atakuyut-dvi-grupi-rosiyskih-hakeriv-derzhspeczv-yazku-novini-vtorgnennya-rosiji-v-ukrajinu-11761861.html> (дата звернення: 28.05.2022 р.).
23. Бондарчук Н., Гуменчук М. Сутність фінансово-економічної безпеки підприємства та необхідність її забезпечення. *Ефективна економіка*. 2016. № 11. URL : <http://www.economy.nayka.com.ua/?op=1&z=5409> (дата звернення: 05.07.2020).
24. Варналій З. С., Кіслова А. О. Реформування податкової системи як чинник забезпечення фінансової безпеки України. *Міжнародний науковий журнал “Інтернаука”*. 2021. № 12 (56), 1 т. С. 14–22. (Серія: “Економічні науки”). URL : <https://doi.org/10.25313/2520-2294-2021-12-7786> (дата звернення: 20.01.2022 р.).
25. Варналій З., Самвелян О. Запобігання фінансовому шахрайству в системі зміцнення фінансової безпеки України. *Міжнародний науковий журнал “Інтернаука”*. 2021. № 12 (56), 1 т. С. 23–32. (Серія: “Економічні науки”). URL : <https://doi.org/10.25313/2520-2294-2021-12-7796> (дата звернення: 01.02.2022 р.).
26. Варналій З. С. Економічна та фінансова безпека України в умовах глобалізації. Київ : Знання України, 2020. 423 с.
27. Варналій З. С. Основні форми та шляхи протидії інституціональним деформаціям фінансової безпеки України. *Фінансова безпека в системі забезпечення національних інтересів: проблеми та перспективи* : Матеріали Міжнар. наук.-практ. конф., 18–19 квітня 2012 р. Полтава : ПолтНТУ, 2012. 184 с.
28. Варналій З. С. Теоретичні засади детінізації економіки України. *Вісник Вінницького політехн. ін-ту*. 2014. № 1. С.46–53.
29. Варналій З. С., Андреев О. О. Фінансова безпека підприємства: сутність та формування системи забезпечення. *Міжнародний*

- науковий журнал "Інтернаука". 2021. № 6 (50). 2 том. С. 95–100. (Серія: "Екон. науки").
30. Варналій З. С., Живко З. Б. Роль державних інституцій в удосконаленні державного регулювання у сфері протидії рейдерству. *Вісник Київ. нац. університету імені Тараса Шевченка*. 2014. Вип. 154. С. 9–14.
 31. Варналій З. С., Мехед А. М. Забезпечення функціонування системи фінансової безпеки підприємства та методи оцінки її ефективності. 2020. *Scientific Collection "Interconf"*. Manchester. № 1(31). 2020. Р. 38–45.
 32. Варналій З. С., Мехед А. М. Теоретико-методичні підходи до оцінки фінансової безпеки суб'єктів підприємництва. *Наукові записки Львівського університету бізнесу та права*. 2022. С. 203–211. (Серія економічна. Серія юридична; вип. 32). URL : <http://dx.doi.org/10.5281/zenodo.6639106> (дата звернення: 30.05.2022 р.).
 33. Василечко Н. В., Васильців Т. Г. Сутнісні характеристики, ризики та загрози фінансової безпеки держави внаслідок ухилення від сплати податків з використанням офшорних зон. *Електронне фахове видання "Ефективна економіка"*. URL : http://www.economy.nayka.com.ua/pdf/11_2019/182.pdf (дата звернення: 19.07.2020 р.).
 34. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : [монографія]. Львів : Арал, 2008. 384 с.
 35. Ващенко І. В. Конфлікти: сучасний стан, проблеми та напрямки їх вирішення в органах внутрішніх справ / Нац. ун-т внутр. справ. Харків : ОВС, 2002. 255 с.
 36. Веклич В. О. Історичний досвід щодо протидії корупції за часів Стародавнього Риму і його значення за умов пострадянського корупційного середовища. *Актуальні проблеми вітчизняної юриспруденції*. Спецвипуск. 2017. Ч. 1. С. 3–7.
 37. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Т. Бусел]. Київ : ВТФ Перун, 2003. 1440 с.

38. Великий тлумачний словник сучасної української мови. Київ : ВТФ “Перун”, 2005. 1728 с.
39. Війни-XXI: полігібресія росії. Дослідження Центру глобалістики “Стратегія XXI”. Київ 2017. 241 с.
40. Воробйова О. І. Фінансова безпека на мікро- та макрорівнях [Текст]. *Науковий вісник: фінанси, банки, інвестиції*. 2012. № 2. С. 6–10.
41. Всесвітнє дослідження економічних злочинів та шахрайства 2020 року. URL : <https://www.pwc.com/ua/uk/survey/2020/economic-crime-survey.html> (дата звернення: 20.03.2021 р.).
42. Гальчинський А. С. Економічна методологія : логіка оновлення. Київ : АДЕФ-Україна, 2010. 572 с.
43. Гальчинський А. С. Політична нооекономіка : начала оновленої парадигми економічних знань. Київ : Либідь, 2013. 472 с.
44. Гарাগонич О. В. Етапи рейдерського захоплення акціонерних товариств. *Вісник Академії адвокатури України*. 2013. № 3(28). С. 27–28.
45. Гаращук В. М., Мухатаєв А. О. Актуальні проблеми боротьби з корупцією в Україні : [монографія]. Харків : Право, 2010. 143 с.
46. Гембарська В. Військова агресія росії вбиває зелену енергетику в Україні та декарбонізує економіку через спад ВВП. Медіаплатформа “Екополітика”. URL : <https://ecopolitic.com.ua/ua/news/ukrainaperevikonuie-nvv2-chi-ie-privodi-dlya-optimizmu-rozpoviv-ekspert-centru-razumkova-volodimir-omelchenko/> (дата звернення: 02.08.2022 р.).
47. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса ; під. заг. ред. проф. Р. О. Додонова. Вінниця : ТОВ “НіланЛТД”, 2017. 412 с.
48. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. *Аналітичний документ* / за загальною редакцією В. Мартинюка ; Центр глобалістики “Стратегія XXI”. Київ, 2018. 105 с.
49. Глущенко О. О. Поняття регуляторної політики стримування нелегального підприємництва. *Актуальні проблеми розвитку економіки регіону*. 2009. Вип. 5. С. 15–20.

50. Головань М. С. Компетенція і компетентність: досвід теорії, теорія досвіду. *Вища освіта України*. 2008. № 3. С. 23–30.
51. Гонтарева І. В. Оцінювання системної ефективності функціонування і розвитку промислових підприємств : монографія. Харків : ІНЖЕК, 2011. 480 с.
52. Гончаров С. М., Кушнір Н. Б. Тлумачний словник економіста / за ред. проф. С. М. Гончарова. Київ : Центр учбової літератури, 2009. 264 с.
53. Господарський кодекс України від 16.01.2003 № 436-IV. URL : <http://zakon2.rada.gov.ua/laws/show/436-15> (дата оновлення : 01.12.2022 р.) (дата звернення: 02.12.2022 р.).
54. Грабченко А. І., Федорович В. О., Гаращенко Я. М. Методи наукових досліджень : навч. посібник. Харків : НТУ “ХПІ”, 2009. 142 с.
55. Грек Б. М. Проблеми кримінальної відповідальності за рейдерство та шляхи їх вирішення. *Вісник Національної академії прокуратури України*. 2009. № 1. С. 75–81.
56. Грищенко Н. М. Кримінальна відповідальність за протиправне заволодіння майном підприємства, установи, організації : дис. ... канд. юрид. наук : 12.00.08. Дніпро. 2019. 216 с.
57. Гудзь Т. П. Управління фінансовою рівновагою підприємства: автореф. дис. ... д-ра екон. наук. Одеса, 2019. 40 с.
58. Даценко В., Шевченко Н. Гарантування фінансової безпеки держави в умовах глобалізації. *Державне управління: удосконалення та розвиток*. 2012. № 5. URL : <http://www.dy.nayka.com.ua/?op=1&z=486> (дата звернення: 13.07.2018 р.).
59. Декларація Організації Об'єднаних Націй про боротьбу з корупцією і хабарництвом у міжнародних комерційних операціях від 16.12.1996 р. Міжнародні правові акти та законодавство окремих країн про корупцію. URL : http://zakon.rada.gov.ua/laws/show/995_369#Text (дата звернення: 15.07.2019 р.).
60. Дем'янишин В. Г., Костецький В. В., Дем'янишин В. В. Модернізація бухгалтерського обліку фінансових ресурсів у державному секторі в умовах реформування системи управління

- публічними фінансами та зміцнення фінансової безпеки суб'єктів господарювання. *Світ фінансів*. 2022. № 4 (73). С. 22–44. URL : <http://sf.wunu.edu.ua/index.php/sf/article/view/1556> (дата звернення: 17.11.2022 р.).
61. Дем'янишин В. Г., Костецький В. В., Дем'янишин В. В. Удосконалення управління фінансовими ресурсами у державному секторі в контексті зміцнення фінансової безпеки суб'єктів господарювання. *Інноваційна економіка*. 2022. № 4. С. 91–102. URL : <http://www.inneco.org/index.php/innecoua/article/view/980/0> (дата звернення: 12.11.2022 р.).
62. Дем'янишин В., Клапків Ю. Соціально-економічні мотиви участі в фінансовому шахрайстві на ринку страхових послуг. *Економічний дискурс*. 2020. Вип. 2. С. 66–74. URL : <http://dspace.wunu.edu.ua/handle/316497/47310> (дата звернення: 15.06.2021 р.).
63. Дем'янишин В., Костецький В. Вплив рейдерства на фінансову безпеку суб'єктів господарювання. *Світ фінансів*. 2022. № 3 (72). С. 156–164. URL : <http://sf.wunu.edu.ua/index.php/sf/article/view/1541> (дата звернення: 01.10.2022 р.).
64. Джуринський О.О. Захист від недобросовісної конкуренції (цивільно-правовий аспект): автореф. дис. ... кан. юрид.наук: 12.00.03 / О. О. Джуринський. Київ : КНУ імені Т. Шевченка, 2010. 18 с.
65. Директива 2005/60/ЄС Європейського Парламенту та Ради про запобігання використанню фінансової системи з метою відмивання коштів та фінансування тероризму від 26.10.2005 р. № 2005/60/ЄС. URL : https://zakon.rada.gov.ua/laws/show/994_774#Text (дата оновлення: 16.09.2009 р.) (дата звернення: 07.08.2022 р.).
66. Дмитренко Е. С. Юридична відповідальність суб'єктів фінансового права у механізмі правового забезпечення фінансової безпеки України : [монографія]. Київ : Юрінком Інтер, 2009. 591 с.

67. Дмитрієв І. А., Нестеренко В. Ю. Управління ризиком рейдерського захоплення підприємства [монографія]. Харків : ХНАДУ, 2011. 178 с.
68. Додонов Р. Конфлікт на Сході України у дзеркалі соціально-філософської рефлексії. Вінниця : ГЛОБУС ПРЕСС, 2016. 200 с.
69. Дослідження DOU (Спільнота програмістів) “Портрет ІТ-спеціаліста”. 2020. URL : <https://dou.ua/lenta/articles/portrait-2020/?from=doufr> (дата звернення: 19.03.2021 р.).
70. Дропа Я. Б., Кульчицький М. І., Яструбецька Л. С. Аналіз структури оборотного капіталу підприємств України за напрямками вкладення. *Актуальні проблеми розвитку економіки регіону* : зб. наук. праць. 2008. Вип. IV, Т. 1. С. 156–162.
71. Дудоров О. О., Каменський Д. В., Титаренко С. С. Стаття 205-1 Кримінального кодексу України як антирейдерська заборона: проблеми тлумачення, застосування і вдосконалення. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2021. Вип. 1 (93). С. 116–135.
72. Дуткевич Т. В. Конфліктологія з основами психології управління : навч. посібник. Київ : Центр навчальної літератури, 2005. 456 с.
73. Економічна теорія : Політекономія : [підручник] / [за ред. В. Д. Базилевича]. 6-те вид., перероб. і доп. Київ : Знання-Прес, 2001. 719 с.
74. Єзеров А. Конституційний конфлікт як феномен та процес в Україні : монографія. Одеса : Юридична література, 2008. 240 с.
75. Єрмошенко М. М. Фінансова безпека держави : національні інтереси, реальні загрози, стратегія забезпечення. Київ : Київ. нац. торг.-екон. ун-т, 2001. 309 с.
76. Єрмошенко М. М., Горячева К. С. Фінансова складова економічної безпеки: держава і підприємство : наук. монографія. Київ : Національна академія управління, 2010. 232 с.
77. Єфименко А. Рейдерство або ринок контролю. *Економічний часопис-XXI*. 2014. 7-8(2). URL : <http://www.justinian.com.ua/article.php?id=3072> (дата звернення: 01.12.2018 р.).
78. Жабинець О. Й. Захист інформації та інформаційна безпека страхових компаній. *Економічний часопис-XXI*. 2014. 7-8(2). URL :

http://soskin.info/userfiles/file/2014/7-8_2014/7-8_2/Zhabynets.pdf
(дата звернення: 03.09.2019 р.).

79. Жаліло Я. А. Економічна стратегія держави: теорія, методологія, практика : [монографія]. Київ : НІСД, 2003. 368 с.
80. Жидецька Х. В., Швайка Л. А. Кількісне оцінювання рівня кадрової безпеки для підприємств видавничо-поліграфічної галузі. *Наукові записки [Української академії друкарства]*. 2012. № 3. С. 96–102. URL : http://nbuv.gov.ua/UJRN/Nz_2012_3_17 (дата звернення: 15.04.2021 р.).
81. Журавель М. Ю., Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки, транспорту і промисловості*. 2011. № 33. С. 171–176.
82. Загорельська Т. Ю. Управління фінансовими ризиками на рівні підприємства. *Вісник Хмельницького ун-ту*. 2009. № 3. Т. 1. С. 168–173. URL : <http://surl.li/iakuo> (дата звернення: 11.06.2020 р.).
83. Задірака В. К., Олексюк О. С. Методи захисту фінансової інформації : [навч. посібник]. Київ : Вища шк., 2000. 460 с.
84. Задорожний С. А. Сучасні передумови виникнення корупції. *Проблеми реалізації державної антикорупційної політики в Україні* : зб. наук. праць. Київ : НАДУ, 2011. С. 43–46.
85. Засць О. В. Абдукція у логіці. *Велика українська енциклопедія*. URL : https://vue.gov.ua/Абдукція_у_логіці (дата звернення: 19.09.2021 р.).
86. Звіт антикорупційної неурядової організації “Transparency International” за 2020 р. URL : <http://cpi.ti-ukraine.org/#/> (дата звернення : 15.03.2021 р.).
87. Звіт Асоціації сертифікованих спеціалістів по розслідуванню шахрайства. URL : <http://www.acfe.com> (дата звернення: 04.02.2021 р.).
88. Звіт Всеукраїнської Мережі Добročесності та Компласнсу (UNIC) “Корупційні ризики у діяльності органів влади: погляд бізнесу”. 2018. URL : <https://unic.org.ua/news/corruption-risks-in-the-government-work-business-point-of-view-90/> (дата звернення: 10.03.2021 р.).

89. Звіт Державної служби спеціального зв'язку та захисту інформації України за 3 квартал 2022 року. URL : <https://scrc.gov.ua/article/163> (дата звернення: 07.11.2022 р.).
90. Звіт з кібербезпеки компанії Check Point за 2022 рік. URL : <https://pages.checkpoint.com/cyber-attack-2022-trends.html> (дата звернення: 03.12.2022 р.).
91. Звіт міжнародної асоціації “TRACE International” за 2020 р. URL : <https://www.traceinternational.org/trace-matrix#matrix-results> (дата звернення : 20.03.2021 р.).
92. Звіт Міністерства економіки України про релокацію вітчизняних підприємств станом на 24.10.2022 р. URL : <https://www.me.gov.ua/News/Detail?lang=uk-UA&id=d152dcfe-7bde-49df-a69a-8d7f9586fc13&title=ProgramaRelokatsii> (дата звернення: 28.10.2022 р.).
93. Звіт про стан конкурентної розвідки “Crayon”. URL : <http://surl.li/iaktr> (дата звернення: 26.04.2022 р.).
94. Звіти Альянсу з майнових прав (PRA). URL : <https://www.internationalpropertyrightsindex.org/country/ukraine> (дата звернення: 10.12.2022 р.).
95. Зеркалов Д. В. Безпека комерційної діяльності: у 2 кн. Кн. 2: Захист. Довідник. Київ : Основа, 2006. 800 с.
96. Зеркалов Д. В. Рейдерство : [монографія]. Київ : Основа, 2011. 272 с.
97. Зубко Т., Лаптева В. Індикатори кадрової безпеки підприємства. *Вісник КНТЕУ*. 2018. № 4. С. 57–67.
98. Івашко О. Фінансова безпека України в умовах кризових явищ в економіці. *Економічний часопис Східноєвропейського національного університету Лесі Українки*. 2015. № 2. С.61–66.
99. Ляшенко С. Н. Складові економічної безпеки підприємства і підходи до їх оцінки. *Актуальні проблеми економіки*. 2003. № 3. С. 12–19.
100. Індекс стійкості до російської дезінформації / Офіційна сторінка Ради зовнішньої політики “Українська призма”. URL : <http://prismua.org/dri/> (дата звернення: 20.11.2022 р.).
101. Юргачова М. І. Корпоративні конфлікти в Україні : основні їх види та значущість. *Вісник НУ “Львів. політехніка”*. 2011. № 698. С. 170–180.

102. Каменський Д. В. Кримінальна відповідальність за злочини, пов'язані з банкрутством в Україні та США. *Вісник Асоціації кримінального права України*. 2014. № 2(3). С. 237–249.
103. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект. Київ : Атіка, 2005. 432 с.
104. Каракуц А., Гордійчук Д., Щедрина Ю. Аграрний бізнес, металурги, IT, хімія та інші: як справи в гігантів української економіки. *Електронне видання “Економічна правда”*. URL : <https://www.epravda.com.ua/publications/2022/06/6/687837/> (дата звернення: 09.07.2022 р.).
105. Карачарова К. А. Методи прогнозування фінансової неспроможності підприємства. *Економічний аналіз*. 2015. Т. 21, № 1. С. 292–297.
106. Картузов Є. П. Визначення фінансової безпеки підприємства: поняття, зміст, значення і функціональні аспекти. *Актуальні проблеми економіки*. 2012. № 8(134). С. 172–181.
107. Кириченко О. А., Кудря І. В. Вдосконалення управління фінансовою безпекою підприємств в умовах кризи [Текст]. *Інвестиції: практика та досвід*. 2009. № 10. С. 22–26.
108. Кладченко І. С. Фінансова рівновага як умова забезпечення збалансованого розвитку промислового підприємства. *Наукові праці Кіровоградського національного технічного університету. Економічні науки*. 2013. Вип. 24. С.369–377.
109. Клименко Н. Г. Еволюція змісту концепту “безпека” за різних історичних епох та політичних систем. *Державне управління: удосконалення та розвиток*. URL : http://www.dy.nauka.com.ua/pdf/8_2019/22.pdf (дата звернення: 07.02.2020 р.).
110. Клишко Т. Ю., Мельник О. О. Корпоративне шахрайство : реалії сучасності. *Наук. вісник Ужгород. ун-ту*. 2015. С. 185–190. (Сер. Економіка ; вип. 2.). URL : http://www.visnyk-ekon.uzhnu.edu.ua/images/pubs/46/1/46_33.pdf (дата звернення: 02.09.2020 р.).
111. Коваленко В. В., Дмитров С. О., Єжов А. В. Міжнародний досвід у сфері запобігання та протидії відмиванню доходів, одержаних

- злочинним шляхом, та фінансуванню тероризму : [монографія]. Суми : УАБС НБУ, 2007. 112 с.
112. Кодекс про адміністративні правопорушення України від 07.12.1984 р. № 8073-X. URL : <http://zakon3.rada.gov.ua/laws/show/80731-10> (дата оновлення : 01.12.2022 р.) (дата звернення: 02.12.2022 р.).
113. Кодекс України з процедур банкрутства від 18.10.2018 р. № 2597-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2597-19#Text> (дата оновлення : 15.12.2021 р.) (дата звернення: 07.10.2022 р.).
114. Козак Л. С., Багровецька І. В. Концептуальні та методичні засади формування механізму забезпечення фінансової безпеки підприємства [Текст]. *Економіка і управління*. 2008. № 13. С. 97–101.
115. Колесник М. А. Адміністративно-правові засади діяльності органів державної влади України щодо протидії рейдерству : дис. ... канд. юрид. наук: 12.00.07. 2012. Харків. 220 с.
116. Колодізев О. М., Плескун І. В. Фінансовий моніторинг у банках України: сутність і визначення проблем реалізації в сучасних умовах розвитку економіки. *Управління розвитком*. 2017. № 3. С. 24–35. URL : http://nbuv.gov.ua/UJRN/Uproz_2017_3-4_6 (дата звернення: 24.03.2018 р.).
117. Комплаєнс для малого та середнього бізнесу. Як ефективно боротись з корупцією. Проект USAID “Впевнений бізнес – заможна громада”, 2015. 25 с.
118. Конвенція про кіберзлочинність № 2824-IV від 23.11.2001 р. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 19.11.2022 р.).
119. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL : <http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>. (дата оновлення 02.12.2019 р.) (дата звернення: 04.01.2020 р.).
120. Копитко М. І. Особливості процесу тіньової діяльності промислових підприємств. *Актуальні проблеми економіки*. 2013. № 9(147). С. 102–107.
121. Копитко М. І., Літвін Н. М. Деструктивні чинники середовища функціонування соціально-економічних систем. *Вчені записки*

- Університету “КРОК”*. 2017. С. 4–15. (Серія : Економіка ; вип. 46).
122. Корнеєв В. В. Загрози фінансовій безпеці підприємств України в умовах воєнного стану // В. В. Корнеєв // *Формування ринкових відносин в Україні: зб. наук. праць*. 2022. № 12 (259). С.71–76. URL: <https://doi.org/10.5281/zenodo.7711759> (дата звернення: 12.12.2022 р.).
123. Корнеєв В. В. Інвестиційна привабливість ринків капіталу: тенденції детінізації бізнес-угод. *Університетські наукові записки*. 2022. № 1–2 (85–86). С. 17–26.
124. Корнеєв В. В. Легалізація капіталу при користуванні послугами фінансових посередників. *Фінанси України*. 2003. № 9. С. 16–20.
125. Корнеєв В. В. Операції на фінансових ринках і загрози реальній економіці. *Стратегічна панорама*. 2001. № 1. С. 120–126.
126. Корнеєв В. В. Повноваження та відповідальність вищих органів корпоративного управління в акціонерному товаристві. *Бізнес Інформ*. 2009. № 9. С. 141–144.
127. Корнеєв В. В. Стабілізація економіки і фінансової системи: роль держави. *Законодавче забезпечення формування та реалізації державної політики України в умовах воєнного стану* : колективна монографія : у 4 т. / заг. ред.: Р. О. Стефанчук, І. М. Мищак, Л. А. Савченко ; Інститут законодавства Верховної Ради України. Київ : Вид-во “Людмила”, 2022. Т. 2. С. 35–54.
128. Корнеєв В. В., Ходжаян А. О. Макроекономічні тенденції діджиталізації фінансового ринку. *Формування ринкових відносин в Україні* : зб. наук. праць. 2022. № 7–8 (254–255). С. 42–47. URL : <https://zenodo.org/record/7323262#.Y6lRQ3ZBzmY> (дата звернення: 30.11.2022 р.).
129. Коулман П., Фергюсон Р. Результативний конфлікт. Незгода – це сила, що працює на вас. Київ : Наш формат, 2016. 320 с.
130. Краснокутська Н. С., Коптева Г. М. Дефініція поняття “фінансова безпека підприємства”: основні підходи та особливості. *Бізнесінформ*. 2019. № 7. С. 14–19.

131. Красюк Є. ІТ-спеціалісти можуть “злити” конкурентам конфіденційну інформацію. *Онлайн медіа видання МС. Today*. URL : <http://surl.li/hxtyz> (дата звернення: 08.06.2021 р.).
132. Кримінальний Кодекс України від 05.04.2001 р. №2341-III. URL : <http://zakon2.rada.gov.ua/laws/show/2341-14> (дата оновлення 01.12.2022 р.) (дата звернення: 02.12.2022 р.).
133. Кришевич О. В., Рощина І. О. Доведення до банкрутства: кримінально-правовий аспект та розмежування з шахрайством. *Юрид. вісник*. 2015. Вип. 1(34). С. 143–147.
134. Крупка І. М. Теоретико-методологічні засади та особливості функціонування фінансового ринку України : монографія. Львів : ЛНУ імені Івана Франка, 2019. 822 с.
135. Крупка М. І. Фінансо-економічна безпека банківської системи України та перспективи розвитку національної економіки. *Бізнес Інформ*. 2012. №6. С. 168–175.
136. Крупка М. І., Яструбецька Л. С. Фінансова безпека суб’єктів господарювання : підручник. Львів : ЛНУ імені Івана Франка, 2018. 320 с.
137. Кужелев М. О. Корпоративні конфлікти: механізм захисту інтересів власників на основі теорії мета-інтересів. *Світ фінансів. Науковий журнал Тернопільського національного економічного університету*. 2011. Вип. 4. С. 162–166.
138. Кужелев М. О., Нечипоренко А. В. Вплив поведінкових факторів на управління фінансовою діяльністю корпорації: теоретичні аспекти. *Збірник наукових праць Університету державної фіскальної служби України*. 2018. № 2. С. 154–168. URL : <https://core.ac.uk/reader/268453100> (дата звернення: 17.08.2019 р.).
139. Куликовський С. Генеза поняття “компетентність” у європейській та українській педагогічній науці. *Людинознавчі студії. Педагогіка*. 2014. № 29(1). С. 92–103.
140. Курочко Н. Як росія та Україна воюють на кіберфронті. URL : <https://www.epravda.com.ua/columns/2022/09/28/691925/> (дата звернення: 03.10.2022 р.).

141. Лаговська О. А., Шайдецька І. І. Корпоративні конфлікти та інформаційна асиметрія: причини і шляхи подолання. *Економічний аналіз* : зб. наук. праць / Тернопільський національний економічний університет; редкол.: О. В. Ярошук (голов. ред.) та ін. Тернопіль : Видавничо-поліграфічний центр Тернопільського національного економічного ун-ту “Економічна думка”. 2016. Том 26. № 1. С. 170–178. URL : <http://dspace.wunu.edu.ua/bitstream/316497/13291/1/26.pdf> (дата звернення: 30.03.2018 р.).
142. Лещенко О. Я. Трансформація системи цивільного захисту України в умовах сучасних воєнно-політичних конфліктів гібридного типу : автореф. дис. ... канд. політ. наук. Київ, 2020. 20 с.
143. Литвак О., Кучеренко І. Проблема рейдерства очима кримінолога і цивіліста. *Вісник Нац. академії прокуратури України*. 2010. № 3(19). С. 40–44.
144. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства : [монографія]. Луганськ : Вид-во СХУ ім. В. Даля, 2011. 400 с.
145. Магас Н. В. Теоретичні основи дослідження фінансової безпеки суб’єктів господарювання в умовах техноглобалізму. *Науковий вісник Львівського державного університету внутрішніх справ*. 2011. № 2. С. 77–88. (Серія економічна).
146. Маренич А. І., Мехеда Н. Г. Виявлення та запобігання загроз кадровій безпеці. *Фінансовий простір*. 2011. № 3(3). С. 127–132.
147. Марчук Є. “Гібридні війни” росії. Відлуння спецоперацій через 100 років. URL : <http://surl.li/iakwa> (дата звернення: 11.03.2020 р.).
148. Маслова М. Є. Грінмейлінг як особливий вид поглинання компаній. *Наук. записки*. 2007. Т. 64. С. 20–24.
149. Медведева І. Б., Погосова М. Ю. Діагностування безпеки промислового підприємства у трирівневій системі фінансових відносин : [монографія]. Харків : Вид-во ХНЕУ, 2011. 262 с.
150. Мельник Л. М. Фінансова рівновага як складова системи фінансово-економічної безпеки підприємств. *Вісник НУВГП*. 2017. С. 22–29. (Серія “Економічні науки”; вип. 2).

151. Мельник М. І. Корупція – корозія влади (соціальна сутність, тенденції та наслідки, заходи протидії). Київ : Юридична думка, 2004. 400 с.
152. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика: монографія. Львів : Растр-7, 2020. 384 с.
153. Методичні рекомендації на тему: “Сучасний стан і характеристика рейдерства в Україні” / Голосіївське районне управління юстиції у м. Києві. URL : golos.kievcity.gov.ua/files/2015/5/22/reyderstvo.doc (дата звернення: 14.11.2018 р.).
154. Методичні рекомендації щодо виявлення ознак неплатоспроможності підприємства та ознак дій з приховування банкрутства, фіктивного банкрутства чи доведення до банкрутства : Наказ Міністерства економіки України № 14 від 19.01.2006 р. URL : <https://zakon.rada.gov.ua/laws/show/v0014665-06#Text> (дата оновлення: 26.10.2010 р.) (дата звернення: 14.11.2018 р.).
155. Михальчишина Л. Г., Калашник В. В. Внутрішній аудит у запобіганні помилок і шахрайства на підприємстві. *Збірник наук. праць ВНАУ*. 2012. № 2(64). С. 95–96. (Сер. екон. науки).
156. Мішина С. В., Мішин А. Ю. Система експрес-моніторингу фінансової безпеки підприємства. *Актуальні проблеми економіки*. 2015. № 1(163). С. 162–172.
157. Моделювання впливу структурних зрушень на економічну динаміку розвитку України / А. І. Ігнатюк, В. В. Корнєєв, А. О. Ходжаян, А. Р. Ходжаян. *Науковий вісник НГУ*. 2021 (2). С. 170–177. URL : http://nvngu.in.ua/jdownloads/pdf/2021/2/02_2021_Khodzhaian.pdf (дата звернення: 26.05.2022 р.).
158. Моделювання економічної безпеки: держава, регіон, підприємство: монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова та ін.; за ред. Гейця В. М. Харків : ВД “ІНЖЕК”, 2006. 240 с.
159. Мойсеєнко І. П. Особливості вимірювання рівня фінансово-економічної безпеки підприємства. *Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Економічні науки*. 2011. Вип. 4. с. 170–174. URL :

- http://nbuv.gov.ua/UJRN/vkpnuen_2011_4_32 (дата звернення : 21.01.2018 р.).
160. Молодик В. В., Седлецький О. О., Гладун О. З. Прокурорський нагляд за додержанням законодавства в сфері захисту прав суб'єктів підприємницької діяльності та протидії рейдерству : [наук.-практ. посібник]. Київ : Алерта, 2013. 144 с.
161. Мужанова Т. М. Конкурентна розвідка як інструмент інформаційно-аналітичного супроводу забезпечення інформаційної безпеки підприємства. *Економіка і суспільство*. 2018. Вип. 16. С. 425–431.
162. Мулик Я. І. Сутність поняття “фінансова безпека підприємства”: систематизація наукових поглядів. *Збірник наукових праць Вінницького національного аграрного університету*. 2013. № 3(80). С. 195–206.
163. Мунтян В. І. Економічна безпека України. Київ : КИИЦ, 1999. 547 с.
164. Назаров Н. К. Конфлікти на підприємстві: визначення, причини, типи. *Науковий вісник Херсонського державного університету*. 2014. Вип. 5. Ч. 2. С. 198–201.
165. Національна безпека України методологічні аспекти, стан і тенденції розвитку : навч. посібник / за ред. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Ірпінь : Академія ДПС України, 2000. 304 с.
166. Невмержицький Е. В. Корупція в Україні: причини, наслідки, механізми протидії : монографія. Київ : КНТ, 2008. 368 с.
167. Некрасенко Л. А., Рибалка Ю. М. Складові управління фінансовою безпекою підприємств. *Вісник Полтавської державної аграрної академії*. 2015. Вип. 4 С. 162–167. URL : <http://www.pdaa.edu.ua/sites/default/files/nppdaa/3.2/162.pdf> (дата звернення: 14.09.2022 р.).
168. Нестеренко В. Ю. Рейдерство в Україні: оцінка сучасного стану, причини та перспективи розвитку. *Проблеми і перспективи розвитку підприємництва*. 2011. № 1. С. 20–23. URL : http://nbuv.gov.ua/j-pdf/pirprp_2011_1_6.pdf (дата звернення: 12.10.2018 р.).
169. Нікіфоров М. М., Пампуха І. В., Лоза В. М. Аналіз загроз воєнної безпеки держави в інформаційній сфері та протидії їм в умовах ведення гібридної війни. *Збірник наукових праць Військового*

- інституту Київського національного університету імені Тараса Шевченка.* 2018. № 61. С. 135–142. URL : http://nbuv.gov.ua/UJRN/Znpviknu_2018_61_16 (дата звернення: 25.05.2022 р.).
170. Нонік В. В. Дослідження сутності та трактування поняття “корупція”: еволюційний аспект. *Інвестиції: практика та досвід.* 2019. № 3. С. 99–105.
171. Носань Н. С. Актуальні загрози та ризики фінансової безпеки на межі посткризового та євроінтеграційного періодів. *Причорноморські економічні студії. Економіка та управління національним господарством.* 2019. Вип. 40. С. 37.
172. Омельченко С. В. Корупція з точки зору різних культур світу. *Підприємництво, господарство і право.* 2000. № 3. С. 54–57.
173. Онищенко С. В., Лапінський І. Е. Міжнародний досвід боротьби з тінізацією економіки в умовах глобалізації. *Ефективна економіка.* 2013. № 2. URL : http://nbuv.gov.ua/UJRN/efek_2013_2_76 (дата звернення: 24.06.2020 р.).
174. Онищенко С. В., Пугач О. А. Загрози економічній безпеці України: сутність, оцінювання та механізм упередження : [монографія]. Полтава : Полтавський НТУ, 2015. 337 с.
175. Орлик О. В. Класифікація та систематизація загроз фінансово-економічній безпеці підприємств. *Вісник соціально-економічних досліджень.* 2017. № 1. С. 106–115. URL : <http://surl.li/iakxs> (дата звернення : 15.06.2019 р.).
176. Орлик О. В. Механізм управління фінансово-економічною безпекою підприємства та його основні складові. *Фінансово-кредитна діяльність: проблеми теорії та практики.* 2015. Вип. 2. С. 222–232.
177. Основи економічної теорії : підручник / С. В. Мочерний, С. А. Єрохін, Л. О. Каніщенко та ін. ; за ред. С. В. Мочерного. Київ : ВЦ “Академія”, 2001. 472 с.
178. Островська О. А., Гавриленко Ю. О. Індекс IPRI в оцінці ризику поглинання компаній. *Інфраструктура ринку.* 2019. Вип. 34. С. 283–290. URL : http://nbuv.gov.ua/UJRN/ifrctr_2019_34_43 (дата звернення: 14.03.2020 р.).

179. Офіційна веб-сторінка Ernst & Young. URL : <http://www.ey.com/ua/uk/home> (дата звернення: 14.11.2022 р.).
180. Офіційна веб-сторінка Transparency International. URL : <http://ti-ukraine.org/about> (дата звернення: 15.03.2021 р.).
181. Офіційна веб-сторінка Антимонопольного комітету України. URL : <https://amcu.gov.ua/pro-nas/zvitnist/ricхни-zviti> (дата звернення: 30.11.2022 р.).
182. Офіційна веб-сторінка Європейської Бізнес Асоціації. URL : <http://eba.com.ua/majzhe-polovyna-kompanij-eva-vidnovyly-povnotsinnu-robotu/> (дата звернення: 06.09.2022 р.).
183. Офіційна веб-сторінка консалтингової групи “Advanter”. URL : <https://advanter.ua/> (дата звернення: 04.09.2022 р.).
184. Офіційна веб-сторінка Міністерства економіки України. URL : <https://www.me.gov.ua/> (дата звернення: 14.11.2022 р.).
185. Офіційна веб-сторінка Міністерства юстиції України: URL : <https://minjust.gov.ua/news/ministry/ofis-protidii-reyderstvu-pidsumovue-2021-y-sistema-zahistu-prava-vlasnosti-efektivno-pratsyue> (дата звернення: 14.02.2022 р.).
186. Офіційна веб-сторінка Ради бізнес-омбудсмена: URL : <https://boi.org.ua/reports/> (дата звернення: 12.02.2022 р.).
187. Офіційна веб-сторінка Ради зовнішньої політики “Українська призма”. URL : <http://prismua.org/dri/> (дата звернення: 03.11.2022 р.).
188. Офіційна веб-сторінка Українського клубу аграрного бізнесу. URL : <https://www.ucab.ua/ua> (дата звернення: 01.11.2022 р.).
189. Офіційна сторінка Міністерства аграрної політики та продовольства України. URL : <https://minagro.gov.ua/> (дата звернення: 02.09.2022 р.).
190. Пазєєва Г. М. Комплексна діагностика в забезпеченні економічної безпеки підприємств (на матеріалах транспортно-експедиційних підприємств України). Київ : Університет економіки та права “КРОК”, 2017. 291 с.
191. Пастернак-Таранушенко Г. Економічна безпека держави. Статика процесу забезпечення : підручник для державних службовців, науковців, студентів і аспірантів вищих навчальних закладів

- економічного профілю / за ред. професора Богдана Кравченка. Київ : “Кондор”, 2002. 302 с.
192. Педан В. І. Актуальність дослідження питань протидії законній господарській діяльності. *Вісник Бердянського університету менеджменту і бізнесу*. 2016. № 2. С. 55–58. URL : http://nbuv.gov.ua/UJRN/vbumb_2016_2_13 (дата звернення: 09.06.2022 р.).
193. Пекін А. Економічна безпека підприємств як економіко-правова категорія. *Економіст*. 2007. № 8. С. 23–25.
194. Питання Міністерства економіки : Постанова Кабінету міністрів України № 459 від 20 серпня 2014 р. URL : <https://zakon.rada.gov.ua/laws/show/459-2014-%D0%BF#Text> (дата оновлення: 27.09.2022 р.) (дата звернення: 14.10.2022 р.).
195. Підхомний О. М. Фінансова безпека України : інструменти і стратегії формування : [монографія]. Львів : ЛНУ імені Івана Франка, 2014. 320 с.
196. Підхомний О. М. Фінансова безпека України в умовах глобалізації : монографія / Львівський національний університет імені Івана Франка. Львів : СПОЛОМ, 2012. 360 с.
197. Підхомний О. М., Глущенко О. О. Нелегальне підприємництво та фінансова система України в умовах глобалізації : [монографія]. Львів : ЛНУ імені Івана Франка, 2011. 348 с.
198. Підхомний О. М., Микитюк Н. О., Вознюк І. П. Типологія загроз фінансовій безпеці суб’єктів підприємницької діяльності. URL : http://vlp.com.ua/files/20_29.pdf, С. 121–122.
199. Підхомний О. М., Яструбецька Л. С. Актуальні проблеми контролю нелегальних систем переказу вартості. *Управління підприємством: проблеми та шляхи їх вирішення* : матеріали Міжнар. наук.-практ. конф. ДонНУЕТ, 2009. С. 235–238.
200. Підхомний О. М., Яструбецька Л. С. Бухгалтерський та податковий облік в системі запобігання та протидії нелегальним фінансовим схемам. *Засоби фінансового забезпечення стійкого економічного розвитку* : матеріали Всеукр. наук.-метод. конф. Севастополь : Вид-во СевНТУ, 2009. С. 39–40.

201. Підхомний О. М., Яструбецька Л. С. Експертні методи в управлінні фінансовою безпекою суб'єктів господарювання. *Сучасні аспекти фінансового управління економічними процесами* : матеріали Всеукраїнської науково-методичної конференції. Севастополь : Вид-во СевНТУ, 2007. С. 80–82.
202. Підхомний О. М., Яструбецька Л. С. Індикатори оцінки рівня фінансової безпеки суб'єктів господарювання. *Економічні науки* : [збірник наукових праць]. 2007. С. 73–80. (Серія “Облік і фінанси”; вип. 4 (16). Ч. 2).
203. Підхомний О. М., Яструбецька Л. С. Інституційні основи стратегії фінансової безпеки України. *Актуальні проблеми розвитку економіки регіону* : наук. збірник / за ред. І. Г. Ткачук. Івано-Франківськ : ВДВ ЦІТ Прикарпатського національного університету ім. В. Стефаника, 2010. Вип. 6. Т. 2. С. 175–182.
204. Підхомний О. М., Яструбецька Л. С. Роль та місце податкової безпеки в структурі фінансової безпеки. *Розвиток фінансових методів державного управління національною економікою* : зб. наук. праць / ДонДУУ. Донецьк : ДонДУУ, 2009. Т. X. С. 59–65. (Серія “Економіка”; вип. 126).
205. Підхомний О. М., Яструбецька Л. С. Управління життєвим циклом інформації суб'єктів ринку цінних паперів. *Актуальні проблеми розвитку економіки регіону* : наук. збірник / за ред. І. Г. Ткачук. Івано-Франківськ : ВДВ ЦІТ Прикарпатського національного університету ім. В. Стефаника, 2007. Вип. III. Т. 2. С. 91–96.
206. Підхомний О. М., Яструбецька Л. С. Фіскальні аспекти фінансового моніторингу в умовах глобалізації. *Вісник Львівського університету*. Львів : ВЦ ЛНУ імені Івана Франка. 2008. С. 336–339. (Серія економічна; вип. 40).
207. Платон. Держава. Орієнтир, 2017. 336 с.
208. Погосова М. Ю. Діагностування фінансової безпеки промислового підприємства : автореф. дис. ... канд. екон. наук: 08.00.08/ УБС НБУ. Київ, 2010. 21 с.

209. Податковий кодекс України від 02.12.2010 р. №2755-VI. URL : <http://zakon5.rada.gov.ua/laws/show/2755-17> (дата оновлення : 01.12.2022 р.) (дата звернення: 02.12.2018 р.).
210. Політична економія : [навч. посібник] / К. Т. Кривенко, В. С. Савчук, О. О. Беляєв [та ін.] ; [за ред. д-ра екон. наук, проф. К. Т. Кривенка]. Київ : КНЕУ, 2001. 508 с.
211. Порядок надання фінансової державної підтримки суб'єктам підприємництва : Постанова Кабінету Міністрів України №28 від 24.01.2020 р. №28. URL : <https://zakon.rada.gov.ua/laws/show/28-2020-%D0%BF#Text> (дата оновлення:14.10.2022 р.) (дата звернення: 10.11.2022 р.).
212. Предборський В. А. Економічна безпека держави : [монографія]. Київ : Кондор, 2005. 391 с.
213. Про акціонерні товариства : Закон України від 27.07.2022 р. № 2465-IX. URL : <https://zakon.rada.gov.ua/laws/show/2465-20#n1985> (дата оновлення: 01.12.2022 р.) (дата звернення: 03.12.2022 р.).
214. Про Антимонопольний комітет України : Закон України від 26.11.1993р. № 3659-XII. URL : <https://zakon.rada.gov.ua/laws/show/3659-12#Text> (дата оновлення : 23.09.2021 р.) (дата звернення : 20.11.2021).
215. Про Бюро економічної безпеки України : Закон України № 1150-IX від 28.01.2021 р. URL : <https://zakon.rada.gov.ua/laws/show/1150-20#Text> (дата оновлення: 22.09.2021 р.) (дата звернення: 30.11.2021 р.).
216. Про вищу освіту : Закон України № 1556-VII від 01.07.2014 р. URL : <https://zakon.rada.gov.ua/laws/show/1556-18#Text> (дата оновлення: 28.07.2022 р.) (дата звернення: 30.07.2022 р.).
217. Про внесення змін до деяких законів України щодо удосконалення механізму протидії рейдерству : Закон України № 2255-IX від 12.05.2022. URL : <https://zakon.rada.gov.ua/laws/show/2255-20#Text> (дата звернення: 14.08.2022 р.).
218. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 № 2149-IX. URL :

- <https://zakon.rada.gov.ua/laws/show/2149-20#Text> (дата звернення: 22.05.2022 р.).
219. Про гарантування речових прав на об'єкти нерухомого майна, які будуть споруджені в майбутньому : Закон України № 2518-IX від 15.08.2022 р. URL : <https://zakon.rada.gov.ua/laws/show/2518-20#Text> (дата звернення : 16.11.2022 р.).
220. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : Закон України № 1952-IV від 01.07.2004 р. URL : <http://zakon5.rada.gov.ua/laws/show/1952-15> (дата оновлення : 03.11.2022 р.) (дата звернення: 16.11.2022 р.).
221. Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань : Закон України № 755-IV від 15.05.2003 р. URL : <http://zakon3.rada.gov.ua/laws/show/755-15> (дата оновлення: 06.10.2022 р.) (дата звернення: 16.11.2022 р.).
222. Про електронні довірчі послуги : Закон України № 2155-VIII від 05.10.2017 р. URL : <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата оновлення: 01.12.2022) (дата звернення: 02.12.2022 р.).
223. Про електронні документи та електронний документообіг : Закон України № 851-IV від 22.05.2003. URL : <http://zakon2.rada.gov.ua/laws/show/851-15> (дата оновлення : 14.12.2021 р.) (дата звернення: 03.02.2022 р.).
224. Про електронні комунікації : Закон України № 1089-IX від 16.12.2020 р. URL : <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата оновлення : 01.12.2022 р.) (дата звернення: 02.12.2022 р.).
225. Про запобігання корупції : Закон України від 14.10.2014 1700-VII. URL : <https://zakon.rada.gov.ua/laws/show/1700-18#Text> (дата оновлення 04.03.2021 р.) (дата звернення: 19.05.2021 р.).
226. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України № 361-IX від 06.12.2019 р. URL : <https://zakon.rada.gov.ua/laws/show/361-20#n831> (дата оновлення: 04.11.2022 р.) (дата звернення: 06.11.2022 р.).

227. Про затвердження плану невідкладних заходів з переміщення у разі потреби виробничих потужностей суб'єктів господарювання з територій, де ведуться бойові дії та/або є загроза бойових дій, на безпечну територію : Розпорядження Кабінету міністрів України № 246-р від 25.03.2022 р. URL : <https://zakon.rada.gov.ua/laws/show/246-2022-%D1%80#Text> (дата звернення: 15.06.2022 р.).
228. Про затвердження Положення про Державну службу фінансового моніторингу України : Постанова Кабінету міністрів України № 537 від 29.07.2015. URL : <https://zakon.rada.gov.ua/laws/show/537-2015-%D0%BF#Text> (дата оновлення : 29.07.2020 р.) (дата звернення: 12.08.2022 р.).
229. Про затвердження Положення про Міністерство фінансів України : Постанова Кабінету міністрів України № 375 від 20.08.2014. URL : <https://zakon.rada.gov.ua/laws/show/375-2014-%D0%BF#Text> (дата оновлення: 07.07.2022 р.) (дата звернення: 15.09.2022 р.).
230. Про затвердження Положення про Міністерство цифрової трансформації України : Постанова Кабінету міністрів України від 18 вересня 2019 р. № 856. URL : <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n12> (дата оновлення : 08.11.2022 р.) (дата звернення: 19.11.2022 р.).
231. Про затвердження Положення про Міністерство юстиції України : Постанова Кабінету міністрів України № 228 від 02.07.2014. URL : <https://zakon.rada.gov.ua/laws/show/228-2014-%D0%BF#Text> (дата оновлення : 02.09.2022 р.) (дата звернення: 08.09.2022 р.).
232. Про затвердження Положення про Спеціалізовану антикорупційну прокуратуру Офісу Генерального прокурора : Наказ Офісу Генерального прокурора № 125 від 05.03.2020 р. URL : <https://zakon.rada.gov.ua/laws/show/v0125905-20#Text> (дата оновлення: 28.08.2020 р.) (дата звернення: 30.08.2022 р.).
233. Про затвердження положень про Державну податкову службу України та Державну митну службу України : Постанова Кабінету міністрів України № 227 від 06.03.2019 р. URL : <https://zakon.rada.gov.ua/laws/show/227-2019-%D0%BF#Text> (дата оновлення : 10.06.2022 р.) (дата звернення: 15.06.2022 р.).

234. Про затвердження Порядку проведення аналізу фінансово-господарського стану суб'єктів господарювання державних підприємств і підприємств, у статутному капіталі яких частка державної власності перевищує п'ятдесят відсотків, та підготовки на запити суду, прокуратури або іншого уповноваженого органу висновків про наявність ознак фіктивного банкрутства, доведення до банкрутства, приховування стійкої фінансової неспроможності, незаконних дій у разі банкрутства : Наказ Міністерства юстиції України від 26.02.2013 р. № 327/5. URL : <http://zakon5.rada.gov.ua/laws/show/z0331-13> (дата оновлення : 12.09.2014 р.) (дата звернення: 17.03.2018 р.).
235. Про затвердження Порядку розгляду скарг у сфері державної реєстрації : Постанова Кабінету Міністрів України № 1128 від 25.12.2015. URL : <http://zakon0.rada.gov.ua/laws/show/1128-2015-%D0%BF> (дата оновлення: 17.06.2022 р.) (дата звернення: 21.07.2022 р.).
236. Про захист від недобросовісної конкуренції : Закон України від 07.06.1996 р. № 236/36-ВР. URL : <https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text> (дата оновлення: 16.10.2020 р.) (дата звернення: 01.04.2021 р.).
237. Про захист економічної конкуренції: Закон України від 11.01.2001 № 2210-III. URL : <https://zakon.rada.gov.ua/laws/show/2210-14#Text> (дата оновлення: 13.02.2020 р.) (дата звернення: 12.03.2021 р.).
238. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94. URL : <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата оновлення: 15.03.2022 р.) (дата звернення: 25.04.2022 р.).
239. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL : <http://zakon5.rada.gov.ua/laws/show/2657-12> (дата оновлення: 03.11.2022 р.) (дата звернення: 25.04.2022 р.).
240. Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів : Закон України від 10.11.2015 р. №772-VIII. URL : <https://zakon.rada.gov.ua/laws/show/772-19#Text> (дата оновлення : 31.05.2022 р.) (дата звернення: 03.07.2022 р.).

241. Про Національне антикорупційне бюро України : Закон України від 14.10.2014 № 1698-VII. URL : <https://zakon.rada.gov.ua/laws/show/1698-18#Text> (дата оновлення: 07.09.2022 р.) (дата звернення : 18.09.2022 р.).
242. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV. URL : <http://zakon2.rada.gov.ua/laws/show/679-14> (дата оновлення: 15.08.2022 р.) (дата звернення: 11.09.2022 р.).
243. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2469-19> (дата оновлення : 16.11.2021 р.) (дата звернення: 20.11.2022 р.).
244. Про Національну комісію з цінних паперів та фондового ринку : Указ Президента України від 23.11.2011 р. № 1063/2011 URL : <http://zakon0.rada.gov.ua/laws/show/1063/2011> (дата оновлення: 07.07.2020 р.) (дата звернення: 09.10.2020 р.).
245. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII URL : <http://zakon2.rada.gov.ua/laws/show/580-19> (дата оновлення: 04.03.2020 р.) (дата звернення: 02.04.2022 р.).
246. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. URL : <http://zakon3.rada.gov.ua/laws/show/2135-12> (дата оновлення : 16.11.2021 р.) (дата звернення: 02.04.2022 р.).
247. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата оновлення: 17.08.2022 р.) (дата звернення: 22.11.2022 р.).
248. Про основні засади здійснення державного фінансового контролю в Україні : Закон України від 26.01.1993 р. № 2939-XII. URL : <http://zakon0.rada.gov.ua/laws/show/2939-12> (дата оновлення : 29.07.2022 р.) (дата звернення: 09.08.2022 р.).
249. Про охорону промислової власності : Паризька конвенція від 20 березня 1883 р. URL : https://zakon.rada.gov.ua/laws/show/995_123#Text (дата оновлення: 02.10.1979 р.) (дата звернення : 15.03.2020 р.).

250. Про прокуратуру : Закон України від 14.10.2014 р. № 1697-VII. URL : <http://zakon2.rada.gov.ua/laws/show/1697-18> (дата оновлення: 14.04.2022 р.) (дата звернення: 01.05.2022 р.).
251. Про публічні закупівлі : Закон України від 25.12.2015 р. № 922-VIII. URL : <https://zakon.rada.gov.ua/laws/show/922-19#Text> (дата оновлення : 23.01.2021) (дата звернення : 28.05.2021 р.).
252. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998р. № 183/98-ВР. URL : <http://zakon2.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80> (дата оновлення: 06.09.2022 р.) (дата звернення: 18.10.2022 р.).
253. Про розвідку : Закону України від 17.09.2020 р. № 912-IX URL : <https://zakon.rada.gov.ua/laws/show/912-20#Text> (дата оновлення: 14.04.2022 р.) (дата звернення: 29.05.2022 р.).
254. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL : <http://zakon0.rada.gov.ua/laws/show/2229-12> (дата оновлення: 04.11.2022 р.) (дата звернення: 09.11.2022 р.).
255. Про Службу зовнішньої розвідки України : Закон України від 01.12.2005 р. № 316-IV. URL : <https://zakon.rada.gov.ua/laws/show/3160-15#Text> (дата оновлення: 30.03.2021 р.) (дата звернення: 29.05.2022 р.).
256. Професійна педагогічна освіта: компетентнісний підхід : монографія / за ред. О. А. Дубасенюк. Житомир, 2011. 564 с.
257. Пундей Сар. Дж. Боротьба з корупцією. Критичний огляд з аналізом міжнародного досвіду. *Матеріали укр.-америк. семінару “Проблеми економічного зростання: питання доброчесності”*. Львів, 1997. 35 с.
258. П’ятницька Г. Т., Федулова І. В. Фінансова безпека країни та підприємства: визначення, взаємозв’язок і ризики забезпечення. URL : http://www.economy.nayka.com.ua/pdf/7_2020/16.pdf (дата звернення: 16.10.2020 р.).
259. П’ять найбільш відомих випадків корпоративного шахрайства. Аналітика ТОВ “ФА Сервіс”. URL : <https://cfo.ua/5vidomykhvipadkiv/ukr> (дата звернення: 14.09.2022 р.).
260. Ревак І. О. Інтелектуальний потенціал у системі економічної безпеки України: проблеми теорії та практики : монографія. Львів : ЛНУ імені Івана Франка, 2015. 416 с.

261. Ринкевич Н. С. Організаційна культура підприємств: виклики, загрози та тенденції. *Економічний вісник Донбасу*. Дніпро, 2019. Вип. 3 (57). С. 123–136.
262. Річний звіт Антимонопольного комітету України за 2020 р. URL : <https://amcu.gov.ua/news/richnij-zvit-amku-za-2020-rik> (дата звернення : 03.04.2021 р.).
263. Річний звіт за 2019 рік Ради бізнес-омбудсмена. URL : https://boi.org.ua/media/uploads/annual2019/annual_report_2019_ua.pdf (дата звернення: 03.04.2022 р.).
264. Руденко Л. Д., Моїсеєнко О. В. Щодо юридичної природи та форм рейдерства в Україні: господарсько-правовий аспект. *Приватне та публічне право*. 2019. № 14. С. 101–105.
265. Рудой К. Запобігання корупції як напрямок забезпечення міжнародної безпеки. *Правова держава*. 2015. № 19. С. 69–73.
266. СБУ встановила причетність спецслужб РФ до атаки вірусу Petya.A. *Мультимедійна платформа Укрінформ*. 2017. URL : <https://www.ukrinform.ua/rubric-technology/2257453-sbu-vstanovilapricetnist-specsluzb-rf-do-ataki-virusu-petyaa.html> (дата звернення: 07.08.2021 р.).
267. СБУ попереджає про можливу кібератаку на установи та підприємства. *Мультимедійна платформа Укрінформ*. 2017. URL : <https://www.ukrinform.ua/rubric-society/2288607-sbu-poperedzae-promozlivu-kiberataku-na-merezi-ukrainskih-ustanov-ta-pidприємstv.html> (дата звернення: 07.08.2021 р.).
268. Свириденко В. М. Про конфлікти у сфері оподаткування : теоретико-правовий аспект. Актуальні проблеми держави і права. 2011. Вип. 57. С. 535–543. URL : http://nbuv.gov.ua/UJRN/apdp_2011_57_80 (дата звернення: 05.12.2018 р.).
269. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.
270. Сервіс моніторингу відкритих даних. URL : <http://opendatabot.ua/open/raiders> (дата звернення : 07.12.2022 р.).
271. Системний звіт Ради бізнес-омбудсмена. Боротьба з рейдерством: сучасний стан та рекомендації. 2017. 56 с. URL :

- https://boi.org.ua/media/uploads/ii_2017_sytem_ua_digital.pdf (дата звернення: 06.10.2018 р.).
272. Словник української мови : в 11 т. Т. 1 / за ред. І. К. Білодіда АН УРСР. Інститут мовознавства. Київ : Наукова думка, 1970.
273. Словник української мови : в 11 т. Київ : Наукова думка, 1978. Т. 9. 916 с.
274. Словник юридичних термінів / Ф. Андерш, В. Винник, А. Красницька та ін. Київ : Юрінком Інтер, 1993. 320 с.
275. Слотило О. Відмежування понять “грінмейл” та “рейдерство”, їх кримінально-правове значення. *Підприємство, господарство і право*. 2019. № 6. С. 258–261.
276. Соколова Л. В., Колісник О. В. Науково-методичний підхід до аналізу ознак банкрутства енергогенеруючих підприємств. *Наук. вісник Херсон. ун-ту*. 2016. С. 76–80. (Сер. екон. науки ; вип. 16, ч. 4).
277. Сосновська О. О., Казак О. О. Актуальні загрози кадровій безпеці сучасних підприємств. *Проблеми економіки*. 2018. № 3 (37). С. 144–150.
278. Статистична інформація Офісу Генерального прокурора. URL : <https://www.gp.gov.ua/ua/1stat> (дата звернення : 28.03.2021 р.).
279. Стогній К. О. Дослідження передумов виникнення корпоративних конфліктів. *Бізнес Інформ*. 2015. № 4. С. 311–315. URL : http://nbuv.gov.ua/UJRN/binf_2015_4_51 (дата звернення: 31.10.2018 р.).
280. Судакова О. І. Стратегічне управління фінансовою безпекою підприємства. *Економічний простір*. 2008. № 9. С. 142.
281. Талєб Н. Н. Чорний лебідь: про неймовірне у реальному житті. Київ : Наш формат. 2017. 392 с.
282. Тараненко М. М., Ярош І. С. Роль людини в гібридній війні: українська революція 1917–1921 рр. та сучасність. *Юридичний науковий електронний журнал*. 2021. № 2. С. 36–39. URL : http://lsej.org.ua/2_2021/8.pdf (дата звернення: 11.11.2021 р.).
283. Терещук О. В. Адміністративна відповідальність за корупційні правопорушення : дис. ... канд. юрид. наук: 12.00.07. Одеса, 2000. 177 с.

284. Тивончук І. О., Глинська Г. Я. Особливості рейдерства в Україні. *Вісник Національного ун-ту “Львівська політехніка”. Менеджмент та підприємництво в Україні : етапи становлення і проблеми розвитку* : збірник наук. праць. Львів : НУ “Львівська політехніка”, 2008. № 624. С. 146–150.
285. Титаренко С. С. Кримінальна відповідальність за протиправне захоплення суб’єктів господарювання : дис. ... канд. юрид. наук : 12.00.08. Дніпро. 2018. 262 с.
286. Тіньова економіка : сутність, особливості та шляхи легалізації / [за ред. З. С. Варналія]. Київ : НІСД, 2006. 576 с.
287. Тіньова економіка в Україні : масштаби та напрямки подолання / Т. А. Тишук, Ю. М. Харазішвілі, О. В. Іванов [та ін.] ; за ред. Я. А. Жаліла. Київ : НІСД, 2011. 31 с.
288. Томма Р. П., Шевчук О. О. Поняття та наслідки фіктивного банкрутства як заходу економічної відповідальності господарюючого суб’єкта. *Наук. вісник Міжнар. гуманітар. ун-ту*. 2015. № 15, т. 2. С. 65–67. (Сер. Юриспруденція).
289. Уроки гібридного десятиліття: що треба знати для успішного руху вперед : Звіт на запит Офісу Віце-прем’єр-міністра з питань європейської та євроатлантичної інтеграції України та Урядового офісу координації європейської та євроатлантичної інтеграції в рамках діяльності Платформи Україна–НАТО з вивчення досвіду протидії гібридній війні / за редакцією Ганни Шелест. Київ, 2019. URL : http://prismua.org/wp-content/uploads/2019/02/Hybrid_10.pdf (дата звернення: 04.02.2020 р.).
290. Фінанси в трансформаційній економіці України : [навч. посібник] / [за ред. д-ра екон. наук, проф. М. І. Крупки]. Львів : Видавничий центр ЛНУ імені Івана Франка, 2007. 614 с.
291. Фінансова безпека підприємств і банківських установ : [монографія] / А. О. Єпіфанов, О. Л. Пластун, В. С. Домбровський [та ін.] ; [за заг. ред. А. О. Єпіфанова]. Суми : ДВНЗ “УАБС НБУ”, 2009. 295 с.
292. Фінансовий менеджмент : підручник / за ред. д-ра екон. наук, проф. М. І. Крупки ; [М. І. Крупка, О. М. Ковалюк, В. М. Коваленко, Л. С. Яструбецька та ін.]. Львів : ЛНУ імені Івана Франка, 2019. 440 с.

293. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення: монографія / Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич, В. В. Каркавчук, [за ред. Т. Г. Васильціва]. Львів : Ліга-Прес, 2012. 388 с.
294. Фіскально-бюджетні механізми забезпечення фінансової безпеки держави: колективна монографія / Г. Я. Аніловська, М. Й. Штангрет [та ін.] ; [за ред. Г. Я. Аніловської та М. Й. Штангрета]. Львів : СПОЛОМ, 2012. 464 с.
295. Ховаючись у всіх на очах. Війна Путіна проти України: Звіт Атлантичної ради США / М. Чуперські, Дж. Ед. Гербст, Е. Гігінз, А. Полякова, Д. Вілсон. 2015. URL : https://www.files.ethz.ch/isn/191186/HPS_Ukrainian_web.pdf (дата звернення: 04.02.2020 р.).
296. Цвайг Х. І., Галайко Н. В. Загрози фінансовій безпеці підприємства та шляхи їх усунення. *Економічний науково-практичний журнал "Причорноморські економічні студії"*. 2016. Вип. 11. С. 183.
297. Чайка Г. Л. Культура ділового спілкування менеджера. Київ : Знання, 2005. 442 с.
298. Чеберяк П. П. Наукова розробленість проблемних питань розслідування справ про банкрутство. *Адвокат*. 2011. № 12 (135). С. 35–37.
299. Чернишов Г. М. До питання про визначення фінансового шахрайства. *Наук. вісник Ужгород. ун-ту*. 2014. С. 230–234. (Сер. Право ; вип. 26.). URL : http://nbuv.gov.ua/UJRN/nvuzhpr_2014_26_61 (дата звернення: 08.02.2018 р.).
300. Чернявський С. С. Становлення та розвиток інституту банківської неспроможності: історико-правовий аспект. *Наук. вісник Нац. академії внутрішніх справ України*. 2005. № 5. С. 282–296.
301. Шевцов І. Корпоративне шахрайство в українських компаніях: розпізнати і запобігти. *Довідник економіста*. № 6. 2019. С. 64–68.
302. Шлемко В. Т., Бінько І. Ф. Економічна безпека України: сутність і напрямки забезпечення: [монографія]. Київ : НІСД, 1997. 144 с.
303. Шульга І. П. Роль інсайдерської інформації у забезпеченні економічної безпеки акціонерних товариств. *Інвестиції : практика та досвід*. 2010. № 17. С. 36–40. URL :

- http://www.investplan.com.ua/pdf/17_2010/10.pdf (дата звернення: 04.04.2018 р.).
304. Юридична енциклопедія : в 6 т. / [редкол.: Ю. С. Шемшученко (голова редколегії) та ін.]. Київ : Укр.енцикл., 1998. Т. 2. 1999.
305. Юридичний словник-довідник / за ред. Ю. С. Шемшученка. Київ : Феміда, 1996. 696 с.
306. Юрченко О. М. Рейдерство в Україні. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2 (28). С. 81–246.
307. Як грамотно захиститися від рейдерства: найпоширеніші помилки бізнесу. *Економічна правда*. URL : <https://www.epravda.com.ua/projects/antyreid/2020/12/22/669323/> (дата звернення: 26.02.2021 р.).
308. Яструбецька Л. С. Вплив персоналу на інформаційну складову фінансової безпеки суб'єктів підприємництва в Україні. *Стратегії інноваційного розвитку економіки країни: підприємство, регіон, держава* : матеріали Всеукр. наук.-практ. конф. Київ : Таврійський національний університет імені В. І. Вернадського. 2022. С. 58–62.
309. Яструбецька Л. С. Гібридний фінансовий конфлікт як загроза фінансовій безпеці суб'єктів підприємництва в Україні. *Науково-практичний журнал “Економічні студії”*. 2021. Вип. 1 (31). С. 173–179. URL : <http://surl.li/epndf>
310. Яструбецька Л. С. Гібридні фінансові конфлікти в підприємницькій діяльності : сутність та узагальнена характеристика. *Економічна безпека: держава, кластер, підприємство* : матеріали II Міжнар. наук. конф. Рига : Baltija Publishing, 2021. С. 63–67.
311. Яструбецька Л. С. Інформаційне забезпечення суб'єктів фінансових відносин як об'єкт захисту. *Економічний простір* : зб. наук. праць. Дніпро : ПДАБА, 2020. № 159. С. 157–161. URL : <http://surl.li/eptbq>
312. Яструбецька Л. С. Класифікація грошових потоків підприємств – важлива складова ефективного управління ними. *Збірник матеріалів на пошану доктора економічних наук, професора, заслуженого діяча науки і техніки Степана Злупка*. Львів : Видавничий центр Львівського національного університету імені Івана Франка, 2006. С. 455–464.

313. Яструбецька Л. С. Класифікація корупційних дій в підприємницькій діяльності. *Конкурентоспроможність економіки країни в світовому аспекті* : зб. матер. Всеукр. наук.-практ. конф. Київ : ГО “Київський економічний науковий центр”, 2022. С. 79–84.
314. Яструбецька Л. С. Комплексна методика оцінки рівня фінансової безпеки суб’єктів підприємництва в Україні за умов гібридних загроз. *Підприємництво та інновації* : наук.-практ. журнал. 2021. № 17. С. 75–83. URL : <http://surl.li/epswg>
315. Яструбецька Л. С. Корупція як системна проблема забезпечення фінансової безпеки суб’єктів підприємництва в Україні. *Визначальні дослідження у сучасному світі економіки* : збірник матеріалів Наук.-практ. конф. Східноукраїнський інститут економіки та управління. Запоріжжя : ГО “СІЕУ”, 2022. С. 62–64.
316. Яструбецька Л. С. Корупція як системна проблема фінансової безпеки в Україні. *Науковий вісник Ужгородського національного університету*. С. 171–178. (Серія : Міжнародні економічні відносини та світове господарство ; вип. 36/2021). URL : <http://surl.li/eptbv>
317. Яструбецька Л. С. Критерій гібридності в класифікації загроз фінансовій безпеці суб’єктів підприємництва України. *Наукові дослідження в сучасному світі економіки : матеріали Наук.-практ. конф.* Дніпро : “Перспектива”, 2022. С. 73–77.
318. Яструбецька Л. С. Методи протидії рейдерству в Україні. *Вісник Львівського університету*. 2019. С. 298–304. (Серія економічна ; вип. 57). Львів : Львівський національний університет імені Івана Франка. URL : <http://surl.li/epsxd>
319. Яструбецька Л. С. Методи протидії фінансовим злочинам в підприємницькій діяльності. *Економічні стратегії в аспекті управлінського розвитку* : збірник тез наукових робіт учасників Всеукр. наук.-практ. конф. ГО “Центр економічних досліджень та розвитку”. Одеса : ЦЕДР, 2022. С. 73–76.
320. Яструбецька Л. С. Недобросовісна конкуренція як гібридний фінансовий конфлікт. *Приазовський економічний вісник*. 2021. Вип. 2 (25). С. 207–212. URL : <http://pev.kpu.zp.ua/vypusk-2-25>
321. Яструбецька Л. С. Нелегальне банкрутство як системна проблема фінансової безпеки суб’єктів господарювання в Україні. *Формування*

- ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2017. Вип. 37 (Ч. 2). С. 260–263.
322. Яструбецька Л. С. Ознаки виявлення рейдерського захоплення бізнесу в Україні. *Актуальні питання економіки в контексті глобальних викликів* : матеріали Всеукр. наук.-практ. конф. ГО “Львівська економічна фундація”. Львів : ЛЕФ, 2022. С. 77–79.
323. Яструбецька Л. С. Ознаки фінансового шахрайства в діяльності суб’єктів підприємництва в Україні. *Реформування економіки в контексті міжнародного співробітництва : механізми та стратегії* : матеріали Міжнар. наук.-практ. конф. Запоріжжя. 2022. С. 78–80.
324. Яструбецька Л. С. Особливості організації рейдерських захоплень підприємств в Україні. *Економіка та суспільство*. 2017. № 9. С. 1107–1112. URL : <http://economyandsociety.in/ua>
325. Яструбецька Л. С. Оцінка благонадійності працівників як інструмент протидії фінансовому шахрайству на підприємстві в умовах пандемії Covid-19. *Economy digitalization in a pandemic conditions: processes, strategies, technologies* : Proceedings of the II International Scientific Conference. Riga, Latvia : “Baltija Publishing”, 2022. 168 p.
326. Яструбецька Л. С. Проблеми та перспективи удосконалення системи податкового обліку в Україні. *Формування ринкової економіки в Україні* : наук. збірник. Львів : Інтереко, 2009. Вип. 19. С. 485–491.
327. Яструбецька Л. С. Рейдерство як конфліктна форма перерозподілу власності в Україні. *Таврійський науковий вісник*. 2021. С. 105–112. (Серія : Економіка ; Вип. 6). URL : <http://surl.li/epsxj>
328. Яструбецька Л. С. Теоретико-методологічні основи формування організаційно-економічного механізму управління грошовими потоками промислових підприємств України. *Вісник Львівського університету*. Львів : ВЦ ЛНУ імені Івана Франка. 2006. С. 385–391. (Серія економічна ; вип. 35).
329. Яструбецька Л. С. Тіньова економічна діяльність як загроза фінансовій безпеці України. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2018. Вип. 40. Ч. 2. С. 264–271.

330. Яструбецька Л. С. Управління грошовими потоками підприємств в умовах ринкової економіки : сутність, значення та принципи реалізації. *Економіка: проблема теорії та практики* : зб. наук. праць. Дніпропетровськ : ДНУ, 2006. Вип. 216. Т. IV. С. 939–944.
331. Яструбецька Л. С. Грошові потоки в оцінці інвестиційного проекту підприємництва. *Фінанси України*. 2005. С. 101–109.
332. Яструбецька Л. С. Фінансове шахрайство як загроза фінансовій безпеці суб'єктів підприємництва в Україні. *Розвиток соціально-економічної системи держави та регіонів* : матеріали наук.-практ. конф. Херсон : Видавництво “Молодий вчений”, 2021. С. 68–72.
333. Яструбецька Л. С. Формування страхового резерву грошових коштів в системі заходів підвищення рівня фінансової безпеки промислових підприємств. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2012. Вип. 26. Ч. 2. С. 324–331.
334. Яструбецька Л. С., Демко В. В. Аналіз фінансових результатів діяльності підприємств України. *Актуальні проблеми економіки і фінансів* : матеріали IV Міжнар. наук.-практ. конф. URL : <http://surl.li/eptdb>
335. Яструбецька Л. С., Дуфенюк О. М. Визначення та систематизація чинників впливу на формування грошових потоків промислових підприємств України. *Науковий вісник Львівського державного університету внутрішніх справ* : зб. наук. праць / за ред. Р. І. Тринько. Львів, 2006. С. 183–193. (Серія економічна ; вип. 1 (3)).
336. Яструбецька Л. С., Дуфенюк О. М. Проблеми визначення джерел інвестиційних ресурсів в умовах розвитку ринкових форм господарювання. *Вісник Львівського університету*. Львів, 2007. С. 417–421. (Серія економічна ; вип. 37 (1)).
337. Яструбецька Л. С., Мелевич С. М. Теоретичні засади державної фінансової підтримки розвитку малих підприємств в Україні. *Тенденції розвитку економіки у 2019 році: аналітичний та теоретико-методологічний аспекти* : матеріали Всеукраїнської науково-практичної конференції / відп. за випуск д. е. н., проф. С. О. Якубовський. Одеса : ОНУ імені І. І. Мечникова, 2019. С. 99–101.

338. Яструбецька Л. С., Онишкевич Н. А. Проблеми виникнення кризових явищ на підприємстві. *Західноукраїнський науковий вісник* : матеріали III Міжрегіональної наук.-практ. конф. “Україна на шляху до реформ: політико-правові проблеми сучасності”. Івано-Франківськ : ГО “ЗУНТ”, 2013. Вип. 2. С. 49–54.
339. Яструбецька Л. С., Підхормний О. М. Особливості забезпечення фінансової безпеки суб’єктів господарювання в умовах кризи. *Формування ринкової економіки в Україні* : зб. наук. праць Львів : Львівський національний університет імені Івана Франка, 2010. Вип. 21. С. 464–468.
340. Яструбецька Л. С., Терешко О. М. Напрями підвищення рівня захисту конфіденційної фінансової інформації підприємств. *Проблеми становлення інформаційної економіки в Україні* : матеріали Всеукр. наук.-практ. конф. (пам’яті завідувача кафедрою інформаційних систем у менеджменті, професора Юринця В. Є. присвячується). Львів : Львівський національний університет імені Івана Франка ; Ліга-Прес, 2014. С. 287–289.
341. Яструбецька Л. С., Терешко О. М. Особливості забезпечення фінансових інтересів суб’єктів господарювання. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2019. Вип. 41 (Ч. 2). С. 165–173.
342. Яструбецька Л. С., Терешко О. М. Рейдерство як загроза фінансовій безпеці суб’єктів господарювання в Україні. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2016. Вип. 35. (Ч. 2). С. 317–322.
343. Яструбецька Л. С., Яремик М. М. Аналіз особливостей злиття та поглинання підприємств в Україні. *Науковий вісник НЛТУ України*. 2015. Вип. 25.7. С. 239–245. URL: <http://surl.li/eptcn>
344. Яструбецька Л. С., Яструбецький В. О. Захист інформації в системі управління фінансовою безпекою підприємств. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2013. Вип. 29. (Ч. 2). С. 292–298.

345. Яструбецька Л. С., Яструбецький В. О. Класифікація загроз фінансовій безпеці підприємницьких структур. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2011. Вип. 24. С. 426–430.
346. Яструбецька Л. С., Яструбецький В. О. Фінансові злочини в банківських установах. *Проблеми забезпечення економічної безпеки держави та суб'єктів господарювання* : матеріали Міжкафедрального круглого столу. Львів : СПОЛЮМ, 2012. С. 109–110.
347. Яструбецька Л. С., Яструбецький В. О., Марченко О. М. Управління фінансовою безпекою господарських структур : суб'єктно-об'єктний підхід. *Формування ринкової економіки в Україні* : зб. наук. праць. Львів : Львівський національний університет імені Івана Франка, 2011. Вип. 23. Ч. 2. С. 356–363.
348. Яструбецька Л. С., Яструбецький В. О., Підхонний О. М. Фінансова компетентність як чинник безпеки суб'єктів господарювання. *Науковий вісник Львівського державного університету внутрішніх справ* : зб. наук. праць / головний редактор Р. І. Тринько. Львів : Львівський державний університет внутрішніх справ, 2011. С. 210–219. (Серія економічна ; вип. 2).
349. A cross-impact analysis of the bank payment card market parameters and non-financial sectors' indicators in the Ukrainian economy / A. Mints, O. Kolodiziev, M. Krupka, B. Vyshyvana, L. Yastrubetska. *Banks and Bank Systems*. 2022. 17 (2). P. 163–177. URL : <http://surl.li/eptci>
350. Bank crediting to the sector of non-financial corporations in Ukraine / Yuliia Verheliuk, Yuliia Koverninska, Vladimir Korneev, Alexey Kononets. *Banks and Bank Systems*. 2019. Vol. 14. Iss. 3. P. 64–75. URL : [http://dx.doi.org/10.21511/bbs.14\(3\).2019.06](http://dx.doi.org/10.21511/bbs.14(3).2019.06) (дата звернення: 24.07.2022 р.).
351. Biden J. R., Carpenter M. How to stand up to the Kremlin. *Foreign Affairs*. 2018. URL : <https://www.foreignaffairs.com/articles/2017-12-05/how-stand-kremlin> (дата звернення: 10.04.2021 р.).
352. Boyatzis R. E. *The Competent Manager: A Model for Effective Performance*. Wiley. 1991. 328 p.

353. Bryce J. *Modern Democracies*. New York : The Macmillan Company, 1921. Vol. 2. 508 p. URL : <https://oll.libertyfund.org/title/bryce-modern-democracies-vol-1> (дата звернення: 06.07.2018 р.).
354. Byrne U. Wheel of Life: Effective steps for stress management. *Business Information Review*. 2005. 22(2). P. 123–130. URL : https://www.researchgate.net/publication/240284066_Wheel_of_LifeEffective_steps_for_stress_management (дата звернення: 01.07.2018 р.).
355. Companies' Financial Security Mechanism Under Hybrid Conflicts / L. Yastrubetska, I. Krupka, V. Kovalenko, N. Zhmurko, O. Mykuliak. *Universal Journal of Accounting and Finance*. 2022. Vol. 10, No. 1. P. 113–123. URL : <http://surl.li/eptca>
356. Confidence as the national economy pricing and shadowing factor: The case of Ukraine / O. Pidkhomnyi, N. Demchyshak, Y. Dropa. *Revista ESPACIOS*. 2019. Vol. 40 No. 20 P. 21. URL : <https://www.revistaespacios.com/a19v40n20/19402021.html> (дата звернення: 08.08.2020 р.).
357. Coser L.A. Social Conflict and the Theory of Social Change. *The British Journal of Sociology*. Vol. 8, No. 3. (Sep., 1957). pp. 197–207. <http://www.csun.edu/~snk1966/Lewis%20A%20Coser%20Social%20Conflict%20and%20the%20Theory%20of%20Social%20Change.pdf> (дата звернення: 31.07.2018 р.).
358. Cressey D. R. The differential association theory and compulsive crimes. *Journal of Criminal Law and Criminology*. 1954. vol. 45, no. 1. pp. 29–40. URL : <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=4221&context=jclc> (дата звернення: 01.07.2018 р.).
359. Dahrendorf R. *Class and Class Conflict in Industrial Society*. Stanford University Press. 1959. URL : <https://cominsitu.files.wordpress.com/2019/01/ralf-dahrendorf-class-and-class-conflict-in-industrial-society-1.pdf> (дата звернення: 10.08.2018 р.).
360. Deutsch M. Conflicts: productive and Destructive. *Journal of Social issues*. 1969. Vol. XXV. № 1. URL : https://www.researchgate.net/publication/229568996_Conflicts_Productive_and_Destructive (дата звернення: 10.08.2018 р.).

361. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. URL : <https://eur-lex.europa.eu/eli/dir/2018/1673/oj> (дата звернення: 01.09.2019 р.).
362. Dubois D. The competency casebook. Amherst, MA: HRD Press. 1998. 334 p.
363. Elsey E. The complete guide to the wheel of life. The Coaching Tools Company. July 27, 2022. URL : <https://www.thecoachingtoolscompany.com/wheel-of-life-complete-guideeverything-you-need-to-know> (дата звернення: 01.09.2022 р.).
364. Emotional intelligence / P. Salovey, B. T. Detweiler-Bedell, J. B. Detweiler-Bedell, J. D. Mayer. In M. Lewis, J. M. Haviland-Jones, & L. F. Barrett (Eds.), *Handbook of emotions*. 2008. P. 533–547. The Guilford Press. URL : <https://psycnet.apa.org/record/2008-07784-033> (дата звернення: 21.03.2021 р.).
365. English Oxford living Dictionaries. URL : <https://en.oxforddictionaries.com/definition/challenge> (дата звернення: 17.09.2021 р.).
366. Financial security management under the conditions of digitalization: the state and business entities / L. Yastrubetska, M. Orel, N. Havrylenko, O. Tonkykh, V. Yefimov. *International Journal of Computer Science & Network Security (IJCSNS)*. October 2021. Vol. 21 No. 10. P. 310–316. URL : http://paper.ijcsns.org/07_book/202110/20211044.pdf
367. Foley E., Kaunert C. Russian Private Military and Ukraine: Hybrid Surrogate Warfare and Russian State Policy by Other Means. *Central European Journal of International and Security Studies*. 2022. Vol. 16, Iss. 3. P. 172–192. URL : https://www.cejiss.org/images/docs/Issue_16-3/Foley_Kaunert_-_16-3_web.pdf (дата звернення: 11.11.2021 р.).
368. Friedrich C. J. Corruption Concepts in Historical Perspective / Edited by A. J. Heidenheimer, M. Johnston. *Political Corruption: Third Edition*. New York: 2017. P. 15–24 URL: <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315126647-2/corruption-concepts-historical-perspective-carl-friedrich> (дата звернення: 11.11.2022 р.).

369. Goleman D. Emotional Intelligence (The 10th Anniversary Edition). Bantam Books: New York. 2005. 352 p. URL : <https://asantelim.files.wordpress.com/2018/05/daniel-goleman-emotional-intelligence.pdf> (дата звернення: 11.11.2021 р.).
370. Hybrid war – hybrid response? *NATO Review*, 01.07.2014. URL : <https://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/EN/index.htm> (дата звернення: 11.09.2018 р.).
371. International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation. *The FATF Recommendations*. 16.02.2012. URL : <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> (дата звернення: 01.08.2022 р.).
372. Internet Crime Report. Internet crime complaint Center & Federal Bureau of Investigation. URL : https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (дата звернення: 02.07.2021 р.).
373. Introduction of NSFR Ratio on the Activities of Commercial Banks in Ukraine / M. Dziamulych, T. Shmatkovska, M. Krupka, L. Yastrubetska, B. Vyshyvana, S. Derevianko. *Universal Journal of Accounting and Finance*. 2021. Vol. 9 (6). P. 1544–1550. URL : <https://www.hrpub.org/download/20211130/UJAF31-12225290.pdf>
374. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response. / European Commission. Brussels. 2016. URL : <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN> (дата звернення: 29.09.2018 р.).
375. Kasapoglu C. Russia's Renewed Military Thinking: Non-Linear Warfare and Relaxed Control. *NATO Research Paper*. November 2015. No 121. URL : <https://nsarchive.gwu.edu/document/16337-nato-defense-college-russia-s-renewed-military> (дата звернення: 16.10.2018 р.).
376. Kelling G. L., Wilson J. Q. Broken Windows. The police and neighborhood safety. *The Atlantic*. March 1982. URL : <https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/> (дата звернення: 30.09.2018 р.).

377. Lasconjarias G., Larsen J. A. NATO's Response to Hybrid Threats. *NDC Research Division*. 2015. 337 p. URL : https://www.files.ethz.ch/isn/195405/fp_24.pdf (дата звернення: 12.07.2018 р.).
378. Maurer T., Nelson A. "Global Cyber Threat". *Finance and development*. March, 2021 P. 24–27. URL : <https://www.imf.org/en/Publications/fandd/issues/2021/03/global-cyber-threat-to-financial-systems-maurer> (дата звернення: 11.10.2021 р.).
379. Mayer J. D., Caruso D. R., Salovey P. Emotional intelligence meets traditional standards for an intelligence. *Intelligence*. 1999. Vol. 27. P. 267–298. URL : <https://www.sciencedirect.com/science/article/abs/pii/S0160289699000161?via%3Dihub> (дата звернення: 12.07.2018 р.).
380. Meyer H. *Real-World Intelligence*. New York : Storm King Press, 1991. 102 p.
381. Nye J. Corruption and Political Development: A Cost-benefit Analysis. *American Political Science*. 1967. №2 (61). P. 417–427. URL : <https://www.jstor.org/stable/1953254> (дата звернення: 22.07.2018 р.).
382. Peter L. J., Hull. R. *The Peter Principle. Why Things Always Go Wrong*. 2020. Profile Books Ltd. London. URL : https://profilebooks.com/wp-content/uploads/wpallimport/files/PDFs/9781788166058_preview.pdf (дата звернення: 12.07.2021 р.).
383. Pindjak P. Deterring Hybrid Warfare: A Chance for NATO and the EU to work together. *NATO Review*, 18 November 2014, URL : <https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html> (дата звернення: 12.07.2018 р.).
384. Racz A. Russia's Hybrid War in Ukraine: breaking the enemy's ability to resist. *FIIA Report*. 43, 2015. URL : https://www.academia.edu/13041864/Russia_s_Hybrid_War_in_Ukraine_Breaking_the_Enemy_s_Ability_to_Resist (дата звернення: 20.07.2018 р.).
385. Reeves Shane R. and Barnsby Robert E. The new griffin of war: hybrid international armed conflicts. *Harvard International Relations Council*.

- Inc. 2013. Vol. 34. Iss. 3. URL : <https://go.gale.com/ps/i.do?id=GALE%7CA316203914&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=07391854&p=AONE&sw=w&userGroupName=anon%7Ea1e6f244> (дата звернення: 18.10.2018 р.).
386. Report to the nations 2020 “Global study on occupational fraud and abuse”. URL : <https://www.acfe.com/report-to-the-nations/2020> (дата звернення: 21.03.2021 р.).
387. Schmidt Frank L., Hunter John E. The Validity and Utility of Selection Methods in Personnel Psychology: Practical and Theoretical Implications of 100 Years of Research Findings. *Working Paper October*. 2016, 74 p. URL : <https://home.ubalt.edu/tmitch/645/session%204/Schmidt%20&%200h%20validity%20and%20util%20100%20yrs%20of%20research%20Wk%20PPR%202016.pdf> (дата звернення: 10.08.2021 р.).
388. Sornette Didier. Dragon-Kings, Black Swans and the Prediction of Crises. *International Journal of Terraspace Science and Engineering*. 2009. Vol. 1. 18 p. URL : <https://arxiv.org/pdf/0907.4290.pdf> (дата звернення: 10.09.2021 р.).
389. Swart J. The Wheel of Life as a Coaching Tool to Audit Life Priorities. November 2022. URL : https://www.researchgate.net/publication/365375169_The_Wheel_of_Life_as_a_Coaching_Tool_to_Audit_Life_Priorities (дата звернення: 05.12.2022 р.).
390. The Global Competitiveness Report 2013–2014 Index. URL : <http://reports.weforum.org/the-global-competitiveness-report-2013-2014/> (дата звернення: 10.08.2021 р.).
391. The management of technology transfer and its impact on business activity and financial security in developing countries / Y. Bocharova, M. Kokhan, L. Yastrubetska, I. Muratova, Y. Ishchuk, V. Kuliavets. *AD ALTA: Journal of interdisciplinary research*. 2021. Vol. 11 (2). Special issue XXIV. P. 204–209. URL : <http://surl.li/eptcf>
392. The Military Balance. URL : <https://www.iiss.org/publications/the-military-balance/the-military-balance-2015> (дата звернення: 10.11.2018 р.).
393. The shadow economy’s phenomenon and its impact on the development of corporate business and households in Ukraine (Феномен тіньової економіки та її вплив на розвиток корпоративного бізнесу та

- домашніх господарств в Україні) / В. В. Коваленко, М. О. Слатвінська, З. С. Варналій, С. А. Шелудько, Т. В. Валігура. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2022. Т. 3(44). С. 328–337. (Web of Science). URL : <https://fkd.net.ua/index.php/fkd/article/view/3763/3603> (дата звернення: 05.11.2022 р.).
394. Vandiver J. “SACEUR: Allies must prepare for Russia “hybrid war””. *Stars and Stripes*. September 4, 2014. URL : <http://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464> (дата звернення: 12.04.2021 р.).
395. Wales Summit Declaration. *NATO Official website*. 05.09.2014. URL : https://www.nato.int/cps/en/natohq/official_texts_112964.htm (дата звернення: 25.08.2018 р.).
396. Warsaw Summit Communiqué. *North Atlantic Treaty Organization*. 09.07.2016 р. URL : https://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата звернення: 12.04.2018 р.).
397. Wever O. Buzan B., Kelstrup M. Identity, Migration and the New Security *Agenda in Europe*. Macmillan, 1993. 221 p.
398. Wheel of Life, an initial investigation: Topic-related polarity visualization in personal stories / H. D. P. Santos, G. P. D. Molin, J. Pinheiro, R. Vieira. *Proceedings of Symposium in Information and Human Language Technology*. Uberlandia, MG, Brazil, October 2–5, 2017. URL : <https://aclanthology.org/W17-6606/> (дата звернення: 08.08.2021 р.).
399. Wucker Michele. *The Gray Rhino: How to Recognize and Act on the Obvious Dangers We Ignore*. St. Martin's Press. 2016. 304 p.
400. Yastrubetska L., Dolyna I. Factors impacting information security of enterprises. *Проблеми становлення інформаційної економіки в Україні* : матеріали Міжнар. наук.-практ. конф. (м. Львів, 2015 р.). Львів : Ліга-Прес, 2015. С. 129–132.

ДОДАТКИ

ДОДАТОК А

Таблиця А.1

Перелік суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні, на яких було проведено анкетування щодо впливу гібридних фінансових конфліктів на їх фінансову безпеку

№п/п	Суб'єкт підприємництва
1.	ТОВ "Поділлянафтозбут"
2.	ТОВ "Вест Ойл Трейдінг"
3.	ТОВ "Західнафтозбут"
4.	ТОВ "Окко-Бізнес партнер"
5.	АТ "Концерн Галнафтогаз"
6.	ТОВ "Поділлянафтотрейд"
7.	ТОВ "СНІРО ОІЛ"
8.	ТОВ "Дімакс-К"
9.	ТОВ "Росток"
10.	ТОВ "ОККО-СХІД"
11.	ТОВ "СП ГАЗ-ЮГ"
12.	ТОВ "ВАМОІЛ-Л"
13.	ТОВ "Лемберг Рітейл"
14.	ТОВ "КОМПАНІЯ ТРЕЙД ОІЛ"
15.	МПП "Ірена"
16.	ТОВ "ОККО-РЕСУРС"
17.	ТОВ "ПЕНТА ОІЛ"
18.	ТОВ "ВІЛАТЕКС-ТК"
19.	ТОВ "ЕВО 5"
20.	ТОВ "МІНІТОП"

Джерело: сформувала автор

ДОДАТОК Б

Таблиця Б.1

Фахівці, залучені до експертної оцінки ефективності протидії гібридним фінансовим конфліктам в діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні

№ п/п	Експерт	Напрямок діяльності
1.	Виконавчий директор ГС “Спілка Українських Підприємців”	Громадська активність щодо захисту інтересів суб'єктів підприємництва України (підхід з позиції громадського моніторингу ситуації)
2.	Керівник ТОВ “Консалтингова група “А-95”	Проведення професійних досліджень (підхід з позиції моніторингу ситуації ЗМІ)
3.	Заступник начальника Управління стратегічних розслідувань в Івано-Франківській області ДСР Національної поліції України	Моніторинг фінансових зловживань в практиці функціонування суб'єктів підприємництва України (підхід з позиції державного контролю)
4.	Начальник Головного управління ДФС у Львівській області (2015-2021 рр.)	Контроль за фінансовими зловживаннями в частині порушень податкового законодавства (підхід з позиції державного контролю)
5.	Керівник управління середнього бізнесу Західного МРУ АТ КБ “Приватбанк”	Оцінка рівня фінансової безпеки (підхід з позиції кредитора)

Джерело: сформувала автор

ДОДАТОК В

Таблиця В.1

Узагальнена експертна оцінка вагомості впливу гібридних фінансових конфліктів на фінансову безпеку суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні

Показник	Оцінка вагомості впливу показника на фінансову безпеку, %					
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Середнє значення
Протидія корупції	20%	5%	20%	10%	10%	13%
Запобігання недобросовісній конкуренції	5%	5%	5%	20%	10%	9%
Попередження та ліквідація фінансового шахрайства працівників	20%	15%	20%	10%	20%	17%
Запобігання відмиванню доходів, одержаних злочинним шляхом	35%	15%	25%	10%	10%	19%
Протидія конфліктам з держ. органами	5%	20%	15%	10%	20%	14%
Запобігання конфліктам з інститутами фінансово-кредитної сфери	5%	30%	5%	5%	5%	10%
Протидія рейдерству	5%	5%	5%	25%	20%	12%
Нейтралізація інформаційних загроз	5%	5%	5%	10%	5%	6%
Разом	100%	100%	100%	100%	100%	100%

Джерело: сформувала автор

ДОДАТОК Г

Таблиця Г.1

Узагальнена експертна оцінка ефективності протидії гібридним фінансовим конфліктам в діяльності суб'єктів підприємництва, що займаються виробництвом та оптовою і роздрібною торгівлею паливом в Україні

Показник	ТОВ “Поділья-нафтозбут”	АТ “Концерн Галнафтогаз”	ТОВ “Захід-нафтозбут”	ТОВ “ОККО-Бізнес Партнер”	ТОВ “Вест Ойл Трейдинг”	МПП “Ірена”
Протидія корупції	0,8	1,1	0,9	1,1	0,9	0,5
Запобігання недобросовісній конкуренції	0,5	0,6	0,6	0,7	0,6	0,4
Попередження та ліквідація фінансового шахрайства працівників	1,1	1,5	1,4	1,3	1,2	0,7
Запобігання відмиванню доходів, одержаних злочинним шляхом	1,2	1,8	1,4	1,6	1,3	0,8
Протидія конфліктам з держ.органами	0,8	1,1	1,0	1,1	0,9	0,6
Запобігання конфліктам з інститутами фінансово-кредитної сфери	0,8	1,0	0,8	0,9	0,8	0,6
Протидія рейдерству	0,8	1,1	0,8	1,1	0,8	0,6
Нейтралізація інформаційних загроз	0,4	0,4	0,4	0,5	0,4	0,3
Показник ЕПГФК	6,4	8,7	7,4	8,3	7,0	4,7

Джерело: сформувала автор

ДОДАТОК Д

Таблиця Д.1

**Аналіз ефективності методів відбору кандидатів
при прийнятті на роботу**

Метод	Валідність (validity)	Множинна регресія	Зміни внаслідок долучення нового методу		Стандартизована зважена регресія	
			Приріст валідності	Зростання валідності, %	GMA	Додатковий метод
Тест загальних розумових здібностей (GMA)	0,51					
Робочі завдання	0,54	0,63	0,12	24	0,36	0,41
Тести на благонадійність	0,41	0,65	0,14	27	0,51	0,41
Тести особистісних характеристик	0,31	0,60	0,09	18	0,51	0,31
Структуроване інтерв'ю	0,51	0,63	0,12	24	0,39	0,39
Неструктурована співбесіда	0,38	0,55	0,04	8	0,43	0,22
Тести професійних знань	0,48	0,58	0,07	14	0,36	0,31
Випробувальний термін	0,44	0,58	0,07	14	0,40	0,20
Оцінка колег	0,49	0,58	0,07	14	0,35	0,31
Біхевіоральний метод	0,45	0,58	0,07	14	0,39	0,31
Перевірка рекомендацій	0,26	0,57	0,06	12	0,51	0,26
Досвід роботи (років)	0,18	0,54	0,03	6	0,51	0,18
Автобіографічні дані	0,35	0,52	0,01	2	0,45	0,13
Центри оцінювання	0,37	0,53	0,02	4	0,43	0,15
Бальний метод оцінки (кількість років навчання)	0,10	0,52	0,01	2	0,51	0,10
Тести професійних інтересів	0,10	0,52	0,01	2	0,51	0,10
Графологія	0,02	0,51	0,00	0	0,51	0,02
Вік	-0,01	0,51	0,00	0	0,51	-0,01
*Збільшення валідності методу у відсотках відповідає росту його практичної цінності						

Джерело: сформувала автор на основі [387]

ДОДАТОК Е

Таблиця Е.1

*Перелік досліджуваних суб'єктів підприємництва в Україні,
що зазнали рейдерських атак*

№п/п	Суб'єкт підприємництва
1.	ВАТ “Житомирхліб”
2.	ВАТ “Агрофірми “Провесін”
3.	Група компаній ТМ “БРСМ-Нафта”
4.	Сільськогосподарське ТОВ “Колос”
5.	НАСК “Оранта”
6.	СПП “Чумаки”
7.	ТОВ “Немирівський лікєро-горілчаний завод “Nemiroff”
8.	ВАТ “КРАЯН”
9.	ВАТ “Львівська макаронна фабрика”
10.	ВАТ “Фармак”
11.	ВК “Захар Беркут”
12.	АТ Дім марочних кон'яків “Гаврія”
13.	ДП “Конярство України”
14.	ВАТ “Житомирські ласощі”
15.	ЗАТ “Оболонь”
16.	ЗАТ “Одесакондитер”
17.	ЗАТ “Фармацевтична фірма “Дарниця”
18.	Група компаній ТМ “Бунге Україна”
19.	ПАТ “Аграрний фонд”
20.	ПАТ “Укрнафта”
21.	АТ “Об'єднана гірничо-хімічна компанія”
22.	ПАТ АК “Київводоканал”
23.	ПАТ ВО “Стальканат-Силур”
24.	ПАТ “Квазар”
25.	ПАТ “Промінвестбанк”
26.	ПрАТ “АТЕК”
27.	ПрАТ “Рижанівський гранітний кар'єр”
28.	ПрАТ ТРК “Фора”
29.	ТВК “Глобус”
30.	Телеканал “Телерадіосвіт”
31.	ТОВ “А-ба-ба- га-ла-ма-га”
32.	ТОВ “Книгарня Сяйво”
33.	ТОВ “Епіцентр”
34.	ТОВ “Профтім”
35.	ТОВ “Фокстрот”
36.	ТОВ ПП “Еконія”
37.	ТОВ “Оптова мережа 2011” (ТРЦ SKY MALL)
38.	ТЦ «“Амстор”»
39.	ПрАТ “Універмаг “Україна”
40.	ФГ “Строгого О.Ф.”

41.	ТОВ “Юридична інвестиційна компанія Форум”
42.	ТОВ “Винхол Оксамитне” (ТМ Villa Tinta)
43.	ТОВ “БФ-АГРО-ТРЕЙД”
44.	ТОВ “Іллінецький цукровий завод”
45.	ТОВ “Октагон-Ауддор”
46.	“Укркінохроніка”
47.	ФГ “Мирлобне”
48.	ТОВ “Миколаївський глиноземний завод”
49.	ФГ “ТРУД 2012”
50.	ЗАТ “ВОЛИНЬ-ЛАДА”
51.	ТОВ “Овостар Юніон”
52.	Група компаній ТМ “Т.В. Fruit”
53.	ПАТ “МСЗ “Океан”
54.	ТОВ “ДФУ “АГРО”
55.	ТОВ “Братський маслопресовий завод”
56.	ТОВ “Вікторія”
57.	ВАТ “Львівський хлібокомбінат”

Джерело: сформувала автор

ДОДАТОК Ж

Таблиця Ж.1

**Результати оцінювання фінансових параметрів забезпечення
фінансової безпеки МПП “Ірена”**

Фінансові показники	Умови за яких забезпечується фінансова безпека		МПП “Ірена”							
	Оптимальне значення	Тенденція зміни значення показника впродовж 2019-2021рр	Значення показника					Виконання умов		Інтерпретація результатів оцінки, бали
			2017 р.	2018 р.	2019 р.	2020 р.	2021 р.	Оптимальне значення	Тенденція	
Показники ліквідності										
Коефіцієнт загальної ліквідності	не менше 1- 2	позитивна	1,63	1,67	1,30	1,71	1,81	+	+	1
Коефіцієнт критичної ліквідності	не менше 0,7-0,8	позитивна	0,82	1,06	1,16	1,70	1,71	+	+	1
Коефіцієнт абсолютної ліквідності	не менше 0,15-0,20	позитивна	0,00	0,00	0,00	0,41	0,17	+	-	1
Показники фінансової стійкості										
Коефіцієнт загальної заборгованості	менше 0,5	позитивна	0,49	0,49	0,51	0,51	0,497	+	+	1
Коефіцієнт співвідношення позикового і власного капіталу	0,7-2,0	позитивна	0,96	0,95	1,05	1,05	0,99	+	+	1
Коефіцієнт фінансової незалежності	більше 0,5	позитивна	0,51	0,51	0,49	0,49	0,503	+	+	1
Показники ділової активності										
Коефіцієнт оборотності дебіторської заборгованості	зростання	позитивна	40,72	46,85	22,99	15,57	24,91		+	1
Коефіцієнт оборотності кредиторської заборгованості	зростання*	позитивна	-	33,08	21,76	20,92	38,44		+	1
Коефіцієнт оборотності активів	зростання	позитивна	3,75	4,78	3,23	2,63	4,47		+	1
Показники прибутковості										
Коефіцієнт рентабельності продажів	більше 0,05	позитивна	0,03	0,01	0,00	0,02	0,01	-	-	0
Коефіцієнт рентабельності активів	більше 0,14	позитивна	0,10	0,06	0,01	0,05	0,07	-	+	0
Коефіцієнт рентабельності власного капіталу	більше 0,20	позитивна	0,21	0,12	0,03	0,09	0,13	-	+	0
РАЗОМ										9

Джерело: сформувала автор

ДОДАТОК И

Таблиця И.1

**Результати оцінювання фінансових параметрів забезпечення
фінансової безпеки ТОВ “Західнафтозбут”**

Фінансові показники	Умови за яких забезпечується фінансова безпека		ТОВ “Західнафтозбут”							
	Оптимальне значення	Тенденція зміни значення показника впродовж 2019-2021pp	Значення показника					Виконання умов		Інтерпретація результатів оцінки, бали
			2017 р.	2018 р.	2019 р.	2020 р.	2021 р.	Оптимальне значення	Тенденція	
Показники ліквідності										
Коефіцієнт загальної ліквідності	не менше 1- 2	позитивна	6,94	15,19	1,34	1,23	0,77	-	-	0
Коефіцієнт критичної ліквідності	не менше 0,7-0,8	позитивна	6,39	15,12	1,34	1,23	0,77	+	-	1
Коефіцієнт абсолютної ліквідності	не менше 0,15-0,20	позитивна	5,09	7,20	0,19	0,28	0,03	-	-	0
Показники фінансової стійкості										
Коефіцієнт загальної заборгованості	менше 0,5	позитивна	0,16	0,11	0,75	0,82	1,285	-	-	0
Коефіцієнт співвідношення позикового і власного капіталу	0,7-2,0	позитивна	0,18	0,12	3,03	4,51	- 4,51	-	-	0
Коефіцієнт фінансової незалежності	більше 0,5	позитивна	0,84	0,89	0,25	0,18	-0,285	-	-	0
Показники ділової активності										
Коефіцієнт оборотності дебіторської заборгованості	зростання	позитивна	209,77	269,21	41,01	21,78	10,58	-	-	0
Коефіцієнт оборотності кредиторської заборгованості	зростання*	позитивна	116,33	305,43	50,26	22,69	16,88	-	-	0
Коефіцієнт оборотності активів	зростання	позитивна	70,46	24,86	30,46	13,32	7,38	-	-	0
Показники прибутковості										
Коефіцієнт рентабельності продажів	більше 0,05	позитивна	0,00	- 0,03	0,00	0,01	- 0,07	-	-	0
Коефіцієнт рентабельності активів	більше 0,14	позитивна	0,31	- 0,74	0,15	0,19	- 0,48	-	-	0
Коефіцієнт рентабельності власного капіталу	більше 0,20	позитивна	0,95	- 0,87	0,44	0,99	-	-	-	0
РАЗОМ										1

Джерело: сформувала автор

ДОДАТОК К

Таблиця К.1

**Результати оцінювання фінансових параметрів забезпечення
фінансової безпеки АТ “Концерн Галнафтогаз”**

Фінансові показники	Умови за яких забезпечується фінансова безпека		АТ “Концерн Галнафтогаз”							
	Оптимальне значення	Тенденція зміни значення показника впродовж 2019-2021pp	Значення показника					Виконання умов		Інтерпретація результатів оцінки, бази
			2017 р.	2018 р.	2019 р.	2020 р.	2021 р.	Оптимальне значення	Тенденція	
Показники ліквідності										
Коефіцієнт загальної ліквідності	не менше 1-2	позитивна	0,58	0,49	0,41	0,44	1,34	+	+	1
Коефіцієнт критичної ліквідності	не менше 0,7-0,8	позитивна	0,56	0,44	0,38	0,44	1,34	+	+	1
Коефіцієнт абсолютної ліквідності	не менше 0,15-0,20	позитивна	0,005	0,001	0,000	0,001	0,001	-	-	0
Показники фінансової стійкості										
Коефіцієнт загальної заборгованості	менше 0,5	позитивна	0,7	0,6	0,6	0,5	0,5	+	+	1
Коефіцієнт співвідношення позикового і власного капіталу	0,7-2,0	позитивна	1,88	1,68	1,34	0,93	1,10	+	+	1
Коефіцієнт фінансової незалежності	більше 0,5	позитивна	0,3	0,4	0,4	0,5	0,5	+	+	1
Показники ділової активності										
Коефіцієнт оборотності дебіторської заборгованості	зростання	позитивна	37,41	30,64	14,78	7,13	7,18		+	1
Коефіцієнт оборотності кредиторської заборгованості	зростання*	позитивна	11,26	13,46	18,26	8,21	6,97		-	0
Коефіцієнт оборотності активів	зростання	позитивна	0,42	0,22	0,28	0,17	0,15		-	0
Показники прибутковості										
Коефіцієнт рентабельності продажів	більше 0,05	позитивна	0,18	0,22	0,31	0,76	0,37	+	+	1
Коефіцієнт рентабельності активів	більше 0,14	позитивна	0,08	0,05	0,09	0,13	0,06	-	-	0
Коефіцієнт рентабельності власного капіталу	більше 0,20	позитивна	0,25	0,13	0,22	0,28	0,12	-	-	0
РАЗОМ										7

Джерело: сформувала автор

ДОДАТОК Л

Таблиця Л.1

**Результати оцінювання фінансових параметрів забезпечення
фінансової безпеки ТОВ “Поділлянафтозбут”**

Фінансові показники	Умови за яких забезпечується фінансова безпека		ТОВ “Поділлянафтозбут”							
	Оптимальне значення	Тенденція зміни значення показника впродовж 2019-2021рр	Значення показника					Виконання умов		Інтерпретація результатів оцінки, бали
			2017 р.	2018 р.	2019 р.	2020 р.	2021 р.	Оптимальне значення	Тенденція	
Показники ліквідності										
Коефіцієнт загальної ліквідності	не менше 1- 2	позитивна	0,9	0,8	0,9	0,7	1,0	+	+	1
Коефіцієнт критичної ліквідності	не менше 0,7-0,8	позитивна	0,4	0,2	0,4	0,3	0,9	+	+	1
Коефіцієнт абсолютної ліквідності	не менше 0,15-0,20	позитивна	0,1	0,1	0,1	0,1	0,1	-	+	0
Показники фінансової стійкості										
Коефіцієнт загальної заборгованості	менше 0,5	позитивна	1,0	1,0	0,9	1,0	1,0	-	-	0
Коефіцієнт співвідношення позикового і власного капіталу	0,7-2,0	позитивна	200,7	90,3	11,6	137,6	-174,5	-	-	0
Коефіцієнт фінансової незалежності	більше 0,5	позитивна	0,0	0,0	0,1	0,0	0,0	-	-	0
Показники ділової активності										
Коефіцієнт оборотності дебіторської заборгованості	зростання	позитивна	43,6	84,4	97,2	117,0	26,8		-	0
Коефіцієнт оборотності кредиторської заборгованості	зростання*	позитивна	10,3	13,7	8,7	7,7	10,8		+	1
Коефіцієнт оборотності активів	зростання	позитивна	9,6	13,3	8,2	7,3	10,9		+	1
Показники прибутковості										
Коефіцієнт рентабельності продажів	більше 0,05	позитивна	0,0	0,0	0,0	0,0	0,0	-	-	0
Коефіцієнт рентабельності активів	більше 0,14	позитивна	0,0	0,0	0,1	0,0	0,0	-	+	0
Коефіцієнт рентабельності власного капіталу	більше 0,20	позитивна	1,4	1,1	1,7	-0,4	-12,2	-	-	0
РАЗОМ										4

Джерело: сформувала автор

ДОДАТОК М

Таблиця М.1

**Результати оцінювання фінансових параметрів забезпечення
фінансової безпеки ТОВ “Вест Ойл Трейдинг”**

Фінансові показники	Умови за яких забезпечується фінансова безпека		ТОВ “Вест Ойл Трейдинг”					
	Оптимальне значення	Тенденція зміни значення показника впродовж 2019-2021pp	Значення показника					Інтерпретація результатів оцінки, бали
			2019	2020	2021	Оптимальне значення	Тенденція	
Показники ліквідності								
Коефіцієнт загальної ліквідності	не менше 1- 2	позитивна	-	0,64	0,65	-	+	0
Коефіцієнт критичної ліквідності	не менше 0,7-0,8	позитивна	-	0,36	0,29	-	-	0
Коефіцієнт абсолютної ліквідності	не менше 0,15-0,20	позитивна	-	0,03	0,06	-	+	0
Показники фінансової стійкості								
Коефіцієнт загальної заборгованості	менше 0,5	позитивна	-	1,09	1,20	-	-	0
Коефіцієнт співвідношення позикового і власного капіталу	0,7-2,0	позитивна	-	-12,60	- 6,03	-	-	0
Коефіцієнт фінансової незалежності	більше 0,5	позитивна	-	- 0,09	- 0,20	-	-	0
Показники ділової активності								
Коефіцієнт оборотності дебіторської заборгованості	зростання	позитивна	-	40,83	45,84		+	1
Коефіцієнт оборотності кредиторської заборгованості	зростання*	позитивна	-	2,30	4,88		+	1
Коефіцієнт оборотності активів	зростання	позитивна	-	1,44	4,90		+	1
Показники прибутковості								
Коефіцієнт рентабельності продажів	більше 0,05	позитивна	-	- 0,15	- 0,06	-	+	0
Коефіцієнт рентабельності активів	більше 0,14	позитивна	-	- 0,21	- 0,30	-	-	0
Коефіцієнт рентабельності власного капіталу	більше 0,20	позитивна	-	-	-	-	-	0
РАЗОМ								3

Джерело: сформувала автор

ДОДАТОК Н

Таблиця Н.1

**Результати оцінювання фінансових параметрів забезпечення
фінансової безпеки ТОВ “ОККО-Бізнес партнер”**

Фінансові показники	Умови за яких забезпечується фінансова безпека		ТОВ “ОККО-Бізнес Партнер”					
	Оптимальне значення	Тенденція зміни значення показника впродовж 2019-2021рр	Значення показника			Виконання умов		Інтерпретація результатів оцінки, бали
			2019	2020	2021	Оптимальне значення	Тенденція	
Показники ліквідності								
Коефіцієнт загальної ліквідності	не менше 1- 2	позитивна	0,72	1,03	1,07	+	+	1
Коефіцієнт критичної ліквідності	не менше 0,7-0,8	позитивна	0,72	0,88	0,86	+	+	1
Коефіцієнт абсолютної ліквідності	не менше 0,15-0,20	позитивна	0,00	0,01	0,01	-	+	0
Показники фінансової стійкості								
Коефіцієнт загальної заборгованості	менше 0,5	позитивна	1,31	0,98	0,94	-	+	0
Коефіцієнт співвідношення позикового і власного капіталу	0,7-2,0	позитивна	-4,24	39,72	14,70	-	-	0
Коефіцієнт фінансової незалежності	більше 0,5	позитивна	-0,31	0,02	0,06	-	+	0
Показники ділової активності								
Коефіцієнт оборотності дебіторської заборгованості	зростання	позитивна	16,91	45,43	65,93		+	1
Коефіцієнт оборотності кредиторської заборгованості	зростання*	позитивна	78,96	86,10	114,63		+	1
Коефіцієнт оборотності активів	зростання	позитивна	5,92	3,56	3,64		+	1
Показники прибутковості								
Коефіцієнт рентабельності продажів	більше 0,05	позитивна	0,06	0,03	0,01	-	-	0
Коефіцієнт рентабельності активів	більше 0,14	позитивна	0,38	0,10	0,04	-	-	0
Коефіцієнт рентабельності власного капіталу	більше 0,20	позитивна	-1,23	-13,48	0,93	+	+	1
РАЗОМ								6

Джерело: сформувала автор

ДОДАТОК П

ТИПОВІ СЦЕНАРІЇ ВПРОВАДЖЕННЯ ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНИХ ЗАХОДІВ ПРОТИДІЇ ГІБРИДНИМ ФІНАНСОВИМ КОНФЛІКТАМ			
Фінансове шкідливість	Підготовчий етап протидії гібридним фінансовим конфліктам	Оцінка наявного стану протидії гібридним фінансовим конфліктам	Впровадження заходів із підвищення ефективності протидії гібридним фінансовим конфліктам
	Формулювання мети, завдань, області, суб'єктів та принципів протидії фінансовому шкідливості	Оцінка шкідливої безпеки суб'єкта підприємства	Удосконалення механізмів виявлення при оцінці кадрової безпеки та не впровадження винних працівників
	Визначення засобів виявлення та розслідування фінансового шкідливості	Аналіз чинників організаційного характеру, недієвих законів і процесів, суттєвих фінансових злочинств	Вирозумлення оптимальних фінансово-економічних заходів протидії фінансовому шкідливості
	Розроблення стандартів і процедур протидії фінансовому шкідливості	Встановлення засадової протидії, як генерують заходи виявлення фінансового шкідливості	Впровадження оптимальних етико-моральних заходів протидії фінансовому шкідливості
Документальне закріплення в Кодексі корпоративної культури	Розслідування фінансового шкідливості та визначення проблем дієвості наявних методів протидії	Заспокоєння оптимальних організаційно-етичних заходів протидії фінансовому шкідливості	Заспокоєння оптимальних організаційно-етичних заходів протидії фінансовому шкідливості
Корупція	Формулювання мети, завдань, області, суб'єктів та принципів формування антикорупційної політики	Оцінка корупційних ризиків, генерованих працівниками суб'єкта підприємства	Усузнення недоліків, виявлених при оцінці корупційних ризиків
	Визначення антикорупційних стандартів і процедур	Оцінка корупційних ризиків, генерованих контрастними суб'єктами підприємства	Інформування уповноважених служб про реальні та потенційні випадки випадки корупції
Недобросовісна конкуренція	Документальне закріплення в Кодексі антикорупційної політики	Оцінка корупційних ризиків, генерованих державними службовцями	Неузгоджене поворнення винних осіб та закриття інформація про випадки корупції
	Формулювання мети, завдань, області, суб'єктів та принципів протидії недобросовісній конкуренції	Розслідування усіх корупційних дій та визначення проблем дієвості наявних антикорупційних заходів	Впровадження спеціальних, технічних та етико-моральних антикорупційних заходів
Недобросовісна конкуренція	Визначення методів, стандартів і процесів дієвої політики	Аналіз корупційної поведінки суб'єкта підприємства на основі кількісних та якісних показників	Усузнення недоліків, виявлених в дієвості опійних конкурентів
	Документальне закріплення в Кодексі конкурентної політики	Аналіз конкурентного середовища на предмет прояву недобросовісної конкуренції	Розроблення та впровадження оптимальних методів і заходів реалізації конкурентної стратегії
Рейдерство	Формулювання мети, завдань, області, суб'єктів та принципів протидії рейдерству	Розслідування випадків антикорупційних дій та зазначення проблем дієвості наявних методів протидії	Інформування уповноважених служб про реальні та потенційні випадки недобросовісної конкуренції
	Встановлення етико-моральної ієрархії загрози рейдерству	Аналіз типових схем рейдерського захоплення в Україні та оцінка наявних методів протидії	Співпраця з державними органами та громадськими асоціаціями в протидії недобросовісній конкуренції
Рейдерство	Визначення та документальне закріплення методів, стандартів і процедур протидії рейдерству	Моніторинг реальних оцінок загрози рейдерства	Впровадження заходів превентивного захисту
	Визначення та документальне закріплення методів, стандартів і процедур протидії рейдерству	Визначення проблем, дієвості наявних заходів протидії рейдерству	Фінансово-економічна Політика
			Організаційно-етичний
			Розроблення заходів естерно о реалізації

Рис. П.1. Типові сценарії впровадження організаційно-економічних заходів протидії гібридним фінансовим конфліктам в діяльності суб'єктів підприємництва

Джерело: сформувала автор

ДОДАТОК Р

Таблиця Р.1

Показники для оцінювання рівня захищеності конфіденційно
фінансової інформації

Індикатор інформаційної безпеки	Розрахункова формула	Умовні позначення	Порогове значення
Оцінка програмно-технічної захищеності конфіденційної фінансової інформації			
Коефіцієнт технічного захисту інформації (Кт.з.)	$K_{т.з.} = I_{а.н.}$	<i>I</i> _{а.н.} – кількість невідвернутих інформаційних атак, од.	Зменшення
Коефіцієнт фінансового захисту інформації (Кф.з.)	$K_{ф.з.} = \frac{B_{а.інф.}}{B_{пр.інф.}}$	<i>B</i> _{з.інф.} – витрати на захист інформаційних ресурсів, грн; <i>B</i> _{пр.інф.} – витрати на придбання інформаційних ресурсів	0,15, зростання
Коефіцієнт фінансування інформаційних служб підприємства (Кфін.)	$K_{фін.} = \frac{B_{фін.}}{B_{з.}}$	<i>B</i> _{фін.} – витрати на фінансування інформаційних служб підприємства, грн; <i>B</i> _{з.} – загальні витрати підприємства, грн	0,05– 0,15, зростання
Коефіцієнт програмної захищеності інформації (Кп.з.)	$K_{п.з.} = \frac{Ч_{б.ф.}}{Ч_{н.ф.}}$	<i>Ч</i> _{б.ф.} – час безперебійного функціонування корпоративної інформаційної системи, год.; <i>Ч</i> _{н.ф.} – нормативний час функціонування корпоративної інформаційної системи, год.	1, зростання
Оцінка інформаційної надійності персоналу, зокрема осіб, що приймають рішення (ОПР)			
Коефіцієнт повноти інформації (Кп.)	$K_{п.} = \frac{I_{н.}}{I_{необ.}}$	<i>I</i> _{н.} – обсяг інформації, що наявна в розпорядженні ОПР, %; <i>I</i> _{необ.} – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %	1, зменшення
Коефіцієнт точності інформації (Кт.)	$K_{т.} = \frac{I_{р.}}{I_{н.}}$	<i>I</i> _{р.} – обсяг релевантної інформації, %; <i>I</i> _{н.} – загальний обсяг наявної в ОПР інформації, %	1, зростання
Коефіцієнт своєчасності надання інформації (Кс.н.)	$K_{с.н.} = \frac{I_{с.н.}}{I_{необх.}}$	<i>I</i> _{с.н.} – обсяг своєчасно наданої ОПР інформації, %; <i>I</i> _{необх.} – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %	1, зростання
Коефіцієнт надійності інформації (Кн.)	$K_{н.} = \frac{I_{н.}}{I_{з.}}$	<i>I</i> _{н.} – обсяг інформації, наданої ОПР з надійних джерел, %; <i>I</i> _{з.} – загальний обсяг наданої ОПР інформації, %	1, зростання
Коефіцієнт правової захищеності інформації (Кпр.з.)	$K_{пр.з.} = \frac{I_{н.н.}}{I_{пр.з.}}$	<i>I</i> _{н.н.} – обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, %; <i>I</i> _{пр.з.} – загальний обсяг юридично захищеної інформації, %	1, зменшення

Продовження таблиці Р.1

Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства (Кн.п.)	$K_{н.п.} = \frac{ЧП_{з.зв.} - ЧП_{зв.в.}}{ЧП_{з.зв.}}$	<i>ЧПз.зв.</i> – загальна кількість звільнених працівників, осіб; <i>ЧПзв.в.</i> – кількість працівників, звільнених з причини витоку інформації, осіб	1, зростання
Коефіцієнт підготовленості персоналу до розпізнавання загроз (Кп.п.)	$K_{п.п.} = \frac{ЧП_з. - ЧП_{н.д.}}{ЧП_з.}$	<i>ЧПз.</i> – загальна кількість працівників, що мають доступ до закритої інформації, осіб; <i>ЧПн.д.</i> – кількість працівників, ненавмисні дії яких призвели до витоку інформації, осіб	1, зростання
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства (Кд.р.)	$K_{д.р.} = \frac{ЧП_{д.1}}{ЧП_з.}$	<i>ЧПд.1</i> – кількість працівників, які мають доступ до закритої інформації та працюють більше одного року, осіб; <i>ЧПз.</i> – загальна кількість працівників, що мають доступ до закритої інформації, осіб	1, зростання

Джерело: сформувала автор на основі [81, с. 174–175]

НАУКОВЕ ВИДАННЯ

Яструбецька Леся Сергіївна
кандидат економічних наук

**ФІНАНСОВА БЕЗПЕКА СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УКРАЇНІ В
УМОВАХ ГІБРИДНИХ ЗАГРОЗ**

Монографія

*Редактор Уляна Крук
Обкладинка Тараса Мухи*

Формат 60×84/16. Гарнітура Times New Roman.
Друк цифровий. Папір офсетний.
Умов. друк. арк. 20,14. Обл.-вид. арк. 18,52.
Наклад 100 прим.

Львівський національний університет імені Івана Франка
79005, м. Львів, вул. Університетська, 1.
тел./факс:, 235-72-13

Свідоцтво державної реєстрації
ДК № 3059 від 13.12.2007 р.