

Львівський державний університет
внутрішніх справ

В. І. Франчук

ТЕОРІЯ БЕЗПЕКИ СОЦІАЛЬНИХ СИСТЕМ

Підручник

Львів–Одеса
Фенікс
2020

УДК 65.012.8(075)
Ф85

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол від 29 січня 2020 р. № 6).

Р е ц е н з е н т и:

М. І. Флейчук – доктор економічних наук, професор, професор кафедри міжнародних економічних відносин Львівської комерційної академії Центральної спілки споживчих товариств України;

П. Я. Пригунов – кандидат психологічних наук, професор, директор департаменту секретаріату Кабінету Міністрів України з питань безпеки, оборони, діяльності органів юстиції та протидії корупції

Франчук В. І.

Теорія безпеки соціальних систем : підручник. 2-ге вид., перероб. і допов. / І. І. Франчук. – Львів; Одеса : Фенікс, 2020. – 224 с.

ISBN 978-966-928-583-6

Розглянуто питання безпеки соціальних систем. Навчальний матеріал викладено з урахуванням інноваційних досягнень безпекової наукової думки, синтезу науки й практики. Це сприяє формуванню системних і комплексних компетентностей щодо питань безпекової діяльності.

Для здобувачів вищої освіти та аспірантів у галузі знань управління й адміністрування під час вивчення навчальної дисципліни «Теорія безпеки соціальних систем», суб'єктів безпекової діяльності, науковців, а також усіх, хто цікавиться окресленою проблематикою.

УДК 65.012.8(075)

ISBN 978-966-928-583-6

© Франчук В. І., 2020

ЗМІСТ

ВСТУП.....	6
Тема 1 БЕЗПЕКА ЯК СОЦІАЛЬНЕ ЯВИЩЕ ТА УМОВА ЖИТТЄДІЯЛЬНОСТІ.....	9
1.1 Етимологія та сутність поняття «безпека соціальної системи».....	10
1.2 Структура поняття «безпека соціальної системи».....	13
1.3 Логіка зв'язків між структурними елементами поняття «безпека соціальної системи»	19
Тема 2 СОЦІАЛЬНА СИСТЕМА ЯК ОБ'ЄКТ БЕЗПЕКИ	26
2.1 Сутність та основні властивості соціальної системи.....	27
2.2 Внутрішнє і зовнішнє середовище соціальної системи.....	30
2.3 Корінні функції життєдіяльності соціальної системи.....	33
Тема 3 КОРПОРАТИВНА КУЛЬТУРА ТА ЇЇ ВПЛИВ НА БЕЗПЕКУ ОРГАНІЗАЦІЇ	40
3.1 Сутність понять «корпоративна культура» та «безпекова корпоративна культура»	41
3.2 Безпекова підготовка фахівців у вищих навчальних закладах	43
3.3 Підвищення кваліфікації, курсова підготовка менеджерів з питань безпеки	46
Тема 4 КОРПОРАТИВНІ ІНТЕРЕСИ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ СОЦІАЛЬНОЇ СИСТЕМИ	51
4.1 Сутність приватних, групових та пов'язаних інтересів, їх вплив на безпеку соціальної системи	52
4.2 Сутність корпоративних інтересів та їх значення для безпеки соціальної системи.....	54
4.3 Корпоративні інтереси з розвитку та безпеки, їх сутність та значення для життєдіяльності організації	56
Тема 5 ЗАГРОЗИ СОЦІАЛЬНІЙ СИСТЕМІ.....	62
5.1 Сутність понять «виклик», «загроза», «небезпека», відмінності між ними та їх вплив на життєдіяльність соціальної системи	63
5.2 Класифікація загроз соціальній системі.....	66

5.3	Форми загроз, їх сутність, зміст та механізми реалізації.....	68
Тема 6	БЕЗПЕКОВА ДІЯЛЬНІСТЬ СОЦІАЛЬНОЇ СИСТЕМИ.....	79
6.1	Сутність та структура безпекової діяльності.....	80
6.2	Механізми безпекової діяльності.....	82
6.2.1	Попереджувально-профілактичні механізми безпекової діяльності.....	82
6.2.2	Інформаційно-виявляючі механізми безпекової діяльності.....	85
6.3	Ліквідаційні механізми безпекової діяльності.....	88
6.4	Відновлювальні механізми безпекової діяльності.....	91
6.5	Видові функції, методи та засоби безпекової діяльності.....	92
Тема 7	МЕТОДОЛОГІЯ БЕЗПЕКОВОЇ ДІЯЛЬНОСТІ СОЦІАЛЬНОЇ СИСТЕМИ.....	101
7.1	Сутність поняття «методологія».....	102
7.2	Безпекова діяльність як об'єкт та метод пізнання.....	104
7.3	Структура методології безпеки організації.....	108
Тема 8	СИСТЕМА БЕЗПЕКИ ОРГАНІЗАЦІЇ.....	117
8.1	Структура та загальна характеристика системи безпеки організації.....	118
8.2	Цілі та завдання системи безпеки організації.....	124
8.3	Принципи та режим функціонування системи безпеки організації.....	126
8.4	Суб'єкти, сили та об'єкти безпеки.....	129
Тема 9	ДІАГНОСТИКА СТАНУ БЕЗПЕКИ СОЦІАЛЬНОЇ СИСТЕМИ.....	144
9.1	Концептуально-методичний підхід до діагностики стану безпеки організації.....	145
9.2	Критерії діагностики стану та визначення рівня безпеки організації.....	148
Тема 10	УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЇ.....	155
10.1	Безпекова філософія та структура системи управління безпековою діяльністю.....	156
10.2	Сутність, структура та загальна характеристика технології управління безпековою діяльністю.....	159
10.3	Сутність та характеристика функцій управління.....	162

ПРАКТИКУМ З ДІАГНОСТИКИ БЕЗПЕКИ СОЦІАЛЬНИХ СИСТЕМ

Вступ	174
Методика діагностики загроз соціальній системі	175
Методика діагностики реалізації безпекових корпоративних інтересів.....	179
Методика діагностики стану справ в акціонерному товаристві із захистом корпоративних прав.....	183
Методика діагностики безпекової корпоративної культури	187
Методика діагностики та визначення рівня ефективності безпекової діяльності	191
Методика діагностики та визначення рівня безпеки організації	204
СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ БЕЗПЕКОЗНАВСТВА.....	211
СПИСОК ЛІТЕРАТУРИ	220

ВСТУП

*Вдумливе вивчення
теорії безпеки соціальних систем
та застосування її на практиці
може врятувати організацію
від руйнування*

Основною ланкою у соціальних системах та у відносинах, що формуються у середині та з навколишнім середовищем, завжди є людина. Своєю поведінкою, діяльністю, окрім позитивного впливу, вона може завдавати шкоди природі, людині, суспільству та машинам. З іншого боку, сама ж людина може бути об'єктом загрози, тобто втратити здоров'я, життя, власне майно тощо. Крім того, природні катаклізми також можуть дестабілізувати діяльність соціальних систем. Відтак кожна соціальна система упродовж свого існування зазнає тих чи інших втрат у різних формах. Щоб їх уникнути чи зменшити фахівцям потрібні відповідні знання та навички з питань безпеки.

Поняття «безпека» багатоаспектне й складне за своєю структурою. У підручнику запропонований підхід, де забезпечення безпеки соціальної системи обумовлене принциповою єдністю трьох його основних функцій – розвитку, безпеки та управління. Водночас безпека розглядається як комплексне явище, що має фізичну й соціальну природу та виявляється, з одного боку, через стан системи, який має бути у допустимих межах, а з іншого – через безпекову діяльність, що має механізми протидії загрозам з метою захисту корпоративних інтересів, збереження цілісності соціальної системи та сприяння її розвитку. Водночас безпекова діяльність має ґрунтуватися на потребі соціальної системи у безпечному функціонуванні,

безпековій організаційній культурі та сприйнятті менеджерами усіх ланок того, що безпека це ще й філософія сучасного менеджменту.

Розуміння категорії безпеки як функції, підсистеми життєдіяльності організації змінює сам зміст управління нею. Його зміст зводиться до того, щоб навчитися управляти через формування та реалізацію корпоративних інтересів у сфері розвитку й безпеки соціальної системи.

Основна мета підручника – системно викласти основні положення теорії безпеки соціальних систем.

Вивчення тем цього підручника дає змогу сформувати основні безпекові компетентності у майбутніх фахівців та опанувати програмні результати навчання на рівні знань та вмінь, а саме:

знати:

- структуру, основні внутрішні та зовнішні елементи організації та можливий їх дестабілізуючий вплив;
- сутність поняття «безпека» та його структурні елементи;
- сутність та вплив корпоративної культури й корпоративних інтересів на безпеку соціальної системи;
- сутність понять «виклик», «загроза», «небезпека», відмінності між ними та механізми їх впливу на безпеку соціальної системи;
- механізм управління безпековою діяльністю соціальних систем;

уміти:

- визначати, аналізувати та оцінювати дію загроз на життєдіяльність соціальної системи;
- аналізувати та визначати рівень безпеки соціальної системи;
- аналізувати та оцінювати ефективність безпекової діяльності соціальної системи;
- формувати систему безпеки організації;
- застосовувати наукові підходи до визначення загроз, рівня безпеки соціальної системи та ефективності функціонування її системи безпеки;

– застосовувати знання методології безпеки соціальних систем у практичній й науковій діяльності.

Підручник складається з двох частин: теоретичної та практичної. У першій – системно викладено основні сучасні знання про безпеку соціальних систем, а у другій – запропоновано практикум, який спрямований на формування безпекових умінь. Всі теми підручника апробовані у навчальному процесі, а також є результатом наукових досліджень, які презентовані на науково-практичних заходах.

Загалом підручник підготовлений згідно з навчальними програмами з предметів «Теорія безпеки соціальних систем», «Теорія та методологія безпеки соціальних систем», які передбачені у навчальних планах підготовки магістрів та докторів філософії у галузі знань управління й адміністрування. Видання також буде корисним науковцям й практикам-менеджерам та безпекознавцям.

Тема 1

БЕЗПЕКА ЯК СОЦІАЛЬНЕ ЯВИЩЕ ТА УМОВА ЖИТТЄДІЯЛЬНОСТІ

*Лише небагато менеджерів та підприємців
сприймають безпеку соціальної системи як явище
та одну із основних умов її життєдіяльності.
Вони беруться за вирішення безпекових проблем
не з'ясувавши істинної сутності та природи
такого комплексного та багатовимірного поняття*

1.1 Етимологія та сутність поняття «безпека соціальної системи»

Поняття «безпека» різноаспектне та складне соціально-політичне і економічне явище, яке об'єктивно має конкретно-історичний характер і пов'язано з усіма формами і напрямками взаємодії в системі «природа–людина–суспільство–машина». У центрі цих відносин завжди є людина, яка своєю поведінкою, діяльністю, окрім позитивного впливу, може завдавати шкоди природі, іншій людині, суспільству та машинам. З іншого боку, людина теж може стати об'єктом загрози, тобто втратити здоров'я, життя, власне майно тощо (рис. 1.1).

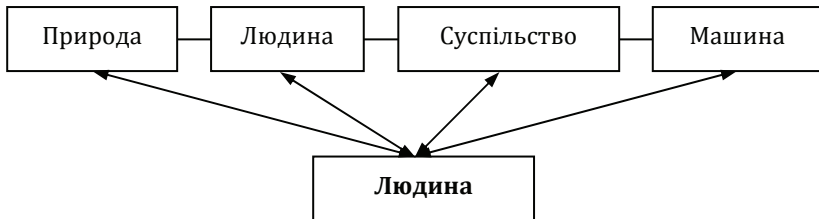


Рис. 1.1 Схема взаємодії людини в системі
«природа–людина–суспільство–машина»

У такій ситуації забезпечення безпеки людини, соціальної системи – це імператив буття, обумовлений принциповою єдністю трьох його основних функцій – розвитку, безпеки та управління.

Без функцій розвитку та управління ефективна реалізація функції безпеки неможлива. Водночас функція безпеки охоплює інструменти до пізнання стану системи та розуміння її як єдиного цілісного нерозривного організму.

Термін «безпека» трактується в енциклопедичних словниках як попередження, усунення та захист від небезпек. Відтак, за В. Далем, термін безпека – це відсутність небезпеки, збере-

женість, надійність [12], за С. Ожеговим, безпека – це стан за якого не загрожує небезпека, є захист від небезпеки [37].

Трактування безпеки через відсутність небезпеки не коректна, оскільки досягти ідеальної ситуації у реальному житті практично не можливо. Для людини бути в безпеці не значить жити без загроз. Вони завжди існували, існують і будуть існувати. Тому важливо навчитися, з одного боку, використовувати такі ситуації для мобілізації зусиль в спілкуванні, поведінці та діяльності, з іншого – протидіяти цим загрозам.

Отже, з наведених трактувань поняття «безпека» зрозуміло, що є поле безпеки й небезпеки. Очевидно, що зміна з безпечного рівня чи навпаки відбувається у першому випадку під дією загроз (дестабілізуючих факторів), а в іншому – внаслідок реалізації заходів, спрямованих на протидію цим загрозам (рис. 1.2).



Рис. 1.2 Стан безпеки соціальної системи

Безпека – це не відсутність небезпеки, а захист від неї на системному рівні. Така безпека визначає цілісність системи та цілісність людини, як біологічної та соціальної істоти [33].

Такий підхід пояснюється тим, що категорія «безпека» має біосоціальну дуалістичну природу: фізичну і соціальну, які взаємопов'язані та виявляють себе як єдине ціле (рис. 1.3) [33].

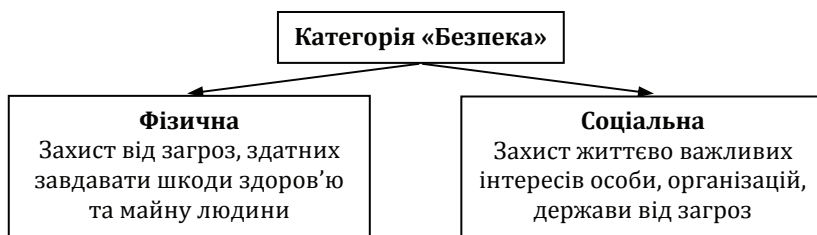


Рис. 1.3 Структура біосоціальної дуалістичної природи категорії «безпека»

Фізична складова категорії «безпека» відображає необхідність захисту закладених природою життєво важливих потреб людини як біологічної істоти і насамперед потреби в самозбереженні. Вона також передбачає протидію загрозам, здатним завдавати шкоди здоров'ю чи майну людини. Сюди належить безпека особи, протипожежна безпека, безпека на транспорті тощо. Також до фізичної безпеки можна віднести захисні механізми, закладені природою. З цього приводу Ціцерон зауважував: «Насамперед кожному виду живих істот природа дарувала властивість захищатися, «...» всього того, що видається шкідливим та набувати і добувати все те, що необхідно для життя» [55].

Соціальна складова категорії «безпека» відображає необхідність захисту життєво важливих інтересів людини як соціальної істоти, підприємства, держави в різних сферах життєдіяльності від внутрішніх і зовнішніх загроз. Це пов'язано з тим, що в соціальних системах біологічна сутність людини має соціально обумовлений характер.

Соціальній складовій категорії «безпека» сьогодні відводиться визначальна і системоутворювальна роль. В міру розвитку людства та держави підхід до категорії «безпека» зміщується від розуміння її як фізичного явища до категорії соціальної, суспільної.

Безпека завжди відносна і має динамічний характер. У кожний конкретний період стан захищеності може мати різні рівні. І це справедливо навіть для кожного вагона одного й того ж поїзда, як доречно зауважує Г. О. Мінаєв.

Змістовного значення категорія «безпека» набуває лише за умови зв'язку з конкретними об'єктами або сферою людської діяльності (безпека людини, безпека організації, безпека економічної системи, безпека держави тощо), характеризуючи стан системи як цілісного організму з погляду досягнутого рівня захисту від загроз [33]. У наукових джерелах є значна кількість тлумачень цього поняття залежно від об'єкта. Наприклад, безпека підприємницької діяльності трактується авторами по-різному – від «захисту проти корисливих злочинів»,

«стану захищеності від внутрішніх та зовнішніх загроз» до «стану ефективного використання корпоративних ресурсів» тощо. Більшість з них мають односторонній, а не системний характер.

Безпека як багатоаспектне та комплексне явище, маючи фізичну й соціальну природу, виявляється, з одного боку, через стан системи, який має перебувати у допустимих межах, а з іншого – через безпекову діяльність, що має:

а) механізми протидії загрозам, а не взагалі;

б) чіткі цілі, а саме: захист корпоративних інтересів, збереження цілісності соціальної системи та сприяння її розвитку.

Водночас безпекова діяльність має ґрунтуватися на потребі соціальної системи у безпечному функціонуванні, на безпековій організаційній культурі, на розумінні менеджерами усіх ланок того, що безпека це ще й філософія сучасного менеджменту.

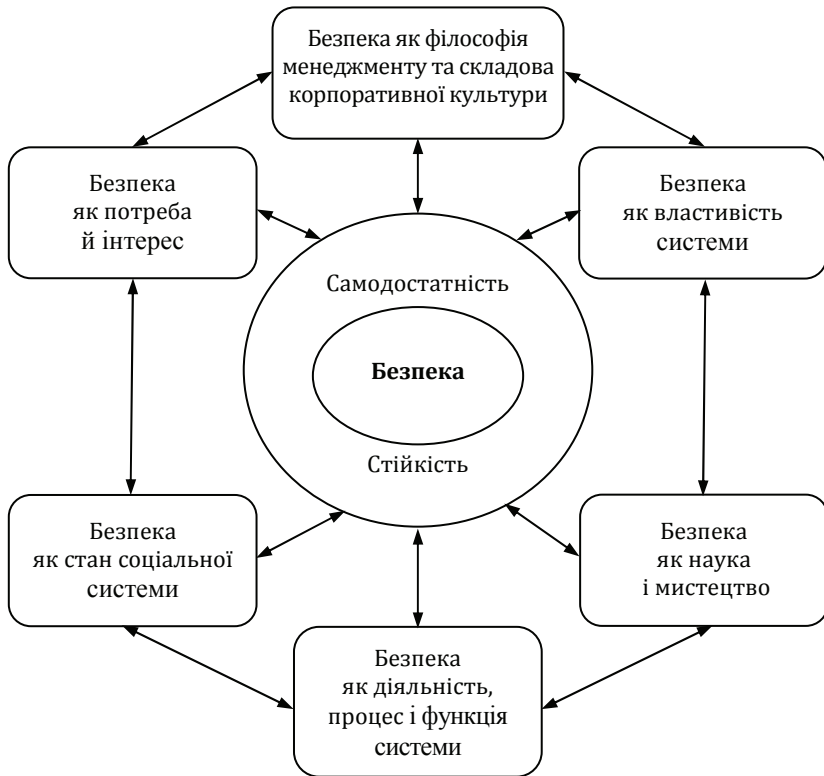
З огляду на такі вимоги, **безпека соціальної системи** – це стан системи в межах граничних значень і здатність протидіяти загрозам чи небезпеці з метою захисту інтересів, збереження цілісності системи та сприяння її розвитку.

1.2 Структура поняття «безпека соціальної системи»

Безпека як біосоціальна дуалістична категорія має низку основних зовнішніх та внутрішніх елементів, кожний з яких розкриває сутність такого складного явища та сукупно формують його змістовну структуру (рис. 1.4).

Безпека як потреба та інтерес соціальної системи. В основі всіх видів та рівнів безпеки соціальних систем знаходиться людина зі своїми потребами та інтересами, які, своєю чергою, є однією із умов життєдіяльності.

Потреба у безпеці є первинною потребою кожної людини і реалізується на індивідуальному, колективному і суспільному рівнях.



*Рис. 1.4 Змістова структура поняття
«безпека» соціальної системи*

Відчуття безпеки – це суб’єктивне сприйняття загроз власному існуванню. Відтак людина має можливість коригувати свою поведінку, тобто виявляти певний інтерес, який стимулює та спрямовує її діяльність щодо задоволення цієї потреби. Отже, необхідно розуміти, що потреба у безпеці є однаковою для усіх людей, а інтерес може бути різним. Водночас необхідно зазначити, що відчуття безпеки може створювати ілюзію і не відображати дійсного стану речей. Трапляються випадки, коли на ті чи інші загрози не зважають, або навпаки сприймають у загостреній формі. З цього приводу римський імператор Марк Аврелій (121–180) дав просту раду: «Зміни своє ставлення

до речей, які тебе турбують». Вона є актуальною і сьогодні у стосунках між людьми та при сприйнятті ними тих чи інших подій. Тому потреба у безпеці виявляється через конкретний інтерес, який є основним мотивом у поведінці людей щодо реалізації цього інтересу, а відтак і реалізації цієї потреби.

У зв'язку з цим людина є беззахисною і найнебезпечнішою істотою на Землі у результатах власної діяльності і для себе, і для навколишнього середовища.

Безпека як стан соціальної системи. Стан системи відображає, з одного боку, остаточні результати виконання функції безпеки, з іншого, – мету організації. Тобто безпека – це мета системи, до якої вона прагне, і її стан, який залежить від ефективності результатів її діяльності. Це результат цілеспрямованої людської діяльності щодо переведення системи з одного рівня безпеки на інший, що відрізняється здатністю до самозбереження та створення умов для розвитку. Найбільш загальними критеріями стану безпеки соціальних систем є «їх цілісність та розвиток».

Стан безпеки системи можна визначити через відповідні критерії та показники (індикатори). Вони сигналізують, з одного боку, про зону безпеки, а з іншого – про розвиток небезпеки внаслідок реалізації загрози. Безпечний стан системи є тоді, коли основні її критерії знаходяться в межах граничних значень, тобто ще зберігаються можливості для розвитку.

Безпека як специфічна діяльність, процес та функція системи. Для захисту особистості, суспільства, держави чи підприємства від різних загроз у системі відповідного рівня має бути така функція. Ще Т. Гоббс (1588–1679) висловив таку думку: «Безпека народу – функція держави». Безпека як функція, діяльність розкривається науковцями через виявлення, попередження, послаблення, усунення і запобігання небезпеці та загрозам, здатним завдати значних збитків, закрити шлях для прогресивного розвитку [43], чи здатність системи протистояти загрозі виникнення втрат [29]. Водночас слід пам'ятати, що це має бути цілеспрямований постійний процес, спрямований на підтримку достатніх параметрів життєдіяльності системи.

Безпека як філософія сучасного менеджменту (управління), цінність та складова корпоративної культури. Сутність такого сприйняття безпеки зводиться до того, щоб навчитися управляти соціально-економічними системами через призму безпеки, розуміти її як функцію буття та життєдіяльності людини і її первинної потреби [32]. За такого підходу безпека реалізується в індивідуальній і суспільній свідомості у формі духовної цінності, у зв'язку з чим має універсальний характер і визнання. Сьогодні є світова тенденція щодо сприйняття безпеки як ціннісних норм корпоративної культури, особливо цей процес заохочується у провідних корпораціях світу. Для них характерні такі цінності: безпека, здоров'я співробітників, високі етичні вимоги до ведення бізнесу, увага до працівника як людини і головної цінності компанії та суспільства. Для українських підприємств сприйняття безпеки як ціннісних норм корпоративної культури є складним процесом, який потребує злагодженої роботи державних інституцій і менеджменту організацій.

Безпека як наука і мистецтво. Потреба людей, особливо керівників, у знаннях щодо протидії загрозам, забезпечення цілісності процесів, що проходять в організації, збереження підприємства як структури і власного бізнесу, створення умов для його розвитку сьогодні є надзвичайно актуальною. Як реакція на цю потребу виникла і розвивається спеціальна галузь наукових знань – сек'юрітологія (від грецьк. – «вчення» та англ. – «безпека»), в Україні – безпекознавство. Розвиток безпеки як науки сприяє формуванню у фахівців і менеджерів сучасних знань та вмінь з безпекознавства. Крім того, дає можливість перекоонатися, що реалізувати ці знання і вміння в реальній виробничій практиці вдається не кожному, оскільки потребує ще й певних природних здібностей відчувати, передбачати ті чи інші загрози, сприймати безпеку як ціннісну норму корпоративної культури. А це вже є питанням мистецтва. Отже, безпека – це наука, яку потрібно вивчати і розвивати, це мистецтво, яке потрібно опановувати, це корпоративна культура, котру потрібно виховувати, від власника і до рядового працівника.

Безпека як властивість системи. Існування будь-якої системи передбачає її захищеність від руйнівних впливів. Своїй руйнації протидіють всі системи [34]. Для цього система має таку властивість, тобто наявність внутрішньо вмонтованих структурних елементів, завдяки яким здатна протидіяти загрозам, що погіршують її стан, порушують встановлений порядок функціонування та цілісність. В біологічних системах це імунні властивості організму, а в соціальних – це стійкість та самодостатність системи.

Самодостатність як поняття є багатовимірним, воно має не тільки безпековий, а й економічний, соціальний, психологічний, політичний та інші аспекти та є дуже чутливим до людського чинника. Особливо, психологічно-політичний вимір поняття «самодостатність» є певною мірою визначальним та для українців має й ще власну історію, що сягає глибини віків.

Довгі 750 років українці залежали від сусідніх держав – Польщі та Московії. Багато поколінь, їх щонайменше 30, з байдужістю жили в рабському становищі, служили іншим державам, націям, культурам, творили чужу історію, вважаючи її своєю [30, с. 4].

Подібна ситуація продовжувалася й в останні роки української незалежності. В таких умовах формування самодостатньої особистості, а відтак самодостатньої соціально-економічної системи України, а надто, коли є певні обмеження країни в тих чи інших ресурсах, існує політичний вплив влади іншої країни чи країн, завдання надскладне. У таких умовах залежність України від постачання ресурсів ззовні та політичних рішень влади, наприклад Росії, зростає. Що вищий рівень залежності, то нижчі показники самодостатності соціально-економічної системи країни, а відтак її рівень безпеки знижується. Для контролю над цим процесом використовуються певні індикатори безпеки.

Отже, **самодостатність соціальної системи** – це наявність у розпорядженні суб'єктів управління відповідних ресурсів та уникнення залежності від джерел їх походження, що може становити загрозу, а також їх використання на рівні, необхідному для збереження параметрів життєдіяльності системи (рис. 1.5).

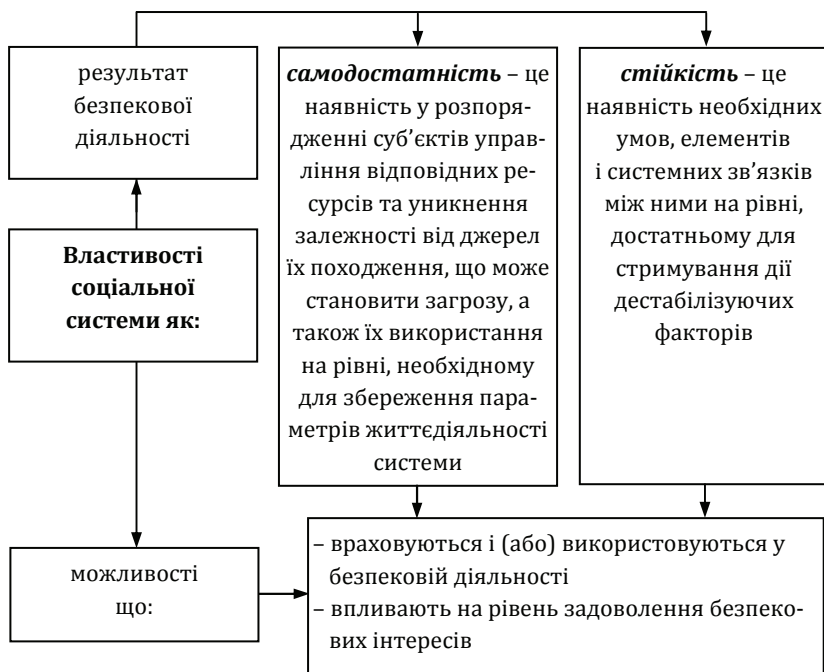


Рис. 1.5 Безпекові властивості соціальної системи

Стійкість соціально-економічної системи також є комплексним параметром, через який вона виявляє власні безпекові властивості, з одного боку, а з іншого, – відображає стан її безпеки, для чого також використовуються відповідні індикатори безпеки.

Стійкість економічної системи відображає міць і надійність її елементів, здатність витримувати внутрішні та зовнішні навантаження. Що стійкіша економічна система, то життєздатніша економіка, а відтак, і оцінка її безпеки буде вищою. Порушення пропорцій і зв'язків між різними компонентами системи призводить до її дестабілізації і є сигналом переходу економіки від безпечного стану до небезпечного [9].

Отже, **стійкість соціальної системи** – це наявність необхідних умов, елементів та системних зв'язків між ними як мінімум на рівні, достатньому для стримування дії дестабілізуючих чинників (рис.1.5).

Відтак безпекові властивості соціальної системи – стійкість та самодостатність, – з одного боку, є результатом безпечної діяльності, а з іншого – вони перетворюються у певні можливості щодо збереження параметрів її функціонування та стримування руйнування (див. рис. 1.5).

1.3 Логіка зв'язків між структурними елементами поняття «безпека соціальної системи»

Для структури поняття «безпека» притаманні не тільки комплексність та багатoeлементність, а й чітка логіка зв'язків між цими елементами, знання та дотримання якої дає змогу на практиці вибудовувати ефективніші системи безпеки. Основний зміст логічних зв'язків між елементами подано на рисунку 1.6.

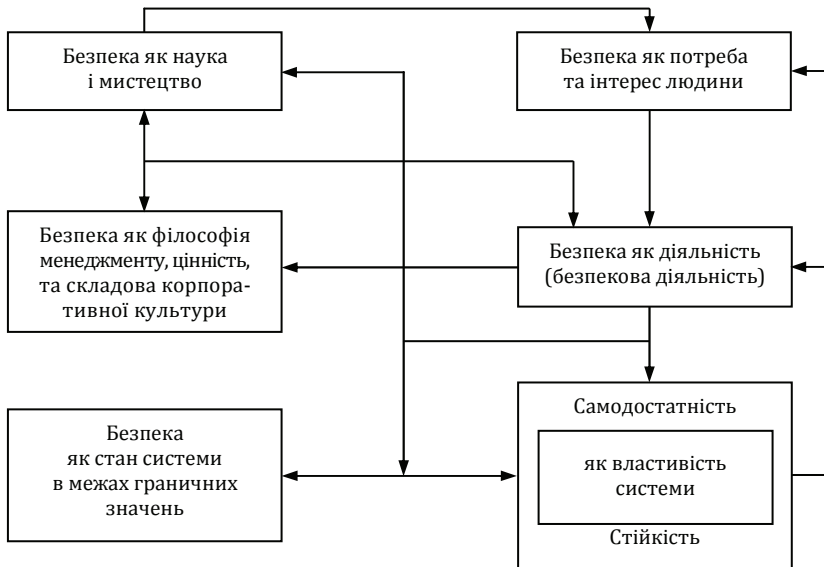


Рис. 1.6 Логічна схема зв'язків між структурними елементами поняття «безпека соціальної системи»

Потреба у безпеці є первинною потребою кожної людини і реалізується на індивідуальному, колективному і суспільному рівнях. Відчуття безпеки – це суб'єктивне сприйняття загроз власному існуванню. З огляду на це, людина має можливість коригувати свою поведінку, тобто виявляти певний інтерес, який стимулює та спрямовує її діяльність щодо задоволення цієї потреби.

Проте на формування безпекового інтересу мають вплив цінності, які є основними складовими безпекової культури. Саме від них залежить характер безпекової діяльності, спрямованої на протидію загрозам та забезпечення цілісності системи. Крім того, на якість та ефективність безпекової діяльності впливає філософія менеджменту, яка зводиться до того, щоб навчитися управляти соціально-економічними системами через призму безпеки. У зв'язку з цим в Україні виникла і розвивається спеціальна галузь наукових знань – безпекознавство. Однак реалізувати ці знання і вміння в реальній виробничій практиці вдасться не кожному, оскільки це потребує ще й певних природних здібностей відчувати, передбачати ті чи інші загрози, сприймати безпеку як ціннісну норму організаційної культури.

За такого підходу через безпекову діяльність у соціально-економічній системі формуються певні безпекові властивості, тобто внутрішні структурні елементи, а саме самодостатність та стійкість. Їхні показники характеризують стан соціальної системи насамперед з погляду її безпеки. Вони сигналізують, з одного боку, про зону безпеки, а з іншого, – про розвиток небезпеки внаслідок реалізації загрози. Крім того, від них певною мірою залежить рівень безпеки соціальної системи, чи окремих її підсистем, а також результативність безпекової діяльності та рівень реалізації безпекових потреб, інтересів суб'єктів безпеки та інших учасників соціально-економічних відносин.

З погляду системного підходу всі ці поняття взаємопов'язані становлять єдине ціле та розкривають сутність поняття «безпека» як потребу системи у безпечності функціонування, стан системи, її властивість, безпекову діяльність її структурних елементів та спосіб управлінського мислення й складову організаційної культури, а також науку і мистецтво одночасно.

Питання та завдання для самоконтролю

1. Розкрийте етимологію поняття «безпека соціальної системи».
2. Що таке біосоціальна дуалістична природа категорії «безпека» та через які складові вона виявляється.
3. Дайте загальну характеристику структури поняття «безпека соціальної системи».
4. Поясніть, чому безпека – це потреба та інтерес соціальної системи.
5. Обґрунтуйте, чому безпека розглядається вченими як стан соціальної системи.
6. Охарактеризуйте безпеку як специфічну діяльність та функцію соціальної системи.
7. Чому безпеку слід розглядати як філософію сучасного менеджменту (управління), цінність та складову корпоративної культури.
8. Поясніть, чому сьогодні безпека сприймається як наука і мистецтво.
9. Обґрунтуйте, чому безпека є властивістю соціальної системи та через які елементи вона проявляється.
10. Розкрийте логічний зв'язок між структурними елементами поняття «безпека соціальної системи».

Тести

1. Категорія «безпека» має біосоціальну дуалістичну природу: ..., які взаємопов'язані та виявляють себе як єдине ціле.
 - а) психологічну і фізичну;
 - б) фізичну і соціальну;
 - в) технологічну і психологічну;
 - г) соціальну і технологічну.
2. Захист від загроз, здатних завдати шкоди здоров'ю та майну людини – це складова категорії «безпека»:
 - а) фізична;
 - б) психологічна;

- в) технологічна;
- г) соціальна.

3. Захист життєво важливих інтересів особи, організацій від загроз – це складова категорії «безпека»:

- а) технологічна;
- б) соціальна;
- в) фізична;
- г) психологічна.

4. Безпека соціальної системи завжди:

- а) відносна і має динамічний характер;
- б) абсолютна і має статичний характер;
- в) відносна і має статичний характер;
- г) абсолютна і має динамічний характер.

5. Безпека як багатоманітне та комплексне явище, маючи дуалістичну природу, виявляється через:

- а) стан системи, який має перебувати у допустимих межах;
- б) стан системи, який має перебувати у допустимих межах та безпекову діяльність;
- в) безпекову діяльність;
- г) немає відповіді правильної.

6. Безпекова діяльність має ґрунтуватися на:

- а) потребі соціальної системи у безпечному функціонуванні;
- б) безпековій організаційній культурі;
- в) розумінні менеджерами усіх ланок того, що безпека – це ще й філософія сучасного менеджменту;
- г) усі відповіді правильні.

7. Наявність у розпорядженні суб'єктів управління відповідних ресурсів та уникнення залежності від джерел їх походження, що може становити загрозу, а також їх використання на рівні, необхідному для збереження параметрів життєдіяльності системи, – це:

- а) розширене відтворення системи;
- б) стійкість системи;

- в) самодостатність системи;
- г) незалежність системи.

8. Наявність у соціальній системі необхідних умов, елементів та системних зв'язків між ними як мінімум на рівні, достатньому для стримування дії дестабілізуючих чинників – це:

- а) стійкість системи;
- б) розширене відтворення системи;
- в) самодостатність системи;
- г) незалежність системи.

9. Потреба у безпеці виникає тоді, коли існує:

- а) загроза;
- б) ризик;
- в) виклик;
- г) усі відповіді правильні.

10. Безпека як стан соціальної системи відображає:

- а) результати фінансової діяльності;
- б) остаточні результати виконання функції безпеки;
- в) мету організації: збереження цілісності та статусу організації;
- г) правильні відповіді б, в.

11. Безпека як властивість системи виявляється через внутрішньо вмонтовані структурні елементи, основними з яких є:

- а) стійкість та самодостатність системи;
- б) економічне розширене відтворення та економічна незалежність системи;
- в) самодостатність та економічне розширене відтворення системи;
- г) стійкість та економічна незалежність системи.

12. Інформацію про зону безпеки чи розвиток небезпеки соціальної системи можна отримати, користуючись:

- а) критеріями безпеки;
- б) показниками безпеки;
- в) індикаторами безпеки;
- г) параметрами безпеки.

13. Наявність у соціальній системі внутрішньо вмонтованих структурних елементів, завдяки яким вона здатна протидіяти загрозам, – це:

- а) завдання системи;
- б) властивість системи;
- в) ознака системи;
- г) функція системи.

14. Виявлення, попередження, послаблення та ліквідація загроз чи небезпеки це елементи поняття «безпека» яке розглядається як:

- а) властивість системи;
- б) функція, діяльність системи;
- в) філософія сучасного менеджменту;
- г) складова корпоративної культури.

15. Який з наведених структурних елементів поняття «безпека» не належить до її складу?

- а) безпека як потреба та інтерес;
- б) безпека як діяльність, процес, функція системи;
- в) безпека як елемент функції розвитку системи;
- г) безпека як властивість системи.

16. Яке з наведених визначень поняття «безпека» характеризує його як комплексне явище?

- а) це стан системи в межах граничних значень і здатність протидіяти загрозам чи небезпеці з метою захисту корпоративних інтересів і загалом розвитку та забезпечення цілісності процесів і системи;
- б) здатність системи протистояти загрозі виникнення втрат;
- в) стан захищеності життєво важливих економічних інтересів підприємства від внутрішніх і зовнішніх джерел небезпеки, який формується адміністрацією та персоналом шляхом реалізації системи заходів правового, організаційного й інженерно-технічного характеру;
- г) стан ефективного використання ресурсів і наявних ринкових можливостей, що дає змогу підприємству уникнути внутрішніх і зовнішніх загроз і забезпечує йому стійкий розвиток на ринку відповідно до обраної місії.

17. Які з наведених характеристик поняття «безпека» повною мірою відображають склад його структурних елементів?

а) потреба системи у безпечності функціонування, її стан у межах граничних значень, властивість, специфічна діяльність її структурних елементів та спосіб управлінського мислення і складова корпоративної культури, а також наука і мистецтво одночасно;

б) це інтерес системи у безпечності функціонування, її стан у межах граничних значень, властивість, специфічна діяльність її структурних елементів та філософія сучасного менеджменту і складова корпоративної культури, а також наука і мистецтво одночасно;

в) це потреба системи у життєдіяльності, її стан, властивість, специфічна діяльність її структурних елементів та філософія сучасного менеджменту і складова корпоративної культури, а також наука і мистецтво одночасно;

г) правильні відповіді а і б.

Тема 2

СОЦІАЛЬНА СИСТЕМА ЯК ОБ'ЄКТ БЕЗПЕКИ

*Соціальна система – це складний
соціальний організм, що подібний до біологічного.
Знання його структури, функцій та підсистем
дозволяє безпекознавцю, як і лікарю,
діяти комплексно, або точково
з урахуванням взаємозв'язків у системі*

2.1 Сутність та основні властивості соціальної системи

Соціальна система – це особливий клас матеріальних живих систем. Основним її елементом є людина, соціальні групи. Їх поєднання з ресурсами формує соціальну або ще називають соціально-економічну систему. Типовими прикладами таких систем є підприємства, організації, та інші суб'єкти господарювання, держава тощо [50, с. 31]. Визначень поняття соціально-економічна система у наукових джерелах є багато. У процесі вивчення навчальної дисципліни «Теорія безпеки соціальних систем» під соціальною системою будемо розуміти сукупність взаємодіючих елементів, що становлять цілісне утворення, яке має властивості, відмінні від властивостей складових елементів та забезпечує її життєдіяльність.

Основні властивості соціальної системи подані на рисунку 2.1.

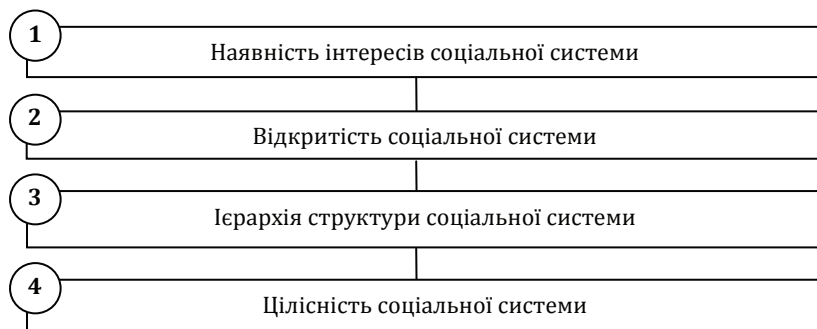


Рис. 2.1 Основні властивості соціальної системи

Наявність інтересів. Інтереси будь-якої системи, для первинної ланки господарювання – корпоративні інтереси, для держави – національні інтереси є основою їх життєдіяльності. Реалізація корпоративних інтересів забезпечує розвиток соціально-економічної системи. Відсутність їх реалізації, навпаки, може спричинити корпоративні конфлікти, які можуть набувати форми

загрози. До того ж успішна реалізація корпоративних інтересів, наприклад, у частині розширення частки на ринку, загострить конкурентну боротьбу з можливим використанням конкурентом недобросовісних методів. Крім того, корпорація, що розвивається, є привабливою для кримінального світу та корупціонерів. Успішному розвитку соціально-економічної системи можуть стати на заваді загрози надзвичайного характеру: природні лиха, теракти тощо. Відтак для реалізації корпоративних інтересів соціальній системі можуть виникати реальні загрози.

Відкритість. Для провадження своєї діяльності соціально-економічна система змушена налагоджувати контакти всередині і за її межами, вступаючи у конкурентну боротьбу в умовах визначального впливу тіньової економіки, корупції, недобросовісної конкуренції, що існує сьогодні в Україні. У зв'язку з цим у неї виникає багато дестабілізуючих чинників, що можуть негативно впливати на її функціонування та розвиток.

Ієрархія структури. Життєдіяльність соціальної системи потребує відповідної організаційної структури, особливо чіткої її ієрархії, тобто підпорядкування одних елементів іншим по вертикалі, встановлення субординаційних зв'язків, повноважень та відповідальності.

Цілісність. Соціальна система може забезпечити функціонування за умови наявності необхідних елементів, ресурсів та можливостей їх застосування як мінімум на достатньому рівні, тобто **самодостатності**, а також за наявності необхідних умов, гарантій та системних зв'язків між елементами як мінімум на достатньому рівні, тобто **стійкості**.

Отже, в основі розвитку соціально-економічної системи є корпоративні інтереси, для реалізації і задоволення яких здійснюється відповідна діяльність. На практиці доволі часто трапляється, коли реалізуючи власні інтереси, соціально-економічна система стає на заваді реалізації чи задоволення інтересів інших юридичних чи фізичних осіб, зокрема, що обумовлені у відповідних угодах чи законодавстві. З іншого боку, соціальна система піддається деструктивним впливам зовнішнього і внутрішнього середовищ, і стаючи в такий спосіб об'єктом

загроз, здійснення яких може викликати небезпеку, яка може спричинити до втрати самостійності та цілісності.

Діяльність соціальної системи, зокрема й безпекова здійснюється керуючою і керованою підсистемами. Їх взаємодія відображається схематично (рис. 2.2).

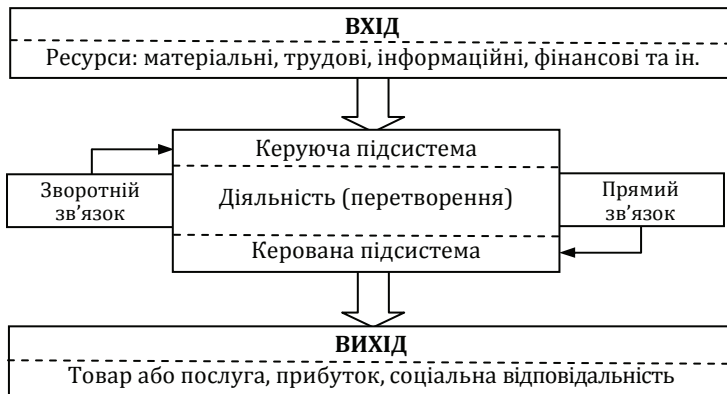


Рис. 2.2 Процес функціонування соціальної системи

Керуюча підсистема складається з апарату управління, до якого входять: на прикладі підприємства керівники і менеджери всіх рівнів, зокрема й начальник служби безпеки, засобів і технології управління, адміністративних приміщень, засобів комунікацій тощо. Тобто керуюча підсистема охоплює елементи, що забезпечують процес управління. Основне призначення керуючої підсистеми полягає у розробці способів впливу та їх трансформації в управлінські рішення. Вони, як правило, спрямовані на створення сприятливих умов для розвитку соціальної системи. Проте існують й випадки, коли ці рішення через різні причини, свідомо чи помилково створюють умови для виникнення загроз соціальній системі.

До складу **керованої підсистеми** входять виконавці, а також необхідні їм для здійснення виробничо-господарської діяльності технічні, організаційні та комунікаційні засоби, приміщення тощо. Тобто ті елементи, які забезпечують безпосередній процес виробничої (виробництво товарів, надання

послуг тощо), господарської, фінансової, комерційної, безпечної та інших видів діяльності. У цій підсистемі, окрім конкретних позитивних результатів роботи, також виникає низка загроз, наприклад, крадіжки, продаж секретів, викрадення провідних фахівців тощо.

Життєдіяльність соціальної системи має чітку структуру: **вхід, діяльність (процес перетворень), вихід**. На вході підприємство отримує відповідні ресурси, які використовуються у виробничому процесі, тобто обробляються і перетворюються у продукцію або послуги. За це отримує прибуток, що, своєю чергою, дозволяє йому забезпечувати працівників заробітною платою та іншими винагородами. Водночас, взаємодіючи із зовнішнім середовищем, організація повинна мати соціальну відповідальність перед ним. У кожному з цих елементів процесу функціонування підприємства можуть виникати загрози. Наприклад, на вході організація може отримати недоброякісні матеріали, чи спеціально засланих недобросовісним конкурентом працівників, у процесі виробництва можуть порушуватися технології, викрадатися секрети, кошти, а на виході можна отримати певну частину бракованої продукції, шкідливі викиди у атмосферу тощо.

2.2 Внутрішнє і зовнішнє середовище соціальної системи

Внутрішнє середовище соціальної системи визначається внутрішніми змінними, тобто ситуаційними чинниками, які взаємопов'язані, та зовнішнім середовищем. Тому сучасним соціальним системам доводиться адаптовуватися до змін у зовнішньому середовищі і відповідно здійснювати зміни в середині самої системи.

Наприклад, основними внутрішніми змінними будь-якої організації, на які може впливати менеджмент, є цілі, структура, завдання, технологія і працівники [27, с. 4].

Цілі – це конкретний очікуваний результат або кінцевий стан організації. Цілі визначаються у процесі планування у масштабах організації і на рівні різних підрозділів і служб. Процес розробки цілей є дієвим механізмом координації, бо він дає працівникам можливість усвідомити, на що вони повинні спрямувати свої дії.

Структура – це взаємовідносини рівнів управління і видів робіт (функціональних обов'язків), які виконують підрозділи організації або окремі працівники. Вона встановлює межі формальних стосунків між завданнями, видами діяльності в організації. Формування структури організації здійснюється шляхом горизонтального та вертикального поділу праці.

Завдання – це види робіт, які необхідно виконати певним способом та в обумовлений термін. Завдання визначаються не для працівника, а для посади, яку він займає. Відповідно до структури організації для кожної посади передбачено конкретні завдання (функціональні обов'язки), виконання яких розглядається як необхідний внесок у досягнення загальних цілей. Завдання, виконувані працівниками, діляться на три категорії: *робота з людьми, інформацією та фізичними матеріалами*.

Технологія – це поєднання відповідних знань, кваліфікаційних навиків, обладнання, інструменту та інфраструктури, необхідних для здійснення бажаних змін у матеріалах, інформації, людях.

Завдання і технологія взаємопов'язані. Виконання завдання включає використання конкретної технології.

Працівники – найважливіший ситуаційний чинник організації і водночас найскладніший – з урахуванням ефективності впливу на нього менеджера. Суть цієї складності полягає в тому, що люди дуже відрізняються один від одного здібностями, потребами, знаннями, поведінкою, ставленням до роботи, позицією, розумінням цінностей. Знання менеджером своїх працівників за такими характеристиками дає йому змогу ефективно впливати на них і сприяти реалізації їхнього потенціалу в досягненні цілей організації. Крім того, слід розуміти, що

поведінка людини змінюється залежно від ситуації. Дослідження психолога Уолтера Мішеля свідчать, що навіть такі основні характеристики особистості, як чесність і здатність викликати довіру, залежать від обставин.

Наведені внутрішні змінні чинники можуть позитивно і негативно впливати на життєдіяльність організації. Фахово встановленні цілі, визначенні згідно з ними завдання та розроблена відповідна організаційна структура, раціонально й ефективно задіяні працівники та використані відповідні технології створюють сприятливі в організації умови для її розвитку. У разі, коли на ці внутрішні змінні фактори менеджментом здійснюється управлінський вплив на низькому якісному рівні, то вони з чинників розвитку можуть перетворюватися у дестабілізуючі фактори, завдаючи тих чи інших збитків організації.

Зовнішні фактори, які впливають на діяльність організації, поділяють на:

1) **прямі дії** – ті, що безпосередньо впливають на діяльність організації (конкуренти, споживачі, законодавчі акти, державні органи, постачальники, профспілки);

2) **непрямі дії** – ті, що впливають не безпосередньо, а через певні механізми і відносини (науково-технічний прогрес, стан техніки та технології; стан економіки, соціально-культурні фактори, політичні фактори, міжнародні події).

Оцінюючи фактори зовнішнього середовища, необхідно враховувати такі основні їх характеристики:

- взаємозалежність всіх факторів зовнішнього середовища (зміна одного може призвести до зміни інших);

- складність зовнішнього середовища (значна кількість факторів, великий спектр значень їх величини);

- динамічність зовнішнього середовища (швидкість зміни оточення організації);

- невизначеність зовнішнього середовища (обмеженість інформації, її недостовірність).

Всі ці зовнішні фактори, аналогічно як і внутрішні, можуть сприяти розвитку соціальної системи, або навпаки завдати їй збитків, тобто бути для неї загрозами.

2.3 Корінні функції життєдіяльності соціальної системи

Для забезпечення цілісності, самозбереження та розвитку соціально-економічна система виконує корінні та видові функції [51].

Корінні функції – це взаємопов’язані функції процесу життєдіяльності соціальної системи, які безпосередньо визначають у цьому процесі напрями діяльності, якісні та кількісні перетворення, його стабільність та довговічність. Такими функціями (рис. 2.3) є:

- а) функція розвитку;
- б) функція безпеки;
- в) функція управління.

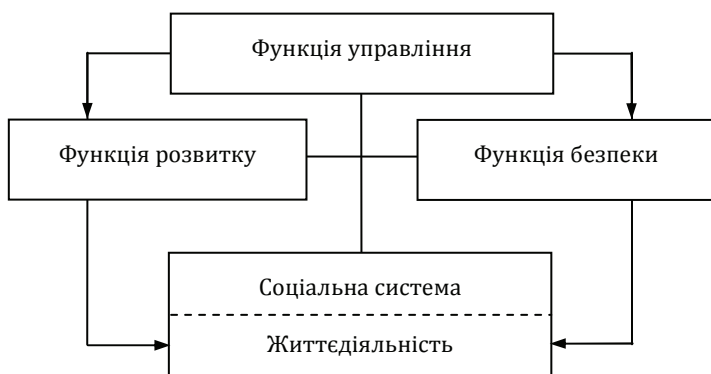


Рис. 2.3 Корінні функції соціальної системи

Видові функції – це будь-які види діяльності, які містять відповідні механізми через які реалізуються корінні функції соціальної системи.

Функція безпеки і функція розвитку становлять два боки одного процесу, процесу життєдіяльності соціально-економічної системи. Проте це різні функції мають власні методи і засоби забезпечення життєдіяльності організації.

Функція розвитку – це конкретні дії, пов’язані з реалізацією інтересів і спрямовані на незворотні та закономірні зміни

конкретних матеріальних об'єктів, що призводять до виникнення їх якісно нових станів або принципово нових об'єктів як цілісних систем [33, с. 43], або ж до забезпечення їх стабільного достатньо кількісного чи якісного станів.

Функція розвитку виявляється через видові функції соціальної системи: операційної, фінансово-ресурсної, трудоресурсної, маркетингової, інноваційної та ін. Залежності між операційною і іншими функціями організації можуть призводити до виникнення конфліктів.

Розвиток органічно потребує кількісних і якісних перетворень у тих чи інших сферах діяльності організації. Наприклад, у сфері виробництва – збільшення кількості товарів та підвищення їх якості; у фінансовій – збільшення прибутку чи забезпечення його стабільності на встановленому рівні, доходності на акцію; у роботі з персоналом – підвищення кваліфікації, професійності та надійності персоналу; в маркетинговій сфері – удосконалення споживчих властивостей товару чи розробка нового, формування більшого попиту на товар тощо.

В основі розвитку соціально-економічної системи є відповідні корпоративні інтереси, які реалізуються за кожною видовою функцією. Рівень їх реалізації є одночасно показником рівня розвитку. Для цього використовують якісні і кількісні показники розвитку, характерною ознакою яких є тенденція до збільшення.

Функція безпеки – це конкретні дії, які необхідно виконати, щоб захистити функцію розвитку соціальної системи від потенційних чи реальних внутрішніх і зовнішніх загроз [33, с. 48], створити в такий спосіб необхідні умови для її реалізації.

Функція безпеки організації реалізується на двох рівнях:

1) суб'єкта господарювання – через виконання видових функцій: детективної діяльності, аналітично-пошукової діяльності, технічного захисту інформації, охоронної діяльності, юридичного захисту, страхування, охорони праці тощо;

2) держави – шляхом використання механізмів видових функцій: державного регулювання економічних відносин, опе-

ративно-розшукової діяльності, сертифікації, стандартизації, квотування, судового захисту та ін.

Ці функції організація може реалізовувати власними силами або за допомогою інших структур з безпеки, які можуть залучатися на умовах договору.

Функція управління – це конкретні дії, які необхідно виконати, щоб інтегрувати в єдиний процес функції розвитку, безпеки і забезпечуючи на цій основі життєдіяльність організації.

Основне призначення функції управління полягає у координації зусиль людей та створенні всіх необхідних умов для реалізації функцій розвитку і безпеки. Управління як функція (діяльність) організації реалізується через видові функції: планування, організування, мотивування, контролювання.

Між *функцією розвитку* та *функцією безпеки* існує природний зв'язок, який характеризується як єдиний процес з суперпозицією (накладанням) цих функцій. Проте їх вплив здійснюється властивими для них методами та засобами [50, с. 58].

Змістовно взаємодія функції безпеки з функцією розвитку здійснюється через їх видові функції та через функцію управління. Видові функції безпеки реалізуються в усіх видових функціях розвитку соціально-економічної системи: *виробництві, фінансовій, кадровій, маркетинговій, інноваційній та ін.*, а також окремо, протидіючи внутрішнім і зовнішнім загрозам, використовуючи управлінські видові функції та їх інтегруючі технології. Тобто, функція безпеки пронизує через функцію управління всі видові функції розвитку, їх складові, що в підсумку забезпечує реалізацію корпоративних інтересів, цілісність процесів і об'єктів соціально-економічної системи та її розвиток.

Крім того, функція безпеки як світоглядна і безпекознавча філософія відображається на управлінських процесах та управлінських рішеннях через суб'єкти управління (керівників і менеджерів). Її філософський вплив виявляється у здатності менеджменту соціально-економічної системи через управлінсько-безпекове мислення, культуру безпеки під час ухвалення управлінських рішень та виконання управлінських функцій не створювати загроз. Виключно в управлінні є механізми, що вико-

нують інтегруючу і координуючу роль у вирішенні завдань з безпеки.

Питання та завдання для самоконтролю знань

1. Розкрийте сутність та основні властивості соціальної системи на прикладі конкретної організації.

2. Охарактеризуйте керуючу та керовану підсистеми організації та їх вплив на безпеку.

3. Розкрийте зміст процесу функціонування соціальної системи та його вплив на безпеку.

4. Вкажіть основні фактори внутрішнього середовища соціальної системи та охарактеризуйте їх вплив на безпеку.

5. Поясніть, які фактори зовнішнього середовища соціальної системи та як саме впливають на стан її безпеки.

6. Що таке корінні функції соціальної системи та яка їх роль і взаємозв'язок у забезпеченні її життєдіяльності?

7. Розкрийте сутність і роль функції розвитку у забезпеченні життєдіяльності соціальної системи.

8. Розкрийте сутність і роль функції безпеки у забезпеченні життєдіяльності соціальної системи.

9. Розкрийте сутність і роль функції управління у забезпеченні життєдіяльності соціальної системи.

Тести

1. Соціальна система – це:

а) сукупність елементів, що становлять цілісне утворення та забезпечують життєдіяльність соціально-економічної системи;

б) сукупність взаємопов'язаних через відповідні механізми елементів, що становлять цілісне утворення, яке має властивості, відмінні від властивостей складових елементів та які забезпечують життєдіяльність соціально-економічної системи;

в) сукупність елементів, що становлять цілісне утворення та механізм забезпечення життєдіяльності соціально-економічної системи;

г) правильні відповіді а, в.

2. Які з наведених елементів соціальної системи не належать до основних?

- а) наявність корпоративних інтересів;
- б) наявність фінансових ресурсів;
- в) ієрархія структури;
- г) взаємодія із зовнішнім середовищем.

3. За яких умов цілі соціальної системи можуть негативно впливати на її безпеку?

- а) коли вони офіційно не встановлені;
- б) коли сформульовані дуже загально;
- в) коли вони є вимірювальними;
- г) правильні відповіді а, б.

4. За яких умов завдання соціальної системи можуть негативно впливати на її безпеку?

- а) коли вони офіційно не передбаченні у посадових інструкціях, функціональних обов'язках працівників та положеннях про структурний підрозділ;
- б) коли не передбачені у планах роботи організації та її структурних підрозділів;
- в) коли немає управлінського контролю за їх виконання;
- г) усі відповіді правильні.

5. За яких умов структура соціальної системи може негативно впливати на її безпеку?

- а) коли вона є дуже громіздкою та багаторівневою;
- б) коли вона є простою та малорівневою;
- в) коли сформована з урахуванням ситуації, що складається на ринку та у середині організації;
- г) коли є гнучкою.

6. За яких умов працівники соціальної системи можуть негативно впливати на її безпеку?

- а) коли недостатній рівень кваліфікації;
- б) коли контроль за якістю роботи персоналу потребує певного покращення;
- в) коли відсутня мотивація до праці;
- г) вірні відповіді а, в.

7. За яких умов технології, що використовуються соціальною системою у діяльності, можуть негативно впливати на її безпеку?

а) коли є поєднання відповідних знань, обладнання, інструменту та інфраструктури, необхідних для здійснення бажаних змін у матеріалах, інформації, людях;

б) коли є поєднання відповідних знань та кваліфікаційних навиків, необхідних для здійснення бажаних змін у матеріалах, інформації, людях;

в) коли немає поєднання відповідних знань, обладнання, інструменту та інфраструктури, необхідних для здійснення бажаних змін у матеріалах, інформації, людях;

г) усі відповіді правильні.

8. Які з наведених факторів прямої дії можуть негативно впливати на безпеку соціальної системи?

а) стан економіки;

б) конкуренти;

в) стан техніки та технології;

г) науково-технічний прогрес.

9. Взаємопов'язані функції життєдіяльності організації, які безпосередньо визначають у цьому процесі якісні і кількісні перетворення, його стабільність та довговічність – це:

а) виробничі функції;

б) управлінські функції;

в) корінні функції;

г) видові функції.

10. Конкретні дії, пов'язані з реалізацією інтересів і спрямовані на незворотні та закономірні зміни конкретних матеріальних об'єктів, що призводять до виникнення їх якісно нових станів або принципово нових об'єктів як цілісних систем або до забезпечення їх стабільного достатньо кількісного чи якісного станів це:

а) функція розвитку;

б) функція зростання;

в) функція управління;

г) функція стабілізації.

11. Конкретні дії, які необхідно виконати, щоб захистити функцію розвитку соціальної системи від потенційних чи реальних внутрішніх і зовнішніх загроз, створити в такий спосіб необхідні умови для її реалізації, – це:

- а) функція розвитку;
- б) функція зростання;
- в) функція управління;
- г) функція безпеки.

12. Конкретні дії, які необхідно виконати, щоб інтегрувати в єдиний процес функції розвитку і безпеки, забезпечуючи на цій основі життєдіяльність організації, – це:

- а) функція стабілізації;
- б) функція зростання;
- в) функція управління;
- г) функція безпеки.

13. Які з наведених ознак не є властивими для соціально-економічних систем?

- а) динамічність та гнучкість у діяльності;
- б) наявність корпоративних економічних інтересів.
- в) наявність внутрішніх і зовнішніх загроз;
- г) реалізація корінних і видових функцій.

14. Начальник служби безпеки організації входить до складу:

- а) виробничої групи в організації;
- б) цільової групи в організації;
- в) комітету в організації;
- г) командної групи в організації.

Тема 3

КОРПОРАТИВНА КУЛЬТУРА ТА ЇЇ ВПЛИВ НА БЕЗПЕКУ ОРГАНІЗАЦІЇ

*Керівник, який сповідує безпекові цінності
та сформував безпекову корпоративну культуру –
заклав оберіг збереження цілісності соціальної системи*

3.1 Сутність понять «корпоративна культура» та «безпекова корпоративна культура»

Корпоративна культура (у наукових джерелах також використовується термін організаційна культура) притаманна будь-якій організації незалежно від того, якою діяльністю вона займається, якими є її розміри, потенціал.

Культура організації характеризує поведінку її членів, методи вирішення проблем, ставлення до зовнішнього впливу, швидкість і спосіб реагування на обставини, що змінюються, підходи до вирішення конфліктних ситуацій.

Основним елементом корпоративної культури є цінності, тобто те, що керує поведінкою людей, визначаючи, що правильно, а що неправильно, що добре, і що погано. Умовою прийняття цінностей є практична участь працівника в її реалізації. Виявляються цінності у формі певного способу мислення та правил і норм поведінки.

Корпоративна культура – це система цінностей, які сформовані та підтримуються членами колективу, виявляються у формі певного способу мислення та правил і норм поведінки, що дає змогу зберігати цілісність організації.

Корпоративна культура змінюється дуже повільно, але керівник, маючи владу, може на неї впливати. Нерозуміння керівником сутності культури і того, що їй властива повільна динаміка, може призвести до виникнення проблем. Дуже часто керівник, діагностуючи їх, як проблеми з окремими людьми, поведінка і реакції яких не відповідають його очікуванням. Однак насправді він має справу з культурою організації. Спроба різкої зміни культури викликає у людей відчуття, що ламається організація, яка до цього, на їхню думку, ефективно функціонувала.

Основне призначення корпоративної культури полягає у зміцненні внутрішньої цілісності організації, формуючи для цього корпоративні цінності і норми. Поняття цілісності організації як

системи є основною метою і результатом функції безпеки. Це пояснюється тим, що безпека є первинною потребою людини, внаслідок чого виникає необхідність у її задоволенні. У цьому процесі визначальну роль виконує безпекова культура, котра має формуватися як складова корпоративної культури.

Безпекова корпоративна культура – це складова корпоративної культури, яка виявляється у формі безпекового мислення як цінності та безпекової поведінки як норми у відносинах для збереження цілісності організації.

Безпекове мислення як корпоративна цінність – це спосіб мислення працівників, менеджерів та власника (засновника) організації, який сприймається у колективі та не спонукає до збурення, нанесення її матеріальних чи моральних збитків, а навпаки до створення сприятливих умов для розвитку.

Безпекова поведінка як норма у відносинах – це відносини, що сформувалися та підтримуються у середині організації та відносини організації до зовнішнього середовища, у яких немає ознак діяльності, спрямованої на збурення, нанесення її матеріальних чи моральних збитків, порушення цілісності.

Основний зміст та структуру безпекової корпоративної культури подано на рисунку 3.1.

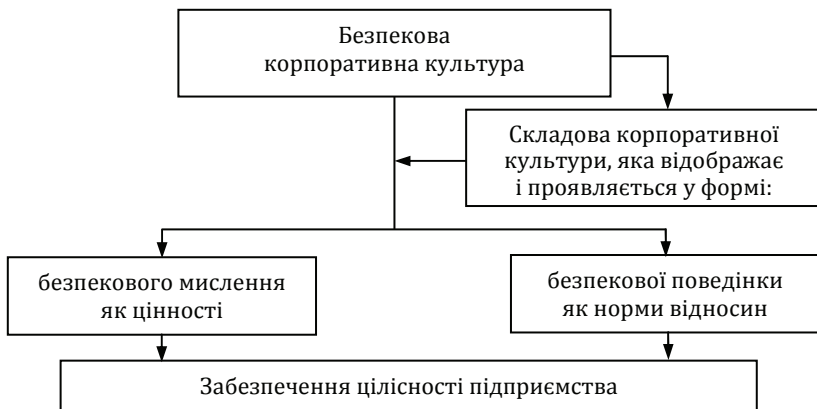


Рис. 3.1 Структурна схема змісту безпекової корпоративної культури

Основним джерелом корпоративної культури є засновники і вищий менеджмент підприємства. Саме від їх безпекових цінностей, поведінкових норм, знань з питань теорії і практики безпеки й управління залежить філософія і політика безпеки підприємства. Відтак є два варіанти розвитку ситуації:

1. У разі, коли безпекова корпоративна культура певною мірою вже сформована, то, як правило, на підприємстві впроваджена дієва система безпеки, у межах якої реалізується необхідна безпекова діяльність, що має комплексний характер.

2. У разі, коли безпекова корпоративна культура сформована незначною мірою або практично не сформована, то організація безпеки на підприємстві, зводиться до охорони на прохідні підприємства. Наслідки такого підходу відомі: від збитків аж до рейдерського захоплення підприємства.

Безпекову корпоративну культуру в організації потрібно формувати та удосконалювати. Це складний процес і залежить, як вже наголошувалося, від вищого менеджменту та власників підприємства, від рівня сформованості їх особистої безпекової культури. Цей процес потрібно розпочинати у вищих навчальних закладах та постійно продовжувати під час трудової діяльності.

3.2 Безпекова підготовка фахівців у закладах вищої освіти

Перспективи розвитку мають ті організації, які значною мірою сформуvalи безпекову корпоративну культуру. Для цього насамперед потрібні кваліфіковані фахівці з креативним мисленням, які добре розуміють процеси, що відбуваються в сучасній економіці, зокрема на рівні організації, а також знають як організувати його безпеку і на практиці здатні це зробити.

В умовах сьогодення безпека підприємств полягає насамперед в площині фінансово-економічних відносин та інтересів, вимагаючи від фахівців певних знань з економіки, фінансів, права [55]. Одночасно потрібні знання з аналітично-пошукової та дете-

ктивної діяльності, організації технічного захисту інформації та охорони праці, теорії безпеки та ін. Тобто, фахівець з безпеки організації повинен мати спеціальну освіту, яка б охоплювала інтегративні знання: фінансові, економічні, юридичні, управлінські, безпекознавчі, психологічні тощо або безпекову підготовку.

Для ефективної безпекової підготовки майбутніх фахівців у закладах вищої освіти (ЗВО) України необхідно дотримуватися концептуальної моделі, яка схематично відображена на рис. 3.2.

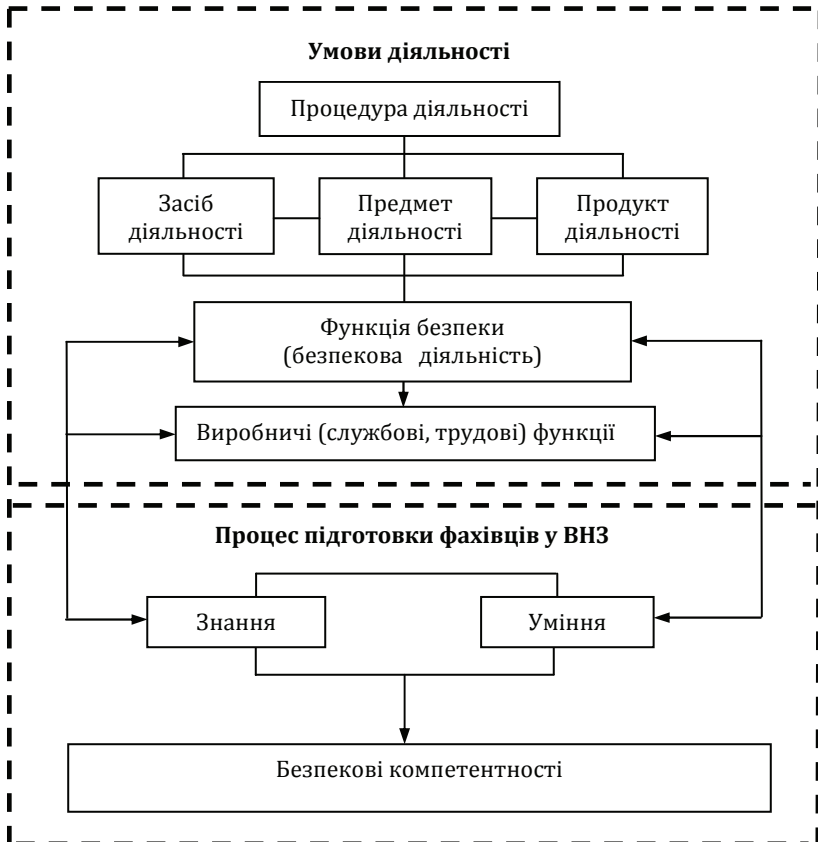


Рис. 3.2 Концептуальна модель безпекової підготовки фахівців у ЗВО України

Відповідно до Класифікатора професій в Україні є багато професій, які потребують безпекової підготовки. Особливо це професії менеджера та професіонала з безпеки. За своїм змістом і характером вони складні, багатофункціональні і надзвичайно відповідальні, у зв'язку з чим вимагають різносторонньої, комплексної, спеціальної і водночас інтегрованої підготовки. Діяльність менеджера та професіонала з безпеки спрямована на роботу з внутрішнім і зовнішнім середовищами.

Робота із внутрішнім середовищем зводиться до вивчення кандидатів на роботу, спостереження за працівниками, організацію охорони товарно-матеріальних цінностей, забезпечення режиму корпорації, контролю за рухом товарно-матеріальних цінностей, протидію технічному шпionажу та захисту комерційної таємниці тощо.

Робота з зовнішнім середовищем передбачає: вивчення конкурентів, партнерів, протидію кримінальним структурам, співпрацю і взаємодію з правоохоронними органами тощо.

Загалом діяльність менеджера та професіонала з безпеки характеризується: динамікою, активним пересуванням, постійною зміною соціально-психологічної атмосфери, дефіцитом часу, певним ризиком, емоційним і вольовим напруженням. Середовище, в якому доводиться їм працювати, є мінливим і складним для оцінки та ухвалення рішень. Залежно від ситуації і завдання, яке виконується, потрібно бути психологом, педагогом, аналітиком, «оперативником», охоронцем тощо. Водночас для діяльності менеджера з безпеки характерним є конспірація, гра ролей різних соціальних і професійних типів та ін.

Під час складання навчальних планів та програм необхідно враховувати окреслені особливості безпекової діяльності, що дають змогу сформувати безпековий спосіб мислення та безпекові цінності у студентів та майбутніх фахівців.

У розвинутих країнах світу, насамперед країнах, які входять до європейської спільноти, підготовка фахівців з безпеки підприємств здійснюється за спеціальністю «сек'юриті менеджмент» (менеджмент безпеки). Такі фахівці мають різні спеціалізації: від приватного детектива до фахівця з конкурентної роз-

відки, від менеджера з забезпечення безпеки персоналу до менеджера з забезпечення технічної безпеки за освітньо-кваліфікаційними рівнями «бакалавр», «магістр».

У сучасних умовах організація і безпосереднє забезпечення безпеки підприємств потребують відповідного якісного наукового супроводження шляхом підготовки наукових кадрів, тобто фахівців вищої кваліфікації докторів філософії і докторів наук.

3.3 Підвищення кваліфікації, курсова підготовка менеджерів з питань безпеки

Крім підготовки фахівців з безпеки у вищих навчальних закладах, потрібна відповідна підготовка з безпеки бізнесу керівників і менеджерів усіх рівнів підприємницьких структур у процесі роботи. Традиційно такою формою професійної підготовки є підвищення кваліфікації у формі тренінгів, семінарів, науково-практичних конференцій. Найефективнішими з цих форм є тренінги та семінари. Сьогодні такі навчання, як правило, проводяться з ініціативи окремих приватних осіб або навчальних закладів, які спеціалізуються у сфері безпеки підприємництва.

Для забезпечення системності та наступності у програмах, які пропонуються на таких тренінгах чи семінарах, потрібно внести низку рекомендацій:

1. Організовувати тренінги і семінари з безпеки треба на двох рівнях:

а) на рівні громадських структур у сфері підприємництва, які виконують координуючу роль (Український союз промисловців і підприємців, Асоціація приватних структур з безпеки та ін.);

б) на рівні підприємства.

2. До складання програм необхідно запрошувати фахівців, які спеціалізуються на організації й проведенні навчань з безпеки.

3. Під час складання програм з навчання слід виходити з проблемних питань, які є, або можуть бути у сфері безпеки, передбачивши для їх усунення відповідні теми.

4. Для проведення тренінгів і семінарів з безпеки слід запрошувати провідних фахівців з питань, що передбачені у програмі навчання зі знанням теорії та практики.

5. Після завершення навчання учасникам тренінгу чи семінару обов'язково слід вручати відповідні сертифікати.

6. Працівник, який пройшов навчання за програмою з безпеки, обов'язково заохочується на роботі матеріально й морально. Сертифікат розміщуються на видному місці, де працює співробітник.

7. Створювати в організації сприятливі умови для керівників, менеджерів та фахівців з безпеки щодо їх участі в тренінгах, семінарах та науково-практичних конференціях з питань безпеки, що проводяться поза межами підприємства та їх об'єднань.

Для великих і середніх організацій, де створені служби безпеки, актуальним є питання щодо фаховості її керівника. Адже саме від цієї структури та її керівника залежить дієвість системи безпеки організації загалом, рівень координації зусиль відповідних підрозділів та фахівців, особливо під час ліквідації тих чи інших загроз. Відтак керівникам служб безпеки організації необхідно пройти навчання на відповідних курсах.

Питання та завдання для самоконтролю

1. Розкрийте сутність понять «корпоративна культура», «безпекова корпоративна культура» та їх значення для безпеки організації.

2. Що таке «безпекове мислення» та яка його роль у формуванні й удосконаленні безпекової корпоративної культури.

3. Що таке «безпекова поведінка» та яка його роль у формуванні й удосконаленні безпекової корпоративної культури.

3. Поясніть, як безпекова підготовка студентів у ВНЗ може сприяти удосконаленню безпекової корпоративної культури організації.

4. Обґрунтуйте, чому удосконалення безпекової корпоративної культури організації потребує підвищення кваліфікації чи курсової підготовки менеджерів з питань безпеки.

5. Наведіть основні організаційно-методичні рекомендації щодо підготовки програм проведення тренінгів чи семінарів з безпеки для забезпечення їх системності та наступності.

Тести

1. Система цінностей, які сформовані і підтримуються членами колективу, виявляються у формі певного способу мислення та правил і норм поведінки, що дає змогу зберігати цілісність організації – це:

- а) корпоративна культура;
- б) корпоративні цінності;
- в) безпекова корпоративна культура;
- г) правильні відповіді в і б.

2. Складова корпоративної культури, яка виявляється у формі безпекового мислення як цінності та безпекової поведінки як норми у відносинах для збереження цілісності організації, – це:

- а) корпоративна культура;
- б) корпоративні цінності;
- в) безпекова корпоративна культура;
- г) правильні відповіді а і б.

3. Спосіб мислення працівників, менеджерів та власника (засновника) організації, який сприймається у колективі та не спонукає до збурення, завдання їй матеріальних чи моральних збитків, а навпаки до створення сприятливих умов для розвитку, – це:

- а) безпекова корпоративна культура;
- б) корпоративні цінності;
- в) безпекове мислення як корпоративна цінність;
- г) правильні відповіді а і б.

4. Відносини, що сформувалися та підтримуються в середині організації та відносини організації до зовнішнього середовища, у яких немає ознак діяльності, спрямованої на збурення, завдання їй матеріальних чи моральних збитків, порушення цілісності, – це:

- а) корпоративні цінності;
- б) безпекова поведінка як норма у відносинах;

- в) безпекова корпоративна культура;
- г) правильні відповіді а і в.

5. Що є основою корпоративної культури організації?

- а) поведінка засновника;
- б) норми внутрішніх документів;
- в) корпоративні цінності;
- г) внутрішні правила.

6. У якій формі виявляються корпоративні цінності працівників організації?

- а) у формі правил і норм поведінки;
- б) у формі правил поведінки;
- в) норм поведінки;
- г) усі відповіді правильні.

7. У якій формі виявляється безпекова корпоративна культура?

- а) у формі правил з безпеки в організації;
- б) у формі безпекового мислення як цінності;
- в) у формі безпекового мислення як цінності та безпекової поведінки як норми у відносинах;
- г) безпекової поведінки як норми у відносинах.

8. Хто є основним джерелом корпоративної, зокрема й безпекової, культури в організації?

- а) керівники середньої ланки в організації;
- б) працівники організації;
- в) вищий менеджмент організації;
- г) усі відповіді правильні.

9. Що є в основі корпоративної культури організації?

- а) поведінка засновника;
- б) норми внутрішніх документів;
- в) корпоративні цінності;
- г) внутрішні правила.

10. У якій формі виявляються корпоративні цінності працівників організації?

- а) правил і норм поведінки;

- б) правил поведінки;
- в) норм поведінки;
- г) усі відповіді правильні.

11. У якій формі виявляється безпекова корпоративна культура?

- а) правил з безпеки в організації;
- б) безпекового мислення як цінності;
- в) безпекового мислення як цінності та безпекової поведінки як норми у відносинах;
- г) безпекової поведінки як норми у відносинах.

12. Хто є основним джерелом корпоративної, зокрема й безпекової, культури в організації?

- а) керівники середньої ланки в організації;
- б) працівники організації;
- в) вищий менеджмент організації;
- г) усі відповіді правильні.

Тема 4

КОРПОРАТИВНІ ІНТЕРЕСИ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ СОЦІАЛЬНОЇ СИСТЕМИ

*Щоб захищати інтерес,
потрібно його знати і сприймати
як об'єкт захисту*

4.1 Сутність приватних, групових та пов'язаних інтересів, їх вплив на безпеку соціальної системи

У центрі соціально-економічних відносин є людина. В основі її поведінки та діяльності – певні потреби, зокрема й потреби у безпеці, які виявляються через конкретний інтерес. Відтак інтереси займають головне місце у життєдіяльності соціальних систем. Під інтересами розуміються усвідомлені потреби, що сформовані суспільством, колективом, соціальною групою, індивідом для забезпечення життєдіяльності. Саме через формування та реалізацію конкретних інтересів задовольняються потреби людей, а саме потреби у безпеці.

У діяльності організації беруть участь різні учасники соціально-економічних відносин, які мають певні інтереси, що виявляються у формі:

- а) приватного (особистого) інтересу;
- б) групового інтересу;
- в) пов'язаного інтересу.

Приватні (особисті) інтереси – це усвідомлені потреби людини, задоволення яких необхідне для її життєдіяльності.

Інтерес кожного учасника соціально-економічних відносин виступає як приватний (особистий) [51, с. 40–44]. Наявність особистих інтересів спонукає людей до діяльності, зокрема й у межах офіційних організацій. Основною рисою приватного інтересу є відособленість. Це зумовлює, з одного боку, суперечливість між носіями інтересів, а з іншого – пошук соціально-економічного партнерства, тобто усупільнення приватного інтересу. Така особливість пояснюється тим, що людина як носій приватного інтересу, працюючи в організації на посаді рядового працівника (фахівця та робітника), менеджера, чи є власником (засновником) організації, усвідомлює, що реалізація її інтересу залежить не тільки від неї особисто, а й від інших працівників. Тому й виникає потреба в певному консенсусі, узгодженості приватних інтересів.

Групові інтереси – це узгодженні приватні інтереси, реалізація яких необхідна для створення умов і механізмів для функціонування групи чи загалом колективу (організації).

У процесі трудової діяльності в соціальній системі формується трудовий колектив, створюються формальні й неформальні групи. Вони також формують так звані групові (колективні) інтереси.

Трудовий колектив створюється для встановлення офіційних відносин між працівниками й адміністрацією (вищим менеджментом й власником) організації, формування й захисту інтересів колективу.

Неформальні групи створюються, як правило, внаслідок неврахованого або нереалізованого приватного інтересу члена цієї групи та задля подальшої боротьби за його досягнення.

Формальні групи створюються керівниками соціальної системи для підвищення ефективності управління нею задля створення чи удосконалення умов і механізмів, необхідних для реалізації інтересів трудового колективу.

Водночас реалізація групових інтересів може сприяти розвитку організації, або навпаки дестабілізувати її діяльність.

Пов'язані інтереси – це інтереси суб'єктів, що мають з організацією відповідні соціально-економічні відносини, необхідні для забезпечення її життєдіяльності та офіційного функціонування.

Життєдіяльність соціальної системи забезпечують не тільки внутрішні суб'єкти соціально-економічних відносин (власники, менеджери, рядові працівники), а й зовнішні (постачальники, партнери, кредитори, споживачі, держава тощо). Вони також мають відповідні інтереси, співпрацюючи з організацією. Крім того, певні інтереси має та чи інша громада, де розміщена організація. Такі інтереси називають пов'язані інтереси, оскільки вони мають враховуватися у діяльності соціальної системи.

Зазначені форми вияву інтересу учасників соціально-економічних відносин мають різне спрямування. Наприклад, якщо акціонери зазвичай зацікавлені в розподілі отриманого

прибутку у формі дивідендів, то товариство як суб'єкт господарських відносин – у поповненні за рахунок прибутку своєї майнової бази (відповідних фондів) для розширення, модернізації виробництва, застосування новітніх техніки і технології. Зрозуміло, що реалізація цих інтересів повністю неможлива, оскільки за природою вони містять елементи конфлікту, що потребує певного консенсусу.

Отже, інтереси, з одного боку, є рушієм розвитку соціальної системи загалом і кожного її учасника зокрема, а з іншого – за своєю спрямованістю є суперечливими, що природно спричиняє конфлікт інтересів, який може набувати форми загроз.

4.2 Сутність корпоративних інтересів та їх значення для безпеки соціальної системи

У зв'язку із суперечливістю інтересів (приватних, групових, пов'язаних) учасників соціально-економічних відносин є необхідність в їх узгодженні і в такий спосіб формуванні інтересів організації, які б враховували основне із зазначених інтересів та необхідне для забезпечення її життєдіяльності. Інакше такі інтереси набувають форми і змісту корпоративних інтересів, які об'єднують усіх учасників, а не конфліктують.

Корпоративні інтереси – це сукупність об'єктивних потреб соціальної системи, які виявляються як узгоджені інтереси відповідних суб'єктів учасників корпоративних відносин, реалізація яких необхідна для її життєдіяльності.

Саме узгодженість інтересів сприяє відсутності або низькому (безпечному) рівню конфліктності і в такий спосіб є об'єднуючим механізмом в їх реалізації. З іншого боку, узгодженість інтересів створює основні передумови для стабільності функціонування та розвитку організації. Для узгодження інтересів можна використовувати різні механізми: відповідні норми Законів України, колективні договори, контракти тощо. Наприклад, для недопущення конфлікту інтересів, пов'язаних з

використанням прибутку, можна провести збори акціонерів і найманих працівників. У разі ухвалення узгодженого рішення щодо того, як використовувати отриманий прибуток, інтереси учасників соціально-економічних відносин набувають форми корпоративних інтересів, які будуть вказівником під час планування і загалом у процесі управлінської діяльності, а також об'єктом безпеки.

Розуміння корпоративних інтересів як узгоджених має принципове концептуальне значення для стабільності функціонування, розвитку і безпеки соціально-економічної системи. У зв'язку з чим саме корпоративні інтереси є об'єктом захисту (безпеки). Водночас, щоб захищати інтерес, потрібно його знати і сприймати як об'єкт захисту [33, с. 86].

Узгодженість чи досягнення консенсусу між носіями приватних, групових та пов'язаних інтересів варто сприймати як результат далекої від «справедливості» їх діяльності. Викремлення загального з приватних й групових інтересів, врахування пов'язаних інтересів здійснюється частково, шляхом формальних процедур, частково стихійно, частково вимушено, тобто не ідеально. Тобто точно сформулювати об'єктивний інтерес соціальної системи принципово неможливо: будь-яке формулювання суб'єктивне, оскільки втілює думку та цінності того, хто її висловлює. Повноваженнями щодо визначення корпоративних інтересів соціальної системи наділений вищий менеджмент (власник). Ця суперечність не може бути вирішена абсолютно, це постійний процес, де вона вирішується відносно, частково шляхом боротьби приватного й групового інтересів. Де інтереси не збігаються, там є суперечності, які, своєю чергою, можуть бути джерелом загрози соціальній системі.

Загалом корпоративні інтереси створюють умови для реалізації інтересів відповідних суб'єктів соціально-економічних відносин. Крім того, вони закладають основи механізмів:

- 1) розвитку організації;
- 2) протигаг щодо протилежних або конкуруючих інтересів;
- 3) сприяння в реалізації спільних інтересів [51, с. 42–61].

4.3 Корпоративні інтереси з розвитку та безпеки, їх сутність та значення для життєдіяльності організації

У структурі корпоративних інтересів можна виокремити дві групи:

1) корпоративні інтереси з розвитку організації (інтереси першого порядку);

2) корпоративні інтереси з безпеки організації (інтереси другого порядку).

Інтереси першого порядку пов'язані з функцією розвитку організації і спрямовані на те, щоб внаслідок економічних відносин отримати певну економічну вигоду.

Корпоративні інтереси з розвитку – це узгоджені інтереси внутрішніх і зовнішніх суб'єктів соціально-економічних відносин, реалізація яких необхідна для створення відповідних умов і механізмів, спрямованих на здійснення цілеспрямованих якісних і кількісних перетворень в організації.

Від їх реалізації залежить рівень розвитку організації, матеріальний добробут і вигода всіх учасників соціально-економічних відносин.

До них можна віднести:

- 1) отримання гарантованого доходу з вкладеного капіталу;
- 2) збереження та ефективне управління власністю;
- 3) вчасна виплата відповідної заробітної плати;
- 4) отримання акціонерним товариством максимального прибутку;
- 5) ефективне використання капіталу товариства;
- 6) налагоджені взаємовідносини «менеджмент-працівник», які б унеможливлювали виникнення конфліктних ситуацій і забезпечували відповідну робочу атмосферу;
- 7) забезпечення фінансової стійкості та незалежності роботи підприємства тощо.

Інтереси другого порядку пов'язані з функцією безпеки полягають у тому, щоб в організації були створені всі необхідні умови і механізми протидії загрозам, які спрямовані на те, щоб той чи інший учасник соціально-економічних відносин зміг отримати

належні йому вигоди. Тобто реалізація в організації інтересів другого порядку створює певні умови для реалізації інтересів першого порядку. Тому всі учасники соціально-економічних відносин мають бути зацікавлені в реалізації інтересів першого і другого порядків. Водночас для безпеки соціально-економічної системи більше значення мають корпоративні інтереси безпеки.

Корпоративні інтереси з безпеки – це узгоджені інтереси внутрішніх і зовнішніх суб'єктів соціально-економічних та безпекових відносин, реалізація яких необхідна для створення відповідних умов і механізмів для протидії внутрішнім й зовнішнім загрозам і сприяння в такий спосіб реалізації інтересів розвитку та збереження цілісності організації.

Основними видами безпекових корпоративних інтересів є:

1) усунення сприятливих умов в організації для вчинення правопорушень;

2) усунення перешкод щодо виплати дивідендів;

3) усунення перешкод щодо вчасної виплати заробітної плати;

4) дотримання вимог охорони праці та створення безпечних умов праці;

5) усунення сприятливих умов для виникнення надзвичайних ситуацій;

6) усунення перешкод для реалізації корпоративних прав;

7) дотримання технологічних вимог щодо якості і безпечності продукції;

8) усунення перешкод щодо виконання організацією договірних зобов'язань з кредиторами, постачальниками, партнерами;

9) усунення перешкод щодо дотримання організацією законів та взаємовідносин з державою;

10) усунення перешкод щодо дотримання організацією правил поведінки на фондовому ринку.

Корпоративні інтереси з функції розвитку і функції безпеки формуються як конкретні цілі, виражені в якісній чи кількісній формі, реалізація яких є необхідною умовою для стабільного функціонування соціальної системи. Наприклад, збільшення

частки на ринку на 3%, зниження собівартості продукції на 6%, збільшення інвестицій у будівництво на 7%, збільшення фінансування на енергозберігаючі технології на 4%, збільшення заробітної плати на 10%, зниження травматизму на виробництві на 2%, зниження рівня браку продукції на 1%, зниження кількості випадків професійного захворювання на 4% тощо [51, с. 42–61].

Питання та завдання для самоконтролю

1. Що таке приватні інтереси та який їх вплив на безпеку соціальної системи?
2. Розкрийте сутність групових інтересів та їх вплив на безпеку соціальної системи.
3. Поясніть, що таке пов'язані інтереси та який їх вплив на безпеку соціальної системи.
4. Розкрийте сутність корпоративних інтересів та їх значення для безпеки соціальної системи.
5. Що таке корпоративні інтереси з розвитку та яка їх роль у життєдіяльності організації.
6. Що таке корпоративні інтереси з безпеки та яка їх роль у життєдіяльності організації.

Тести

1. Усвідомлені потреби, що сформовані суспільством, колективом, соціальною групою, індивідом, – це:
 - а) корпоративні економічні інтереси;
 - б) інтереси;
 - в) економічні інтереси;
 - г) усі відповіді правильні.
2. У діяльності організації беруть участь різні учасники соціально-економічних відносин, які мають певні інтереси, що виявляються у формі:
 - а) приватного (особистого) інтересу;
 - б) групового інтересу;

- в) пов'язаного інтересу;
- г) усі відповіді правильні.

3. Основною ознакою приватного інтересу є:

- а) роздвоєність;
- б) відособленість;
- в) суперечливість;
- г) правильні відповіді б, в.

4. Усвідомлені потреби людини, задоволення яких необхідне для її життєдіяльності, – це:

- а) групові інтереси;
- б) приватні інтереси;
- в) особисті інтереси;
- г) правильні відповіді б, г.

5. Узгоджені приватні інтереси, реалізація яких необхідна для створення умов і механізмів для функціонування групи чи загалом колективу (організації), – це:

- а) групові інтереси;
- б) корпоративні інтереси;
- в) особисті інтереси;
- г) правильні відповіді б, в.

6. Інтереси суб'єктів, що мають з організацією відповідні соціально-економічні відносини, необхідні для забезпечення її життєдіяльності та офіційного функціонування, – це:

- а) групові інтереси;
- б) корпоративні інтереси;
- в) особисті інтереси;
- г) пов'язані інтереси.

7. Що є характерною ознакою корпоративних інтересів?

- а) узгодженість інтересів;
- б) універсальність інтересів;
- в) роздвоєність інтересів;
- г) комплексність інтересів.

8. Корпоративні інтереси – це:

а) сукупність життєво важливих інтересів відповідних учасників корпоративних відносин і самого підприємства;

б) сукупність узгоджених життєво важливих інтересів відповідних внутрішніх учасників корпоративних відносин і самого підприємства;

в) сукупність об'єктивних потреб соціальної системи, які виявляються як узгоджені інтереси відповідних суб'єктів учасників соціально-економічних відносин, реалізація яких необхідна для її життєдіяльності;

г) правильні відповіді б і в.

9. Корпоративні інтереси за ієрархічною структурою поділяються на:

а) управлінські інтереси;

б) інтереси безпеки організації;

в) інтереси розвитку організації;

г) правильні відповіді б, в.

10. Узгоджені інтереси внутрішніх і зовнішніх суб'єктів соціально-економічних відносин, реалізація яких необхідна для створення відповідних умов і механізмів, спрямованих на здійснення цілеспрямованих якісних і кількісних змін в організації, – це:

а) групові інтереси;

б) корпоративні інтереси з розвитку;

в) особисті інтереси;

г) пов'язані інтереси.

11. Узгоджені інтереси внутрішніх і зовнішніх суб'єктів соціально-економічних та безпекових відносин, реалізація яких необхідна для створення відповідних умов і механізмів для протидії внутрішнім й зовнішнім загрозам і сприяння в такий спосіб реалізації інтересів розвитку та збереження цілісності організації – це:

а) групові інтереси;

б) корпоративні інтереси з розвитку;

в) корпоративні інтереси з безпеки;

г) пов'язані інтереси.

12. Які з наведених видів інтересів є об'єктом безпеки?

- а) інтереси власника;
- б) корпоративні інтереси;
- в) інтереси менеджменту;
- г) інтереси найманих працівників.

13. Які з наведених видів корпоративних інтересів належать до інтересів безпеки?

- а) збереження та ефективне управління власністю;
- б) дотримання вимог охорони праці;
- в) усунення сприятливих умов для виникнення надзвичайних ситуацій;
- г) правильні відповіді б, в.

Тема 5

ЗАГРОЗИ СОЦІАЛЬНІЙ СИСТЕМІ

*Загроза подібна до випущеної із лука стріли.
Що більше ми знаємо з чого вона зроблена
та про лучника, то краще зможемо захиститися.
Це завжди складно, але цьому потрібно вчитися
та робити, а ще краще попереджувати постріл*

5.1 Сутність понять «виклик», «загроза», «небезпека», відмінності між ними та їх вплив на життєдіяльність соціальної системи

У теорії безпеки соціальних систем основними категоріями є «виклик», «загроза» та «небезпека». Кожна з них має власний зміст та особливості, які необхідно враховувати й застосовувати у безпековій діяльності (рис. 5.1).

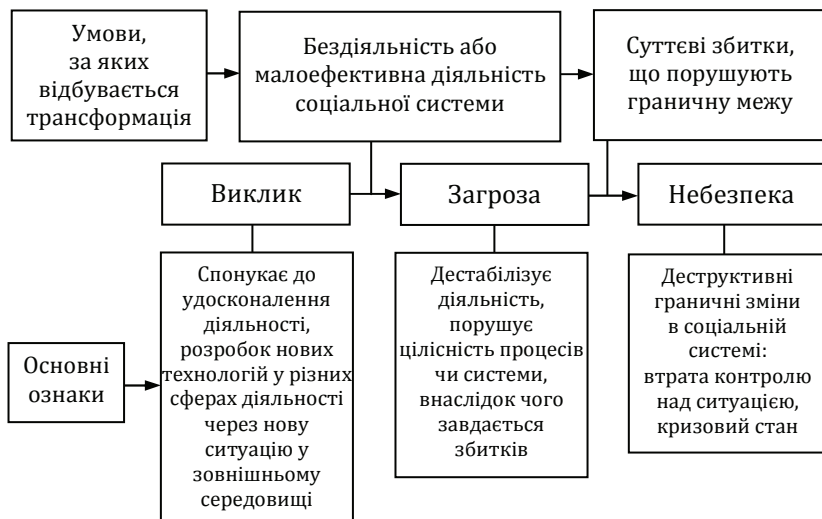


Рис. 5.1 Основні категорії безпеки соціальних систем

Виклик за своєю сутністю і змістом є новою ситуацією у зовнішньому середовищі, яка ставить нові вимоги до ухвалення рішень власниками і менеджментом організації, спрямованих на подальший розвиток. Виклики мобілізують зусилля власників, менеджерів і фахівців до удосконалення їх діяльності та спонукають до розробок нових технологій виробництва, більш конкурентних товарів тощо. Отже, виклик як явище створює для організації мотиваційне середовище для розвитку. Водночас, за умови бездіяльності чи малоефективної діяльнос-

ті відповідних суб'єктів виклик може призвести до виникнення загрози для конкретного об'єкта безпеки.

Поняття «загроза» у літературних джерел розглядається з різних боків:

1) розмаїття внутрішніх і зовнішніх, об'єктивних і суб'єктивних суперечностей суспільного розвитку у середовищі функціонування об'єкта, які ускладнюють або унеможливають створення сприятливих умов для реалізації його інтересів і створюють небезпеку для його системи безпеки, життєзабезпечення її системоутворюючих елементів [45, с. 37–38];

2) сукупність умов і чинників, що створюють небезпеку життєво важливим інтересам об'єкту охорони [45, с. 37–38];

3) реальні або потенційно-можливі дії, що призводять до моральних чи матеріальних збитків [56, с. 259–261].

З наведених та інших визначень поняття «загроза» зрозуміло, що загрози, які реалізуються, дестабілізують діяльність соціальної системи, порушують її цілісність та завдають збитків. Своєю чергою, збитки можуть стати на заваді реалізації корпоративних інтересів та спричинити небезпеку для організації. З цього однозначно випливає, що загроза – це негативна дія, вплив на об'єкт.

Основними ознаками загроз соціально-економічній системі можна вважати такі:

1) свідоме завдання збитків, погіршення стану процесів, об'єктів чи системи та порушення їх цілісності;

2) свідоме створення перешкод для реалізації корпоративних економічних інтересів, прав та обов'язків;

3) потенційний чи реальний економічний стан підприємства у різних сферах діяльності і загалом, що є нижчим від оптимального, але не нижче від встановлених граничних показників (індикаторів її безпеки).

4) природні дестабілізуючі чинники, внаслідок дії яких завдаються економічні збитки, які можна ще поновити.

Отже, не всі негативні чинники можна кваліфікувати як «загрози». Відтак не слід вважати загрозою економічній безпеці організації діяльність її керівництва, що спрямована на реалі-

зацію функції розвитку, наприклад: придбання цінних паперів, упровадження нових технологій, розробка нового товару тощо. Такі рішення є складовою підприємницької діяльності та завжди припускають ризик і певні втрати. Проте дії, які спрямовані на одержання будь-якої вигоди від економічної дестабілізації організації, розцінюються як загрози.

Якщо дія будь-якого внутрішнього чи зовнішнього чинника, що не завдає збитків, буде сприйматися корпоративною системою як загроза, то це відволікатиме зайві трудові, фінансові, технічні та інші ресурси. Тому до загроз необхідно відносити лише фактори, які формують зміст відносин у сфері економічної безпеки. Це фактори об'єктивні чи природні (наприклад, дії стихійних явищ природи можуть руйнувати продуктивні сили суспільства і призводити до економічних й корпоративних втрат та ін.), суб'єктивні (наприклад, недобросовісна конкуренція, порушення технологій, суспільних законів і норм, цілісності процесів чи об'єктів тощо). Водночас загрози можуть виникати і в середині корпоративних систем, і поза їх межами.

Отже, основною ознакою загрози є потенційні чи реальні збитки. Вони можуть бути моральними і матеріальними. За наслідками від таких, що обмежують діяльність, – аж до виникнення економічної небезпеки, зокрема кінцевої її стадії – припинення існування організації.

Отже, **загроза** – це дія дестабілізуючих природних і (або) суб'єктивних факторів, що спричиняє збитки соціальній системі чи конкретній фізичній особі.

Наведене свідчить про те, що потреба у безпеці виникає не тоді, коли є виклики, а коли виникають загрози. Для забезпечення безпеки соціальним системам необхідно протидіяти саме загрозам, оскільки в іншому разі виникне небезпека, подолати яку буде значно важче.

Загроза завжди ушкоджує, руйнує конкретний об'єкт. Водночас межею, за якою починається для підприємства небезпека, є деструктивні граничні зміни внаслідок збитків (рис. 5.2) [51, с. 4]. Деструктивні граничні зміни – це такі зміни, після яких у організації виникає кризовий стан, практично немає

ресурсів для розвитку і, у підсумку, для життєдіяльності. Межа, за якою настає небезпека, для кожної соціальної системи буде індивідуальна, її має знати принаймні вища ланка управління.

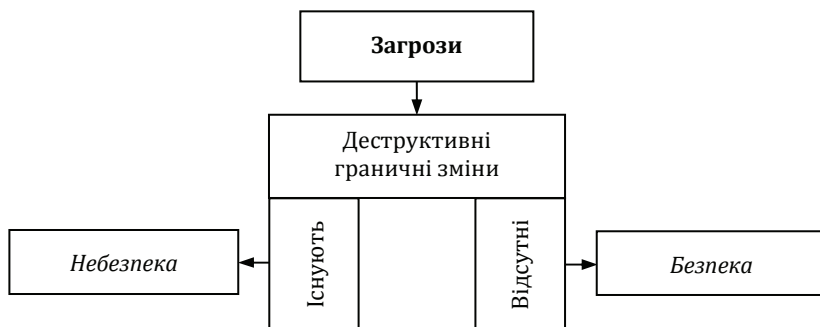


Рис. 5.2 Схематичне відображення основного змісту понять «небезпека» та «безпека»

Основними ознаками небезпеки є:

- 1) втрата контролю над ситуацією;
- 2) кризовий стан.

Отже, **небезпека** – це деструктивні граничні зміни, спричинені реалізацією загрози в соціальній системі, що зумовлюють її кризовий стан.

5.2 Класифікація загроз соціальній системі

Загрози можуть бути різноманітними, тому їх доцільно класифікувати за низкою основних критеріїв:

1) за стадіями життєвого циклу:

- а) на етапі організації фірми;
- б) на стадії функціонування;

2) за місцем виникнення:

- а) внутрішні;
- б) зовнішні;

3) за джерелом надходження:

- а) внутрішні:
 - керівники організації;
 - менеджери;

- працівники фірми;
- працівники служби безпеки;
- б) зовнішні:
 - кримінальні структури;
 - фірми-розвідники;
 - конкуренти (прямі і непрямі);
 - контрагенти;
 - корумповані представники: органів влади; правоохоронних органів; контрольних органів; засобів масової інформації;
 - стихійні лиха, аварії, катастрофи;

4) за ступенем ймовірності:

- а) потенційні;
- б) реальні;

5) за формами:

- а) економічні;
- б) фізичні;
- в) психоінформаційні;

6) за об'єктами:

- а) загрози персоналу фірми;
- б) загрози матеріальним ресурсам;
- в) загрози фінансовим ресурсам;
- г) загрози інформаційним ресурсам;
- г) загрози корпоративним інтересам;
- д) іміджу організації;
- е) загрози управлінню;

7) за наслідками:

- а) загрози, що не викликають небезпеки;
- б) загрози, що можуть викликати небезпеку;

8) за видами карності:

- а) адміністративно карні;
- б) кримінально карні;
- в) юридично не карні.

Класифікація спрямовує суб'єктів безпеки на збір інформації про загрози за певною структурою, а саме: необхідно знати місце і джерело виникнення загрози, яка їх ймовірність та

наслідки, якої вони форми та на який об'єкт спрямовані, а також який вид карності можуть мати.

5.3 Форми загроз, їх сутність, зміст та механізми реалізації

Аналіз наведених у літературних джерелах загроз засвідчив, що реальну небезпеку для соціально-економічної системи становлять загрози суб'єктивного походження, які реалізуються у формі *тіньової економіки, корупції, економічних правопорушень і злочинів та недобросовісної конкуренції* (рис. 5.3) [51].

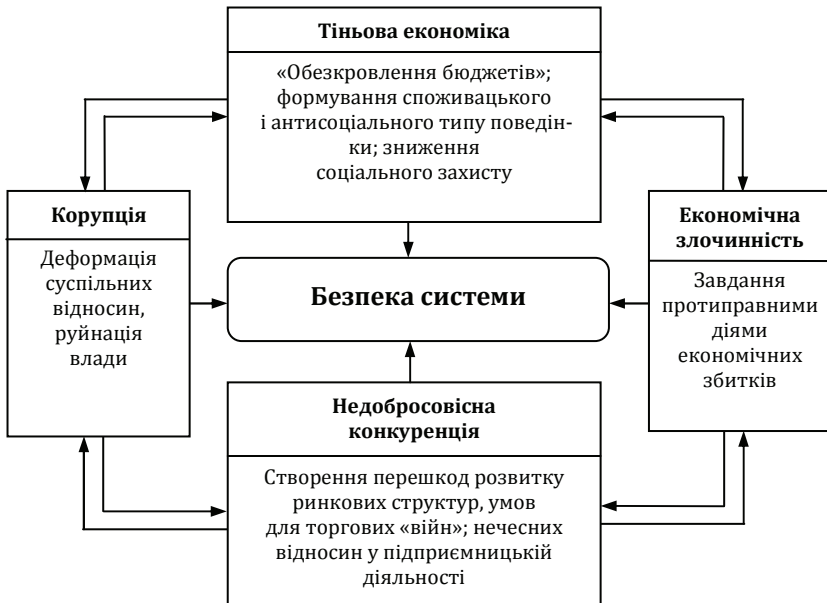


Рис. 5.3 Форми загроз соціальній системі та їх взаємозв'язок

Тіньова економіка – це протиправна економічна діяльність, а також та, що не враховується офіційною статистикою і не потрапляє до ВВП.

Дестабілізуючий вплив тіньової економіки можна відслідкувати за відповідними показниками. Особливо вони були руйнуючими у 2007 році. Так, за даними Міністерства економіки, обсяг тіньового обігу обчислювався в 180 млрд грн., 80% товарів широкого вжитку надходили до України за тіньовими схемами контрабандним шляхом. За незалежними експертними оцінками, близько 90% приватизованих підприємств працювали під контролем кримінально-олігархічних кланів, а тіньова економіка становила 50–60% [51].

В основі тіньової економічної діяльності є низка закономірностей:

1) провадження тіньової економічної діяльності, як правило, ініціюється і визначається наявністю тіньової вигоди, отримуваної в процесі порушення вимог і обмежень, висунутих державою до економічної діяльності;

2) що більша величина сумарного податкового навантаження на суб'єктів економічної діяльності, то більша тіньова вигода від заняття тіньовою діяльністю;

3) що більша величина витрат приховування, необхідних для здійснення тіньової економічної діяльності, то нижча тіньова вигода;

4) тіньова вигода від заняття забороненими видами діяльності визначається величиною попиту в суспільстві на заборонені товари і послуги, а також ефективністю державної протидії і переслідування цих видів діяльності;

5) величина тіньових доходів від корупційних діянь і масштаби розповсюдження корупції в державі залежать від рівня адміністративно-правових обмежень і регламентації економічної діяльності, обмеження легальних доходів працівників держапарату, а також від ступеня суб'єктивного впливу з боку чиновників на ухвалення рішень, які є в компетенції державного апарату.

Структура тіньової діяльності подана на рисунку 5.4.

Надзвичайно дестабілізуючий вплив на безпеку соціальної системи має корупція. Це своєрідне дзеркало суспільства, його моральної і правової чистоти, економічного, політичного та соціального стану. Корупція характеризує основні соціальні процеси, які відбуваються у державі та суспільстві, у

ній відображаються найбільш значущі для держави та суспільства проблеми.

За останні роки в Україні корумповані відносини щораз більше витісняють правові, та етичні відносини між людьми, поступово перетворюючись із аномалії у норму поведінки. На міжнародному рівні Україна має репутацію надзвичайно корумпованої країни.



Рис. 5.4. Структура тіньової економіки

Корупція є одним із головних чинників роздвоєння суспільства на дві соціальні підсистеми, які паралельно співіснують між собою (рис. 5.5): одна з них орієнтується на правові та моральні норми, інша – на використання протиправних засобів.

Суб'єкти корупції функціонують у неофіційній системі, в якій панує власна система цінностей, свої цілі і засоби їх досягнення. Через протиправність своєї діяльності вони не можуть «засвітити» суспільству свої корумповані відносини, оскільки у такому разі настане реакція з боку закону на їхні дії.

Водночас суб'єкти корупції не можуть існувати без офіційної підсистеми. Остання для них є обов'язковою передумовою встановлення корумпованих відносин: для того, щоб зловживати владою, її потрібно мати: обіймати відповідну посаду в органах державної влади (місцевого самоврядування), бути наділеним певними повноваженнями, мати можливість їх офіційно використовувати. Крім того, офіційна підсистема є прикриттям неофіційної підсистеми. По-перше, суб'єкти корупції для досягнення своїх протиправних цілей використовують надані законом повноваження. По-друге, офіційний статус використовується ними для ухилення від передбаченої законом відповідальності.

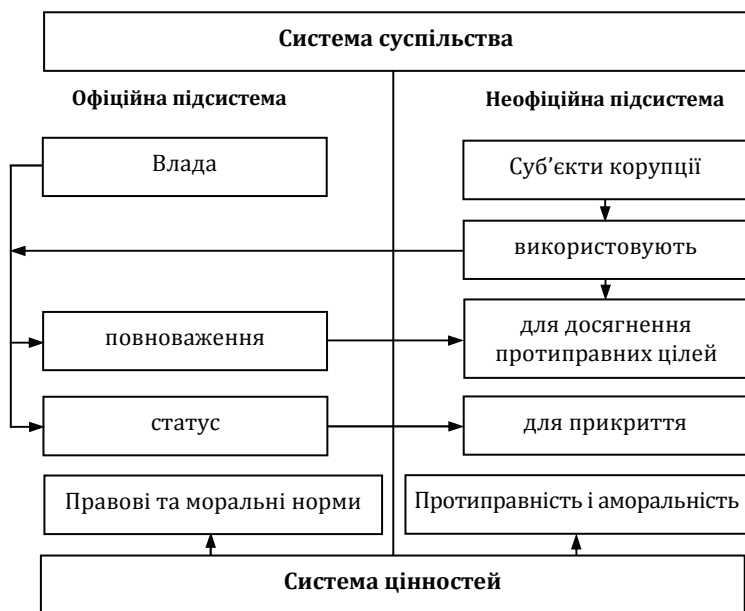


Рис. 5.5 Зміст корупційної діяльності

Корупція стала невід'ємною частиною сучасного державного і суспільного механізму, пронизуючи всі його структури та рівні. Вона уніфікує методи і форми відносин державних органів влади з представниками легального бізнесу та організованої злочинності, інтегруючи їх у єдину систему тіньових (кримінальних) відносин.

Зв'язок між корупційними діями створює сприятливі умови для вчинення. Відтак розкрадання чужого майна з використанням посадового становища дає можливість давати хабар, фальсифікація документів дозволяє вчинити розкрадання та ін.

Недобросовісна конкуренція:

– це будь-які дії у конкуренції, які не відповідають правилам, торговим або іншим чесним звичкам у підприємницькій діяльності (Закон України «Про захист від недобросовісної конкуренції», 1997 р.);

– будь-який акт конкуренції, що є не сумісним із чесними звичками в промислових і торгових домах (Паризька конвенція з охорони промислової власності, 1988 р.)

Згідно з Паризькою конвенцією недобросовісна конкуренція може виявлятися у таких формах:

а) усі дії, котрі будь-як можуть спотворювати інформацію щодо підприємств, товарів, промислової і торгової діяльності конкурента;

б) неправдиві твердження під час здійснення комерційної діяльності, що здатні дискредитувати підприємство, товари, промислову або торгову діяльність конкурента;

в) вказівки або твердження, використання яких у процесі здійснення комерційної діяльності може обдурити щодо характеру, способу виробництва, властивостей, здатності до використання або якості товару.

Відповідно до Закону України «Про захист від недобросовісної конкуренції» недобросовісна конкуренція може виявлятися у таких основних формах:

1. *Неправомірне використання ділової репутації суб'єкта господарювання* (неправомірне використання чужих позначень, рекламних матеріалів і упаковки; неправомірне використання товару іншого виробника; порівняльна реклама).

2. *Неправомірний збір, розголошення і використання комерційної таємниці* (неправомірний збір відомостей, які становлять комерційну таємницю; розголошення відомостей, які становлять комерційну таємницю; схилення до розголошення відомостей, які становлять комерційну таємницю; неправомірне використання комерційної таємниці).

3. Створення перешкод суб'єктам господарювання в процесі конкуренції і досягнення неправомірних переваг у конкуренції (дискредитація суб'єкта господарювання; купівля-продаж товарів, виконання робіт, надання послуг з примусовим асортиментом; схиляння до бойкоту суб'єкта господарювання; підкуп працівника постачальника; схиляння постачальника до дискримінації покупця (замовника); схиляння суб'єкта господарювання (підприємця) до розірвання договору з конкурентом; підкуп працівника покупця (замовника); досягнення неправомірних переваг у конкуренції).

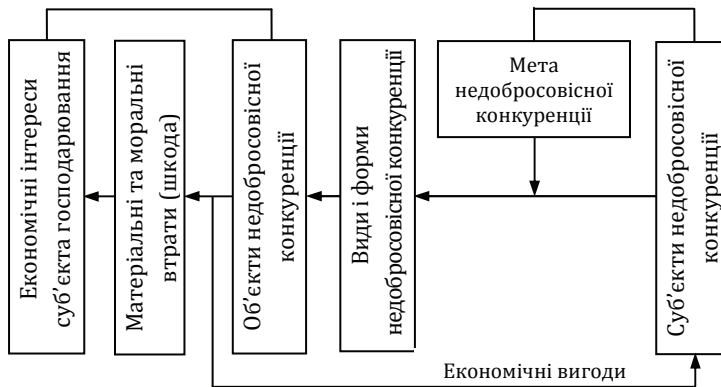


Рис. 5.6 Зміст недобросовісної конкуренції

Більшість загроз у сфері економічних відносин, особливо, коли існує тіньова економічна діяльність, мають цілеспрямований характер і виявляються у вигляді економічних правопорушень. Своєю чергою, це зумовлює втрати для держави, юридичних та фізичних осіб. Однак не всі втрати можуть спричинити загрозу, а надто небезпеку для учасників економічних відносин. Небезпечними є ті, які за нанесеною шкодою є вагомими і погіршують соціально-економічне становище фізичної особи, підприємницької структури, держави. Завдати таких втрат (шкоди) вказаним суб'єктам, чи економіці загалом можуть правопорушення, які згідно з чинним законодавством, кваліфікуються як злочин (економічний злочин). Саме економічна злочинна діяльність є основною структурною складовою ілєгального і кримінального тіньового сектора економіки, живильним середовищем і своєрід-

ним чинником його поширення, що становить серйозну загрозу економічній безпеці України, зокрема й організаціям.

Економічний злочин – це умисна суспільно небезпечна діяльність або бездіяльність, яка призводить до значних втрат суб'єкта господарювання і фізичних осіб, і стає на заваді реалізації економічних інтересів, зумовлюючи цим погіршення їх соціально-економічного стану.

Зміст економічного злочину схематично подано на рис. 5.7.

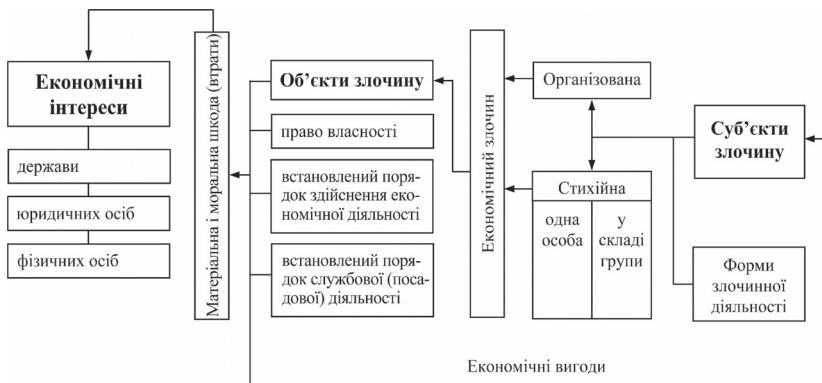


Рис. 5.7 Зміст економічного злочину

Сутність його зводиться до того, що суб'єкти злочину умисно в організованій формі, чи стихійно використовуючи можливості пристосування внутрішнього і зовнішнього середовища управління для свідомого прикриття, порушують право власності інших (наприклад, привласнюють майно) чи порушують встановлений порядок на економічну діяльність, завдаючи цим значних збитків економічним інтересам держави, юридичним і фізичним особам чи економіці країни загалом. Своєю чергою, злочинці за рахунок протиправних дій отримують надприбутки або інші економічні вигоди. Водночас таку злочинну економічну діяльність, не зважаючи на те, що вона має множинність епізодів злочину, складно вчасно виявити. Жертва економічного злочину, як правило, лише через певний період відчує, що її інтересам була заподіяно шкоди і лише після цього вживатиме активних дій захисту.

Запитання й завдання для самоконтролю

1. Як Ви розумієте поняття «виклик», які його основні ознаки та вплив на життєдіяльність соціальної системи?
2. Що таке «загроза», які її основні ознаки та вплив на безпеку соціальної системи?
3. Що таке «небезпека», які її основні ознаки та вплив на безпеку соціальної системи?
4. Розкрийте основні умови трансформації понять: «виклик» – «загроза» – «небезпека», їх відмінності та вплив на життєдіяльність організації.
5. Наведіть класифікацію загроз соціальній системі.
6. Охарактеризуйте тіньову економіку як форму загрози соціальній системі.
7. Поясніть, чому корупція є формою загрози соціальній системі та розкрийте її сутність.
8. Обґрунтуйте, чому економічні злочини виявляються у формі загрози соціальній системі.
9. Чому недобросовісна конкуренція є формою загрози для соціальної системи?

Тести

1. Нова ситуація у зовнішньому середовищі, яка ставить нові вимоги до ухвалення рішень, спрямованих на подальший розвиток соціально-економічної системи – це:
 - а) загроза;
 - б) небезпека;
 - в) виклик;
 - г) усі відповіді правильні.
2. Удосконалення діяльності, спрямованої на розробку нових технологій виробництва, більш конкурентних товарів тощо – це реакція на:
 - а) загрозу;
 - б) виклик;
 - в) небезпеку;
 - г) усі відповіді правильні.
3. Бездіяльність чи малоефективна діяльність відповідних суб'єктів господарювання може призвести до виникнення:
 - а) загрози;

- б) виклику;
- в) небезпеки;
- г) усі відповіді правильні.

4. Потреба у безпеці виникає тоді, коли існують:

- а) загрози;
- б) виклики;
- в) небезпеки;
- г) правильні відповіді а і в.

5. Придбання цінних паперів соціально-економічною системою – це діяльність, спрямована на:

- а) виникнення виклику;
- б) виникнення загрози;
- в) створення умов для розвитку;
- г) виникнення небезпеки.

6. Упровадження нових технологій соціально-економічною системою – це діяльність, спрямована на:

- а) виникнення небезпеки;
- б) створення умов для розвитку;
- в) виникнення загрози;
- г) виникнення виклику.

7. Загроза – це:

а) реальні або потенційно-можливі дії, що призводять до моральних чи матеріальних збитків;

б) сукупність діянь (дій або бездіяльності), а також умов і чинників, що зумовлюють економічну небезпеку життєво важливим інтересам країни;

в) дія дестабілізуючих природних і (або) суб'єктивних факторів, що спричиняють збитки;

- г) правильні відповіді а, в.

8. Стан соціально-економічної системи, за якого організація практично немає ресурсів для життєдіяльності, кваліфікується як:

- а) загроза;
- б) виклик;
- в) небезпека;
- г) правильні відповіді а і б.

9. Деструктивні граничні зміни в корпоративній системі, спричинені реальними збитками (втратами), кваліфікуються як:

- а) загрози;
- б) небезпека;
- в) виклик;
- г) правильні відповіді а і в.

10. Основними ознаками загроз соціально-економічній системі є:

а) погіршення стану процесів, об'єктів чи системи та порушення їх цілісності;

б) потенційний чи реальний економічний стан підприємства у різних сферах діяльності загалом, що є нижчим від оптимального, але не нижче від встановлених граничних показників (індикаторів економічної безпеки).

в) природні дестабілізуючі чинники, внаслідок дії яких заважаються економічні збитки, які неможна поновити.

- г) правильні відповіді а, б.

11. За формами впливу загрози можна поділяти на загрози:

- а) потенційні;
- б) економічні;
- в) реальні;
- г) правильні відповіді а, в.

12. За впливом на об'єкт загрози можна поділяти на загрози:

- а) персоналу фірми;
- б) матеріальним ресурсам;
- в) іміджу організації;
- г) правильні відповіді а, б, в.

13. Тіньова економіка – це:

а) протиправна економічна діяльність, а також та, що не враховується офіційною статистикою і не потрапляє до ВВП;

б) економічна діяльність, що не враховується офіційною статистикою і не потрапляє до ВВП;

в) протиправна економічна діяльність, що не враховується офіційною статистикою і не потрапляє до ВВП;

- г) правильні відповіді б, в.

14. Суб'єкти корупції для прикриття своєї протиправної діяльності та уникнення відповідальності використовують:

- а) делеговані владою обов'язки;
- б) посадовий статус;
- в) фінансові ресурси;
- г) зв'язки у виконавчих структурах влади.

15. Діяльність, яка інтегрує відносини державних органів влади з представниками легального бізнесу та організованої злочинності у єдину систему тіньових відносин, – це:

- а) корупція;
- б) тіньова економіка;
- в) економічна злочинність;
- г) недобросовісна конкуренція.

16. Недобросовісна конкуренція – це:

а) це будь-які дії у підприємницькій діяльності, які здійснюються за правилами чи звичками суб'єкта недобросовісної конкуренції;

б) будь-який акт конкуренції, що є не сумісним із чесними звичками в промислових і торгових домах;

в) це будь-які дії у конкуренції, які не відповідають правилам, торговим або іншим чесним звичкам у підприємницькій діяльності;

г) правильні відповіді б, в.

17. Економічний злочин – це:

а) небезпечна діяльність або бездіяльність, яка призводить до істотних втрат суб'єкта господарювання і фізичних осіб, і стає на заваді реалізації їх економічних інтересів;

б) умисна суспільно небезпечна діяльність або бездіяльність, яка призводить до істотних втрат суб'єкта господарювання і фізичних осіб, і стає на перешкоді реалізації економічних інтересів, зумовлюючи цим погіршення їх соціально-економічного стану;

в) умисна діяльність або бездіяльність, яка призводить до втрат суб'єкта господарювання і фізичних осіб, і стає на перешкоді реалізації економічних інтересів;

г) небезпечна діяльність або бездіяльність, яка призводить до значних втрат суб'єкта господарювання і фізичних осіб.

Тема 6

БЕЗПЕКОВА ДІЯЛЬНІСТЬ СОЦІАЛЬНОЇ СИСТЕМИ

*Діяльність – основа життєдіяльності людини
та організації, а безпекова діяльність –
це їх корінна функція самозбереження.
Її здійснення – запорука руйнації
та банкрутства соціальної системи*

6.1 Сутність та структура безпекової діяльності

Соціальна система для забезпечення власної життєдіяльності та самозбереження виконує корінну функцію – функцію безпеки, тобто здійснює напрям діяльності у сфері безпеки. Для зручності його можна назвати безпековою діяльністю системи чи суб'єктів безпеки.

Безпекова діяльність – форма активного ставлення суб'єктів безпеки до безпекової дійсності, зміст якого полягає у проведенні в ній відповідних змін на основі засвоєння та розвитку безпекової культури. Тобто це діяльність, спрямована на протидію загрозам з метою захисту корпоративних інтересів, збереження цілісності процесів чи системи та сприяння її розвитку на основі засвоєння та розвитку безпекової культури.

За змістом безпекова діяльність має комплексний характер, що дає змогу володіти відповідною інформацією оперативного і аналітичного характеру про загрози, на основі якої попереджати їх виникнення чи реалізацію. У випадках настання загрози – ліквідовувати її, після реалізації – відновлювати, цілісність процесів чи об'єктів, компенсувати втрати. Відтак безпекова діяльність структурно містить такі механізми:

- 1) попереджувально-профілактичні;
- 2) інформаційно-виявляючі;
- 3) ліквідаційні;
- 4) відновлювальні.

На практиці кожний з цих механізмів безпекової діяльності реалізується через низку видових функцій безпеки (видів безпекової діяльності), які містять відповідні методи і засоби. Водночас логіка послідовності цього процесу технологічно має такий вигляд: конкретний механізм безпекової діяльності реалізується через видові функції безпеки, кожна з яких, своєю чергою, виконується шляхом використання відповідних методів і засобів. Наприклад, для реалізації механізмів

му виявлення загрози у формі крадіжки на підприємстві з метою отримання інформації про можливості її реалізації можна здійснювати детективну чи охоронну діяльність з використанням методу відеоспостереження. Для цього обов'язково потрібна відеокамера як засіб, яка встановлюється у потрібних місцях. Також необхідно дотримуватися основних безпекових принципів: своєчасності, правомірності та поєднання гласності й конфіденційності. В результаті буде отримана відповідна інформація, яка дозволить виявити потенційну чи реальну загрозу крадіжки. Загалом структуру безпекової діяльності подано на рисунку 6.1.

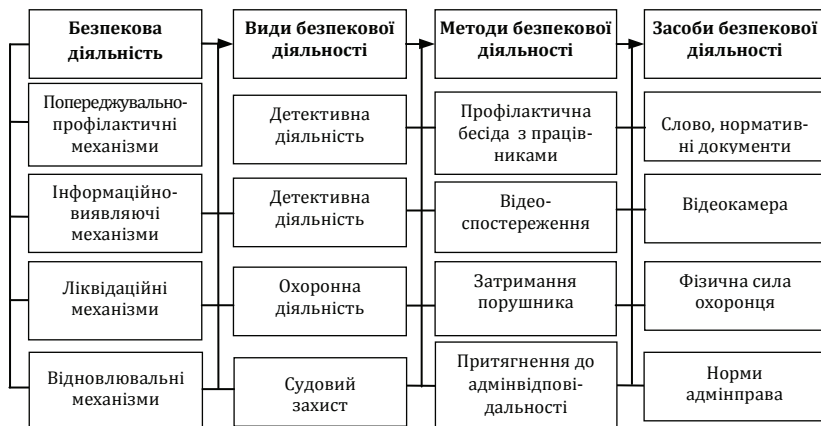


Рис. 6.1 Змістовна структура безпекової діяльності

На цьому рисунку види безпекової діяльності (видові функції безпеки), відповідні методи та засоби для реалізації безпекових механізмів наведені як приклади. Це наочно демонструє зв'язок між ними та формує розуміння технології практичної безпекової діяльності. Водночас необхідно розуміти, що для реалізації того чи іншого безпекового механізму на практиці використовуються комплекс відповідних видових функцій, методів та засобів. Їхня кількість залежить від виду загрози та об'єкта, на який її вплив спрямований.

6.2 Механізми безпекової діяльності

6.2.1 Попереджувально-профілактичні механізми безпекової діяльності

Під *попереджувально-профілактичними механізмами* безпекової діяльності розуміється сукупність відповідних видів діяльності, методів та засобів, пов'язаних з розробкою та дотриманням законів, підзаконних актів з питань безпеки, а також нормативів безпеки та інших управлінських рішень, від режиму до регламентації поведінки працівників підприємства [51].

Основне призначення попереджувально-профілактичних механізмів полягає у формуванні умов, які б не створювали живильного середовища для виникнення загроз та були своєрідним «фільтром» на їх шляху. Схематично цей процес відображено на рисунку 6.2.

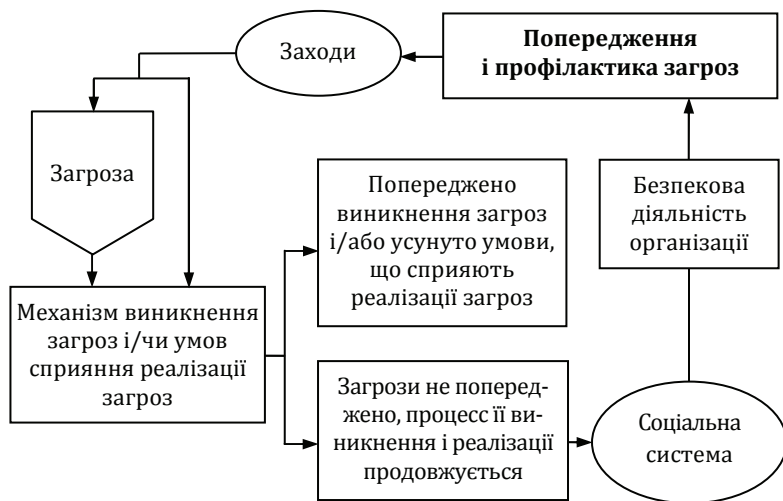


Рис. 6.2 Схеми моделі
попереджувально-профілактичних механізмів
безпекової діяльності

Варто зауважити, що зазначенні механізми мають формуватися на двох рівнях: державному та на рівні підприємства. На державному вони розробляються та застосовуються у формі законів України та підзаконних актів, які регулюють та регламентують процес функціонування організації, а також й таких, що дозволяють забезпечувати її безпеку. На рівні підприємства, мають бути передбачені відповідні безпекові норми: в статуті, положеннях про структурні підрозділи, посадових інструкціях, у контрактах тощо. Наприклад, правила техніки безпеки під час виконання зварювальних робіт; план дій на випадок пожежі; регламентація у контрактах на постачання матеріалів питань відповідальності покупця за порушення умов договору тощо.

Попередження втрат є основним завданням системи економічної безпеки підприємства, що в підсумку має попередити загрозу банкрутства організації [25, с. 545]. Попередження загрози в економічному плані є більш ефективним, адже співвідношення витрат, здійснених до моменту настання негативної події та завдання шкоди підприємству, і витрат на ліквідацію наслідків загрози та відновлення майна і ресурсів, дорівнює 1/15 [4].

Для реалізації попереджувально-профілактичних механізмів безпекової діяльності необхідно виконувати низку видових функцій безпеки й управління, виконання чи невиконання яких впливає на її ефективність. Основний її зміст полягає у розробці нормативно-правового забезпечення та створення відповідних мотиваційних умов з питань економічної безпеки. За умови їх наявності, виконання та дотримання попереджувально-профілактичні механізми виконують роль «фільтра», що перешкоджає створенню сприятливого середовища для виникнення загроз або послаблення процесу їх реалізації та мінімізації впливу.

Запроваджені в організації пропускний режим, патрулювання охоронниками території і вартова служба є перешкодою для вчинення тих чи інших порушень (самовільний вивіз матеріальних цінностей організації, учинення крадіжок, безперешкодне проникнення на територію з метою завдання збитків тощо). Організація фізичної охорони відповідних посадових

осіб соціальної системи попереджає виникнення і реалізацію загроз для їх здоров'я чи життя.

Планування і реалізація протипожежних заходів дають змогу створити в організації умови, за яких ймовірність виникнення пожежі залишається незначною.

Використовуючи в безпековій діяльності технічні засоби, можна попередити витік інформації з відповідних приміщень, що може зніматися спеціальними пристроями дистанційного відеоспостереження, а також з обчислювальних систем і засобів зв'язку.

Шляхом детективної діяльності можна вчасно виявляти наміри щодо вчинення правопорушень, спрямованих на завдання збитків організації.

Проводячи внутрішню експертизу нормативних документів, можна захищати корпоративні економічні інтереси та права. Проведення відповідної правової оцінки неправомірних дій чи бездіяльності менеджерів чи інших працівників організації є ефективною профілактикою для вчинення таких дій у майбутньому.

Плануючи відповідні заходи з безпеки з усіх напрямів і видів діяльності організації, зокрема й на випадок надзвичайних ситуацій, більшість загроз можна попередити.

Оптимізація заробітної плати, преміювання менеджерів і працівників організації, відносини між керівниками і підлеглими та загалом у колективі соціальної системи формують умови, що не спонукають їх до цілеспрямованого і свідомого завдання збитків.

Особливо ефективною в плані попередження виникнення і реалізації загроз є система контролю за роботою менеджерів і працівників, зберіганням і використанням товарно-матеріальних цінностей, фінансово-господарською діяльністю.

Визначальну роль у попередженні загроз виконує реально створена і оформлена в організації система безпеки, основне місце в якій займає власна служба безпеки та відповідна нормативно-правова база (норми з питань безпеки у Статуті, концепція безпеки, положення про захист інформації тощо).

Отже, результатом реалізації попереджувально-профілактичних механізмів є застосовані зовнішні та створені внутрішні нормативно-правові документи та умови і можливості для попередження і профілактики потенційних чи реальних загроз. Наприклад, з питань виробництва такими можуть бути:

- а) правила техніки безпеки на виробництві;
- б) технологічні вимоги захисту від підробок;
- в) план дій на випадок надзвичайних подій на виробництві;
- г) регламентація у контрактах на постачання сировини, матеріалів тощо, питань відповідальності постачальника за порушення умов договору;
- г) режим технічного захисту інформації з обмеженим доступом, у тому числі й комерційної таємниці;
- д) режим технічного контролю доступу у виробничі будинки, приміщення;
- е) нормативно-правові документи з питань охорони матеріальних цінностей та виробничих об'єктів;
- є) режим допуску і перебування на виробничих об'єктах;
- ж) екологічні вимоги до процесу виробництва та продукту тощо.

6.2.2 Інформаційно-виявляючі механізми безпекової діяльності

Під **інформаційно-виявляючими механізмами** розуміється сукупність відповідних видів діяльності, методів та засобів, пов'язаних зі збором і аналізом інформації про загрози та документуванням протиправних дій у відповідному часі та просторі [51].

Зміст механізмів виявлення загроз подано на рисунку 6.3.

Основним призначенням інформаційно-виявляючих механізмів безпекової діяльності є вчасне документування протиправних дій, отримання або передача відповідним керівникам, структурам чи виконавцям інформації про потенційні чи реальні загрози, які були чи є в організації або на ринках, і сто-

суються підприємства. Також у межах цього механізму здійснюється зворотній зв'язок з працівниками організації з метою інформування їх про необхідність дотримання режимних заходів, підвищення кваліфікації з питань безпеки та відповідальності за протиправні вчинки.

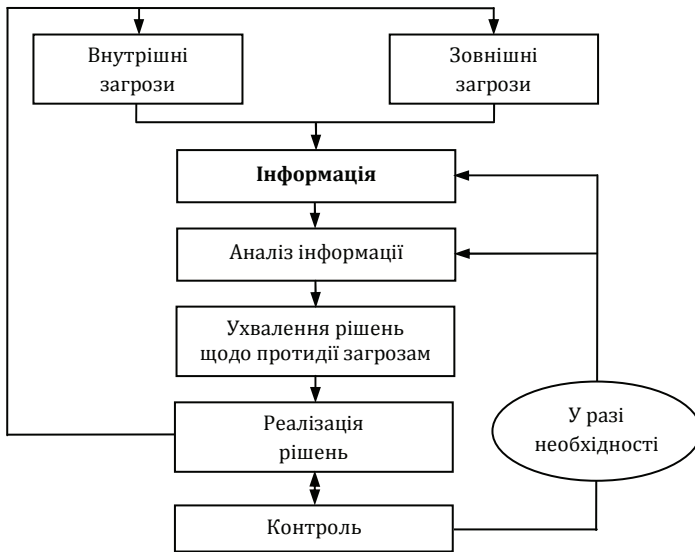


Рис. 6.3 Схема моделі інформаційно-виявляючих механізмів безпекової діяльності

Відтак, використовуючи технології аналітично-пошукової діяльності, вищий менеджмент і власники соціальної системи можуть вчасно отримувати інформацію про потенційні чи реальні загрози стратегічного характеру з боку зовнішнього середовища (основного конкурента, держави у вигляді зміни законодавства тощо), а також з боку внутрішнього середовища (про рівень зносу виробничих фондів, про зниження рівня кваліфікації персоналу тощо).

За допомогою детективної діяльності можна отримувати інформацію про потенційні чи реальні загрози протиправного характеру з боку зовнішнього середовища і на ринку (підробку

продукції, недобросовісну рекламу, рейдерське захоплення підприємства тощо), а також в середині організації (наміри про виведення чи розмивання капіталу, наміри про підтримку групи осіб у рейдерському захопленні підприємства та інші можливі чи реальні порушення на ринку). Водночас, використовуючи технології детективної діяльності, факти протиправних дій документуються, що значно може покращити взаємодію з правоохоронними органами. Також може бути ситуація, коли правоохоронні органи, які мають право здійснювати оперативно-розшукову діяльність, інформують суб'єктів безпеки організації про ті чи інші загрози протиправного характеру (можливі рейдерські захоплення, інтерес злочинних угруповань до організації чи його власників тощо).

У процесі здійснення фізичної і технічної охорони збирається інформація про вчинення різних порушень у середині підприємства (крадіжки, спроби чи факти знищення або ушкодження майна, спроби чи факти порушення встановленого режиму тощо).

Інформаційно-виявляючі механізми також реалізується через функцію організування, яка забезпечує розподіл функцій між підрозділами та службами, а також закріплення функціональних обов'язків між працівниками, що пов'язані зі збором, аналізом і передачею відповідної інформації. Функція організування містить і механізми інформування (збори, наради тощо) про порушення на ринку і всередині підприємства.

Особливе місце в реалізації інформаційно-виявляючої складової займає контроль. Фахово створена система контролю в організації дає змогу отримувати інформацію про невиконання чи не ефективне виконання функціональних обов'язків, про порушення внутрішнього розпорядку чи встановлених режимів роботи підприємства та допусків до комерційної таємниці, внаслідок чого підприємству завдаються збитки. Проведення в організації інвентаризації дозволяє виявляти проблеми чи порушення обліку і зберігання матеріальних цінностей. Через аудит виявляються факти неефективного використання капіталу, а через перевірку ревізійною комісією фінансово-

господарської діяльності виявляються і встановлюються факти порушення, якими завдаються збитки.

Слід зважити на те, що предметом інформаційно-виявляючих механізмів безпекової діяльності є збір і аналіз інформації та документування протиправних дій, які кваліфікуються як загрози. Їх результатом має бути конкретна інформація про загрози. Наприклад, з питань виробництва такою інформацією можуть бути наміри:

- а) про виведення з ладу виробничих засобів;
- б) про порушення технологічних процесів;
- в) про підготовку технологічних аварій, пожеж, учинення інших надзвичайних дій;
- г) про підготовку крадіжки, псування продукції тощо;
- г) про протиправні спроби проникнення в комп'ютерні мережі з обмеженим доступом з метою одержання виробничих секретів;
- д) про можливий зрив постачання сировини, матеріалів тощо.

Під час реалізації інформаційно-виявляючої складової безпекової діяльності забезпечуються процес ухвалення рішень інформацією про потенційні чи реальні загрози соціальній системі, а також оперативні зв'язки з іншими структурами безпеки і відповідними підрозділами правоохоронних органів.

За умови врахування інформації під час ухвалення відповідного рішення та його виконанні загрози можуть бути ліквідовані чи їх вплив пом'якшений, а відтак можна уникнути втрат чи звести їх до мінімуму, або навпаки.

6.3 Ліквідаційні механізми безпекової діяльності

У реальній діяльності у силу різних причин та обставин суб'єктам безпеки не вдається повністю попереджувати загрози, через що вони все ж таки дестабілізують роботу підприємства, наносять йому збитки. Для їх ліквідації потрібні відповідні механізми. ***Під ліквідаційними механізмами безпекової дія-***

льності розуміється сукупність видів безпекової діяльності та відповідних конфіденційних методів, методів роботи у надзвичайних ситуаціях, а також засобів, здатних ліквідовувати (припиняти дію) загрози на будь-якій стадії її реалізації.

Схему моделі ліквідаційних механізмів безпекової діяльності подано на рис. 6.4.

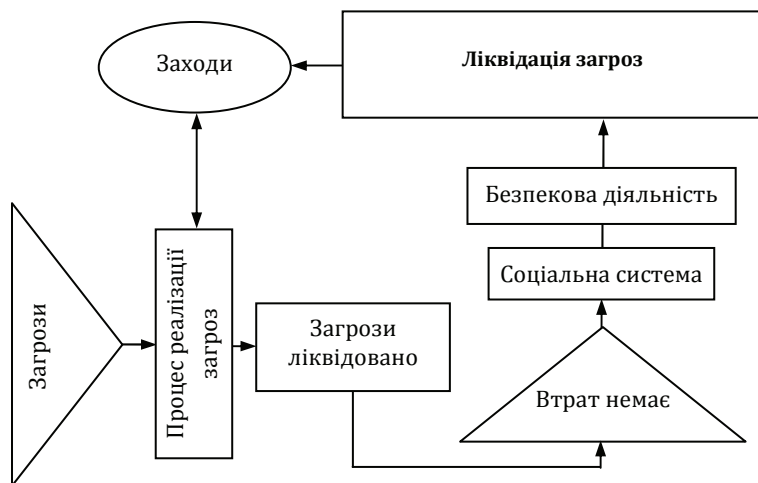


Рис. 6.4 Схema моделі ліквідаційних механізмів безпекової діяльності

Основне призначення ліквідаційних механізмів полягає у створенні відповідних умов та можливостей для ліквідації (припинення) загроз соціальній системі.

Для реалізації ліквідаційних механізмів безпекової діяльності необхідно виконувати низку видових функцій безпеки й управління, виконання чи невиконання яких впливає на її ефективність.

Відтак, використовуючи методи і засоби фізичної та технічної охорони, протиправні дії осіб в організації, зокрема ті, що пов'язані з витоком інформації з обчислювальних систем, засобів зв'язку та спеціальних приміщень, можна вчасно припиняти.

Особливо результативною у ліквідації тих чи інших загроз може бути система контролю в організації, завдяки якій можна вчасно виявити: порушення організацією договірних зобов'язань із постачання власної продукції; зловживання менеджерами і невиконання чи неналежне виконання роботи працівниками; зловживання під час зберігання і використання товарно-матеріальних цінностей та грошових коштів, використовуючи методи інвентаризації, спеціальні методи економічного аналізу, методи дослідження документів та методи фактичного контролю за господарськими операціями, а також порушення у фінансово-господарській діяльності, використовуючи методи аудиту та ревізії тощо.

Під час ліквідації загроз соціальній системі можна використовувати відповідні власні організаційні структури або залучати зовнішні, а також механізми взаємодії між організацією і правоохоронними органами.

За допомогою методів і засобів юридичного захисту можна успішно припинити низку загроз протиправного характеру, а саме: несправедливі рішення державних органів та претензії контрагентів чи партнерів; рейдерські атаки або інші протиправні дії з приводу заволодіння капіталом організації; порушення авторських прав соціальної системи тощо.

Результатом реалізації ліквідаційної складової є показники, які відображають її підсумки щодо ліквідації загроз. Наприклад, з питань виробництва такими показниками можуть бути:

- а) припинення випуску бракованої продукції;
- б) ліквідація умов, причин чи самого процесу порушення правил техніки безпеки на виробництві;
- в) ліквідація умов і причин профзахворювання;
- г) ліквідація технологічної аварії чи пожежі на виробництві;
- д) затримання осіб, що вчиняли крадіжки на виробництві;
- е) виявлення і припинення порушення умов договору на постачання сировини, комплектуючих тощо;
- є) затримання осіб за незаконне проникнення у будівлі чи приміщення виробничого призначення;

ж) затримання осіб за несанкціоноване проникнення в інформаційну систему організації з обмеженим доступом.

6.4 Відновлювальні механізми безпекової діяльності

У реальному житті система безпеки організації може мати різні за якістю «фільтри», внаслідок чого загрози мають можливість реалізуватися. У такому випадку, для зменшення їх впливу чи відновлення роботи безпекова діяльність повинна мати відновлювальні механізми (рис. 6.5).

Під **відновлювальними механізмами** безпекової діяльності розуміється сукупність видів безпекової діяльності та відповідних методів й засобів, необхідних для відновлення процесів, кількісних чи якісних показників діяльності, зв'язків та цілісності підприємства тощо після реалізації загрози, а також відшкодування за завданні збитки.

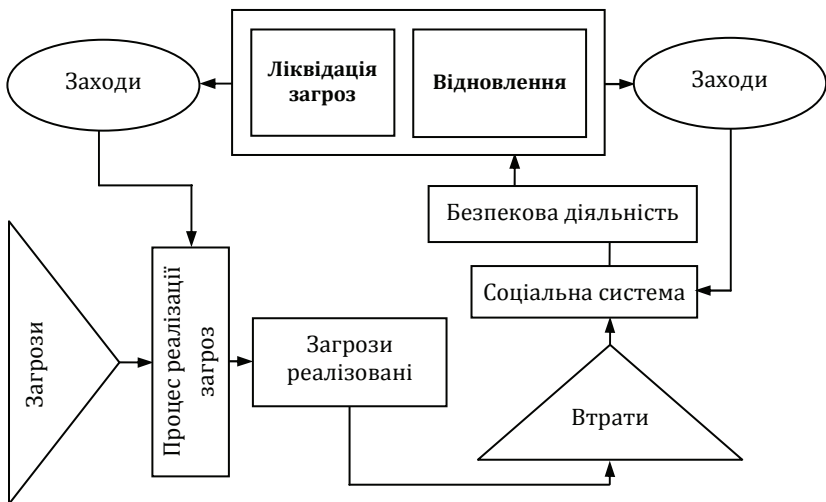


Рис. 6.5 Схема моделі відновлювальних механізмів безпекової діяльності

Основне призначення відновлювальних механізмів полягає у створенні відповідних умов та можливостей для відновлення процесів, цілісності системи та відшкодування за завдані збитки.

Для реалізації відновлювальних механізмів безпекової діяльності необхідно виконувати низку видових функцій безпеки й управління, виконання чи невиконання яких впливає на її ефективність.

Відшкодування збитків, яких зазнала організація, може здійснюватися шляхом використання механізмів страхування, резервного фонду соціальної системи, з огляду на його можливості та інш.

Результатом реалізації відновлюваної складової безпекової діяльності є показники, які відображають її підсумки щодо відновлення робочого стану, процесів чи цілісності об'єктів тощо. Наприклад, такими показниками можуть бути:

- а) страхове відшкодування внаслідок страхового випадку - пожежі;
- б) відшкодування завданих збитків підприємству за рішенням суду;
- в) фінансування заходів з резервного фонду підприємства;
- г) відновлення чи придбання нового замість пошкодженого або знищеного обладнання.

6.5 Видові функції, методи та засоби безпекової діяльності

Видові функції (види) безпекової діяльності – це будь-які види діяльності, які містять інформаційно-виявляючі, попереджувальні, ліквідаційні та відновлювальні механізми, завдяки яким здійснюється безпекова діяльність (функція безпеки соціальної системи).

У практичній діяльності для забезпечення безпеки соціальної системи можуть використовуватися будь-які види діяльності, які дають змогу документувати протиправні дії, отримуюча-

ти інформацію про загрози чи небезпеки, попереджувати та ліквідовувати їх, а у разі реалізації відновлювати діяльність чи цілісність процесів, або компенсувати отриманні збитки. Основними видами безпекової діяльності можуть бути: охоронна діяльність, аналітично-пошукова діяльність, детективна діяльність, страхування, юридичний захист, судовий захист, охорона праці, технічний захист інформації з обмеженим доступом, страхування та ін., а також управлінські загальні функції планування, організування, контроль.

Метод – це спосіб, що охоплює певний алгоритм дій. У безпековій діяльності методи потрібні для виконання її видових функцій.

Методи безпекової діяльності – це способи, за допомогою яких реалізуються засоби безпеки у межах виконання відповідних видових функцій безпеки. Тобто, методи безпеки переводять засоби безпеки зі статичного стану в динамічний. Наприклад, відеокамера як засіб може бути використана лише за умови, якщо у безпековій діяльності застосовуватиметься метод відеоспостереження.

Методів безпекової діяльності може бути багато. Проте до безпекових їх можна віднести лише тоді, коли їхнє використання дозволяє отримати інформацію про загрози й небезпеки, попереджувати виникнення чи реалізацію загроз, або припиняти негативну дію загроз, ліквідовувати їх негативні наслідки. Наприклад, аналіз виробничих показників на підприємстві можна проводити для того, щоб ухвалити рішення щодо покращення та розвитку виробничого процесу, або виявлення загроз, які можуть його дестабілізувати. У першому випадку цей метод використовується для удосконалення виробництва, у другому – для уникнення його руйнування та збереження цілісності.

Методи, які можуть використовуватися у безпековій діяльності можна об'єднати в такі групи:

- 1) адміністративно-організаційні;
- 2) інформаційно-аналітичні;
- 3) економічні;
- 4) правові;

- 5) технічні;
- 6) соціально-психологічні.

Адміністративно-організаційні методи – група методів, які використовуються для впорядкування безпекової діяльності у логічно структуровану та створення відповідного організаційного механізму забезпечення безпеки соціальної системи.

Методи цієї групи здійснюють організаційний вплив на безпекову діяльність. Наприклад, створення адекватної організаційної структури безпеки підприємства; визначення функцій та обов'язків кожної ланки та підрозділу із забезпечення безпеки; створення системи контролю, яка б попереджувала завдання збитків, зокрема й співробітниками; організацію системи навчання співробітників, котрі забезпечують процес безпеки соціальної системи тощо.

Інформаційно-аналітичні методи – це група методів, що передбачають механізми збору, обробки й аналізу інформації та дають змогу кваліфікувати дестабілізуючі чинники у загрози чи небезпеки, а також визначати рівень безпеки організації.

Методи цієї групи використовуються для забезпечення відповідною інформацією для ухвалення управлінських рішень щодо забезпечення безпеки соціальної системи. Наприклад, спеціальні методи проведення детективної діяльності: приховане спостереження; відкрите та зашифроване опитування; наведення довідок; вивчення предметів і документів; зовнішній та внутрішній огляд будівель, приміщень та інших об'єктів.

Економічні методи – це методи, які дозволяють оцінювати економічний стан соціальної системи погляду безпеки, ідентифікувати загрози економічного характеру, припиняти дію загроз чи небезпек і ліквідовувати їх наслідки, відновлювати втрати.

Ці методи включають моніторинг, контроль та аналіз виробничих, фінансових та регулятивних показників роботи організації, які впливають на безпеку, аналіз ризиків; визначення індикаторів економічної безпеки; методи страхування та кредитування для компенсації втрат, відновлення діяльності та ін.

Правові методи – це способи юридичного й судового захисту корпоративних інтересів соціальної системи та формування нормативно-правових документів, які регламентують її внутрішню діяльність, зокрема з питань безпеки.

Ці методи формують правові механізми безпекової діяльності, організації її у формі системи безпеки.

Технічні методи – це способи технічного захисту засобів обчислення інформації, телекомунікаційних мереж та технологій виробництва. Наприклад, відеоспостереження, підслуховування за допомогою так званих «жучків», криптологічний захист інформації тощо.

Соціально-психологічні методи – способи психологічного впливу на потенційні чи конкретні особи (джерела) з метою отримання інформації про можливі загрози, їх попередження чи припинення. Наприклад, переконання позичальника добровільно повернути борг, не доводячи справу до суду.

У процесі безпекової діяльності для реалізації того чи іншого методу використовуються відповідні засоби.

Засоби забезпечення безпеки – це можливості, інструменти матеріального і нематеріального характеру, за допомогою яких здійснюється безпекова діяльність.

У підсумку вони впливають на самодостатність та стійкість соціальної системи. Цікавим є те, що деякі сили одночасно можуть використовуватися і як засоби безпеки. Відтак особи, які здійснюють фізичну охорону підприємства, або супроводження вантажів (будучи силами забезпечення безпеки), окрім застосування таких засобів охорони як зброя, спеціальні пристрої, мають право застосовувати власну фізичну силу для затримання порушників. У цій якості вони виступають засобом забезпечення безпеки.

Засобів безпеки, що можуть використовуватися суб'єктами і силами безпеки, існує безліч. Викласти вичерпний їх перелік неможливо та й недоцільно. Проте їх можна виокремити в певні групи, основними з яких є:

1. *Технічні засоби* – це засоби які мають технічні можливості чи властивості для протидії загрозам. Це системи

сигналізації, контролю, різноманітні автоматичні та механічні пристрої тощо. Наприклад, відеокамери, засоби перевірки автотранспорту на наявність вибухівки, комп'ютерні програми та програмні продукти, спеціально обладнані автомобілі тощо. Вони використовуються для виключення можливості здійснення крадіжок, знищення матеріальних цінностей, проникнення в інформаційні системи, викрадення персоналу тощо.

2. *Технологічні засоби* – це засоби, що забезпечують унікальність продукту або послуги, унеможливають його копіювання чи підробку. Такими засобами можуть бути: технології виробництва, голографічний захист та ін.

3. *Економічні засоби* – економічні відносини з державними структурами, юридичними і фізичними особами з метою забезпечення конкурентоспроможності, а також фінансово-матеріальні ресурси – гроші, цінні подарунки та ін., які використовуються здебільшого під час отримання інформації через агентурні джерела та зв'язки в органах влади, контрольних органах у цілях детективної діяльності та забезпечення безпеки.

4. *Правові засоби* – це засоби, які містять правові механізми безпекової діяльності у вигляді законів та нормативно-правових документів.

Правові засоби розробляються та використовуються у безпековій діяльності на двох рівнях:

1) на загальнодержавному (закони та підзаконні нормативні акти з питань безпеки, та такі, що використовуються у безпековій діяльності.)

2) на рівні самого підприємства (накази, стратегії безпеки, концепції безпеки, порядок здійснення охоронних та профілактичних дій та ін.).

5. *Інформаційні засоби* – інформаційні й аналітичні матеріали, наукові розробки, публікації, комп'ютерні технології, журнали тощо з питань безпеки, а також комунікаційний зв'язок підприємства з громадськістю, владою, засобами масової інформації, працівниками й акціонерами.

6. *Фізичні засоби* – це засоби, що використовуються для фізичної охорони об'єктів, а також застосування фізичної сили під час затримання правопорушників.

7. *Організаційно-управлінські засоби* – це структури, процедури, режими, що обмежують або виключають можливість завдання економічних збитків акціонерному товариству.

8. *Службові тварини* – застосовуються для фізичної охорони об'єктів безпеки і для пошуку певних предметів та осіб.

Питання та завдання для самоконтролю

1. Сутність, структура та загальна характеристика безпекової діяльності.

2. Розкрийте зміст інформаційно-оперативних механізмів безпекової діяльності на конкретному прикладі.

3. Розкрийте зміст попереджувально-профілактичних механізмів безпекової діяльності на конкретному прикладі.

4. Розкрийте зміст ліквідаційно-відновлювальних механізмів безпекової діяльності на конкретному прикладі.

5. Розкрийте сутність видових функцій безпекової діяльності на конкретному прикладі та наведіть їх види.

5. Наведіть класифікацію методів безпекової діяльності та розкрийте їх сутність й практичне використання на конкретному прикладі.

6. Наведіть класифікацію засобів безпекової діяльності та розкрийте їх сутність й практичне використання на конкретному прикладі.

Тести

1. Діяльність, спрямована на протидію загрозам з метою захисту корпоративних інтересів, збереження цілісності процесів чи системи та сприяння її розвитку на основі засвоєння та розвитку безпекової культури – це:

- а) репродуктивна діяльність системи безпеки організації;
- б) безпекова діяльність;

- в) функція безпеки організації;
- г) правильні відповіді б і в.

2. Взаємодія суб'єктів і сил безпеки та системне застосування ними видових функцій, методів, засобів та принципів безпеки для забезпечення безпеки організації – це:

- а) механізм безпекової діяльності;
- б) технологія безпекової діяльності;
- в) режим безпекової діяльності;
- г) правильні відповіді а, б.

3. Конкретні напрями чи види діяльності, які необхідно виконувати, щоб протидіяти потенційним чи реальним внутрішнім і зовнішнім загрозам та зберігати цілісність процесів чи об'єктів – це:

- а) методи безпекової діяльності;
- б) засоби безпекової діяльності;
- в) видові функції безпекової діяльності;
- г) правильні відповіді а, б.

4. Можливості та інструменти матеріального і нематеріального характеру, за допомогою яких реалізуються видові функції безпекової діяльності, – це:

- а) методи безпекової діяльності;
- б) засоби безпекової діяльності;
- в) завдання безпекової діяльності;
- г) правильні відповіді а, в.

5. Які з поданих нижче механізмів належать до безпекової діяльності?

- а) інформаційно-виявляючі;
- б) попереджувально-профілактичні;
- в) ліквідаційні;
- г) усі відповіді правильні.

6. Безпекова діяльність організації, що пов'язана зі збором і аналізом інформації про загрози та документування протиправних дій у відповідному часі та просторі містить механізми:

- а) інформаційно-виявляючі;
- б) попереджувально-профілактичні;

- в) ліквідаційно-відновлювальні;
- г) усі відповіді правильні.

7. Які з наведених видів діяльності не належать до змісту інформаційно-виявляючих безпекових механізмів організації?

- а) вчасне документування протиправних дій;
- б) отримання або передання відповідним керівникам, структурам чи виконавцям заходів безпеки інформації про потенційні чи реальні загрози;
- в) запровадження в організації пропускового режиму;
- г) документування фактів протиправних дій.

8. Результатом виконання інформаційно-виявляючих безпекових механізмів є конкретна інформація про загрози:

- а) про виведення з ладу виробничих засобів;
- б) про порушення технологічних процесів;
- в) про підготовку технологічних аварій, пожеж, учинення інших надзвичайних дій;
- г) усі відповіді правильні.

9. Безпекова діяльність системи безпеки, що пов'язана з розробкою та дотриманням законів, підзаконних актів з питань безпеки, а також нормативів безпеки та інших управлінських рішень, від режиму до регламентації поведінки працівників підприємства містить механізми:

- а) інформаційно-виявляючі;
- б) попереджувально-профілактичні;
- в) ліквідаційно-відновлювальні;
- г) аналітично-інформаційні.

10. Який з наведених видів діяльності не належить до змісту попереджувально-профілактичних механізмів?

- а) нормативно-правове забезпечення та створення відповідних антимотиваційних умов з питань безпеки;
- б) патрулювання охоронниками території підприємства;
- в) контроль за використанням товарно-матеріальних цінностей;
- г) зв'язок з іншими структурами безпеки.

11. Які з наведених документів є результатом реалізації попереджувально-профілактичної функції?

- а) правила техніки безпеки на виробництві;
- б) правила роботи з вхідною документацією;
- в) план дій на випадок надзвичайних подій на виробництві;
- г) правильні відповіді а, в.

12. Механізми діяльності, що пов'язані з ліквідацією (припиненням) загроз на будь-якій стадії реалізації конфіденційними методами та методами роботи у надзвичайних ситуаціях, а також їх наслідків та/чи відновленням якісних чи кількісних показників, зв'язків, цілісності об'єкта, діяльності тощо – це механізми:

- а) інформаційно-оперативні;
- б) попереджувально-профілактичні;
- в) ліквідаційні та відновлювальні;
- г) аналітично-інформаційні.

13. Який з наведених видів діяльності не відноситься до змісту відновлювальних механізмів безпекової діяльності?

- а) відшкодування збитків, яких зазнала організація шляхом використання механізмів страхування;
- б) проведення внутрішньої експертизи нормативних документів;
- в) повернення через суд авторських прав організації;
- г) добровільне відшкодування працівником завданих збитків організації.

14. Які з наведених показників є результатом реалізації ліквідаційних механізмів безпекової діяльності?

- а) призупинення випуску бракованої продукції;
- б) екологічні вимоги до процесу виробництва та продукту;
- в) ліквідація умов і причин профзахворювання;
- г) правильні відповіді а, в.

Тема 7

МЕТОДОЛОГІЯ БЕЗПЕКОВОЇ ДІЯЛЬНОСТІ СОЦІАЛЬНОЇ СИСТЕМИ

*Методологія – шлях до пізнання світу,
зокрема й безпекової дійсності.
Той, хто його пізнав, має реальні можливості
щодо використання його скритих потенційних резервів
та впливу на нього з метою зміни негативного
безпекового потенціалу*

7.1 Сутність поняття «методологія»

Методологія – складний феномен, через який відображається специфіка пізнавального процесу. Вона є складною для сприйняття не тільки практичними працівниками та фахівцями, які не займаються професійно науковою діяльністю, а й у науковому середовищі.

Необхідність удосконалення методології безпеки підприємства зумовлена ускладненням й динамізмом об'єкта пізнання – безпекової реальності, а також самого процесу наукового пізнання.

Методологія тривалий час розглядалася у вузькому розумінні лише як учення про методи діяльності (метод і «логос» – вчення). Таке розуміння методології обмежувало її предмет аналізом методів [36, с. 32–40].

Інша крайність у трактуванні поняття «методологія» полягає у тому, що традиційно склалося уявлення, що методологія стосується лише науки, наукової діяльності. У цьому аспекті методологія (від грецьк. *metodos* – спосіб, метод і *logos* – наука, знання) розглядається як вчення про правила мислення у процесі створення науки, проведення наукових досліджень. Під методологією науки зазвичай розуміється вчення про науковий метод пізнання або систему наукових принципів, на яких ґрунтується дослідження і здійснюється вибір засобів, прийомів і методів пізнання [28, с. 72].

На сучасному етапі поняття «методологія» трактується як:

а) вчення про структуру, логічну організацію, методи та засоби діяльності [3, с. 795];

б) вчення про структуру, логічну організацію методів і засобів діяльності; вчення про принципи побудови, форми і способи наукового пізнання [3, с. 801];

в) система принципів і способів організації та побудови теоретичної і практичної діяльності, а також вчення про цю систему [49, с. 250];

г) сукупність підходів, способів, прийомів та процедур, що застосовуються в процесі наукового пізнання та практичної діяльності для досягнення наперед визначеної мети [1, с. 171];

г) система визначених способів і прийомів, що застосовуються у тій або іншій сфері діяльності (в науці, політиці, мистецтві тощо), вчення про цю систему, загальна теорія методу, теорія в дії [38, с. 185];

д) вчення про структуру, логічну організацію, методи, засоби і форми діяльності дослідника в процесі пізнання ним досліджуваних явищ [21, с. 11–125];

е) система принципів і засобів організації та формування теоретичної і практичної діяльності [39, с.11];

є) дисципліна про загальні принципи і форми організації мислення і діяльності [31, с. 323].

Розглядаючи структуру методології науки, вчені розділили її на чотири рівні: філософський (застосовується у загально-філософських дослідженнях); загальнонауковий (аналіз найзагальніших результатів, отриманих в різних галузях наукового знання); конкретно-науковий (методологія конкретних наук: фізики, біології, психології та ін.); технологічний (конкретні методики та техніка дослідження) [36, с. 32–40].

Такий підхід до поділу методології на рівні був визнаний у середовищі методологів. Він цілком може бути застосованим й до такої науки, як безпекознавство (наука у сфері безпеки організації), що сьогодні активно розвивається в Україні.

Однак наукова діяльність – це така ж як і інші професійні види діяльності людини, зокрема й ті, що належать до практики. На них також має поширюватися поняття «методологія практичної діяльності», зокрема й «методологія забезпечення безпеки суб'єкта господарювання» або «методологія безпекової діяльності».

Підтвердженням такої думки є формування наукового напрямку під назвою «системо-мислєдіяльнісна» методологія [54, с. 42]. Позитивним у цьому підході є те, що знати основи методології та вміти користуватися нею повинен кожен учений і спеціаліст-практик.

7.2 Безпекова діяльність як об'єкт та метод пізнання

З наведених визначень поняття «методологія» зрозуміло, що серед вчених немає одностайності щодо розуміння його сутності та змісту. Крім того, практична діяльність, як і науково-дослідницька, потребує відповідної методології, внаслідок чого почав формуватися новий напрям – методологія практичної діяльності. Їх слід розглядати сукупно, тобто будь-яка практична діяльність, якщо вона осмислена суб'єктом, охоплює науково-теоретичні компоненти. А будь-яке наукове дослідження щонайменше в емпіричній частині буде вмещувати практичні компоненти. Отже, основним під час розгляду поняття методології є наукова і практична діяльність. Діяльність – форма активного ставлення до довкілля, а її зміст становить доцільність зміни і перетворення цього світу на основі засвоєння та розвитку культури [48, с. 254].

Діяльність може поділятися на репродуктивну й продуктивну [19, с. 189].

Репродуктивна діяльність – це діяльність, що заснована на попередньому досвіді на рівні засвоєних технологій. Така діяльність використання методології не потребує.

Продуктивна діяльність – це діяльність, що спрямована на отримання нового результату чи нових знань і потребує відповідного впорядкування, логічної її організації тощо, тобто виникає необхідність у застосуванні методології. Безпека як функція, діяльність суб'єкта щодо забезпечення безпеки (безпекова діяльність) організації є продуктивною діяльністю.

Безпекова діяльність – форма активного ставлення суб'єктів безпеки до безпекової дійсності, зміст якого полягає у проведенні в ній відповідних змін і перетворень на основі засвоєння та розвитку безпекової культури.

Поняття «діяльність» має дуже важливу методологічну властивість, яка полягає у тому, що «діяльність», з одного боку, є об'єктом пізнання, а з іншого, – виступає його методом. Від

рівня пізнання суб'єктом стану об'єкта безпеки, внутрішніх і зовнішніх щодо нього загроз, можливостей й механізмів протидії їм залежить якість ухвалення рішень у сфері безпеки.

Зміст, механізми та форми процесу пізнання продуктивної наукової та практичної безпекової діяльності подані на рисунку 7.1.

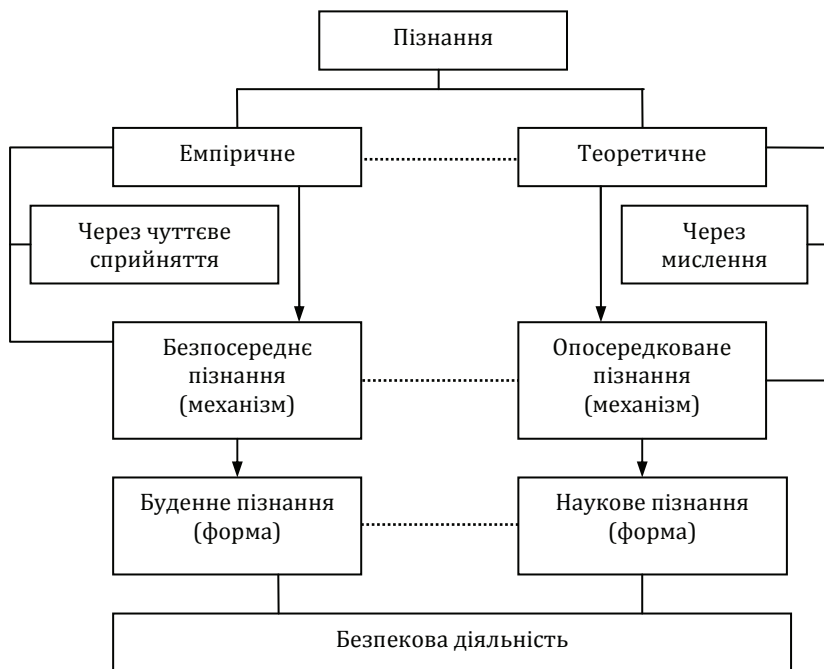


Рис. 7.1 Зміст, механізми та форми процесу пізнання продуктивної наукової та практичної безпекової діяльності

Пізнання – це процес активного, цілеспрямованого, категоріального відображення дійсності свідомістю людини [48, с. 669], що виявляється у вигляді емпіричного й теоретичного пізнання, які взаємопов'язані. Цей процес відбувається шляхом абстрагування суб'єктом пізнання від емпіричних даних з подальшим поверненням на емпіричний рівень, оскільки саме він дає змогу зробити висновок про істинність або хибність отриманих знань.

Емпіричне пізнання – це пізнання, яке досягається здебільшого за допомогою органів чуття. Це нижчий рівень пізнавального процесу, що спрямований на виявлення та опис фактів, накопичення первинної інформації про явище, яке пізнається зазвичай за допомогою емпіричних методів пізнання. Він менше впорядкований, та не вимагає абстрагування.

Основний зміст емпіричного пізнання у сфері безпеки полягає у такому:

- 1) встановленні реальності досліджуваних об'єктів у сфері безпеки суб'єкта господарювання;
- 2) виявленні, уточненні та класифікації загроз, їхніх якісних й кількісних характеристик;
- 3) виявленні залежностей між подіями, явищами, поведінкою людей тощо у сфері безпеки підприємства та конкретних умов, у яких вони виявляються;
- 4) розробці та застосуванні точних способів опису фактів тих чи інших загроз, а також залежностей між подіями, явищами, поведінкою людей тощо у сфері безпеки підприємства.

Теоретичне пізнання – це вище відображення дійсності за допомогою абстрактного мислення й дослідження, у процесі якого виділяються істотні властивості або сторони об'єкта, виявляються об'єктивні закономірності, зв'язки та тенденції його розвитку, недоступні для чуттєвого пізнання.

Основний зміст теоретичного пізнання у сфері безпеки полягає у:

- 1) виявленні та вивченні конкретних причин, зв'язків, залежностей, взаємодій, процесів, які дають змогу пояснити факти виникнення й дії загроз, порушення цілісності процесів й об'єктів;
- 2) абстрагуванні від безпосередньо спостережуваних характеристик, висуванні й обґрунтуванні гіпотез, які дають можливість пояснити причини, процеси або механізми, встановлених фактів виникнення загроз, порушення цілісності процесів й об'єктів;
- 3) формулюванні теоретичних висновків у сфері безпеки організації.

Розглядаючи емпіричне й теоретичне пізнання сфери безпеки організації, необхідно зауважити, що в їх основі є відповідно, механізми безпосереднього та опосередкованого пізнання. Відтак емпіричне пізнання реалізується через безпосереднє чуттєве сприйняття безпекової дійсності, а теоретичне – шляхом логічного розмірковування, умовиводів, використовуючи водночас результати власного особистого досвіду та знання інших людей у безпековій сфері, тобто опосередковано за допомогою мислення.

Пізнання діяльності, пов'язаної з забезпеченням безпеки організації, може здійснюється у буденній або науковій формі. Ці форми об'єднує те, що вони є процесом, що спрямований на досягнення істинного знання про безпекову дійсність в організації, проте різняться способами й засоби досягнення цих знань.

Для буденного пізнання характерними ознаками є:

1) зв'язок з буденною практичною діяльністю у сфері безпеки;

2) стихійність у формуванні уявлень про об'єктивну безпекову дійсність.

Отже, практичне мислення, тобто буденне пізнання не дає змоги суб'єктам досягнути внутрішні закономірності, зв'язки й відносини у сфері забезпечення безпеки суб'єкта господарювання.

Науковому пізнанню властиві такі ознаки:

1) цілеспрямованість, послідовність й систематичність відображення безпекової дійсності та її об'єктивності у доказовій формі;

2) самостійність у процесі діяльності, пов'язаної з забезпеченням безпеки організації;

3) методичність та раціональність процесів пізнання сутності процесів, явищ та безпекової дійсності щодо організації.

Окреслене свідчить, що основним під час розгляду поняття «методологія» є процес пізнання продуктивної діяльності, якою є наукова і практична діяльність, що, зокрема, й пов'язана з забезпеченням безпеки організацій.

7.3 Структура методології безпеки організації

Будь-яка методологія, якщо розглядати її як учення про систему наукових принципів, має трирівневу структуру, утворену з фундаментальних (загальнонаукових), міждисциплінарних і конкретних принципів. Фундаментальними принципами, що забезпечують отримання достовірних результатів наукового дослідження, є принципи: детермінізму, системності та розвитку [44, с. 23]. Використання їх у безпекознавстві має такий зміст:

1) *принцип детермінізму*: встановлює причинно-наслідкові зв'язки всіх явищ безпекової дійсності;

2) *принцип системності*: передбачає встановлення взаємопов'язаних елементів, які формують цілісне утворення, тобто систему;

3) *принцип розвитку*: визнає безперервні зміни, перетворення в усіх предметах і явищах безпекової дійсності в часі та просторі, внаслідок яких здійснюється їх перехід від одних форм і рівнів до інших.

Крім того, в значній кількості визначень поняття «методологія» вчені вважають, що змістовною його стороною є: вчення, тобто сукупність теоретичних положень про структуру діяльності та логічну організацію діяльності.

Логічна організація діяльності – це цілеспрямована активність людини з метою упорядкування її в цілісну систему з чітко визначеними характеристиками (логічно структуровану). Логічна структура включає такі компоненти: суб'єкт, об'єкт, предмет, форми, засоби, методи діяльності, її результат. Зовнішніми щодо цієї структури є характерні ознаки, відображені в особливостях, принципах, умовах, нормах. За такого підходу методологію можна розглядати як вчення про організацію будь-якої людської діяльності: наукової, практичної тощо [36, с. 32–40].

Методологія сучасного безпекознавства, зокрема й безпекової діяльності, є цілісним утворенням з вертикальними та горизонтальними зв'язками (рис. 7.2). Реалізація її на тому чи іншому вертикальному рівні потребує відповідного компоненту чи компонентів на горизонтальному. Наприклад, для застосу-

вання методології на світоглядному рівні необхідно обрати серед існуючих, або сформувати новий домінуючий безпековий світогляд та тип безпекового мислення. У такий спосіб створюється ідеальна модель методології безпеки на основі її вертикальних і горизонтальних структурних компонентів та зв'язків між ними.

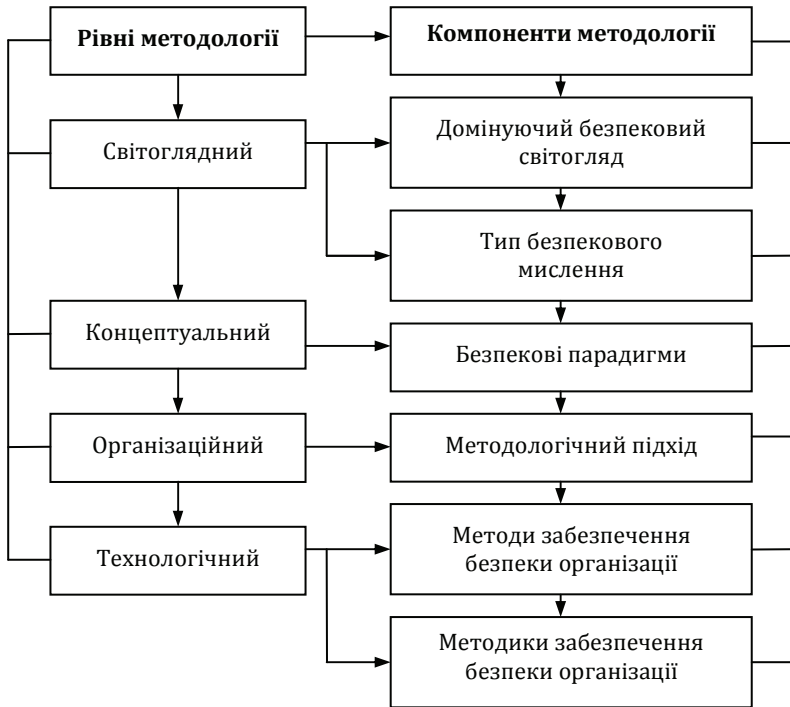


Рис. 7.2 Структура моделі методології безпеки організації

При вертикальній структурі методологію безпекознавства можна використовувати на чотирьох рівнях:

- світоглядному, на якому безпека розуміється як форма світогляду й складова корпоративної культури та визначаються основні напрями і загальні принципи наукового пізнання загалом;
- концептуальному, на якому формується загальне розуміння безпеки та бачення як забезпечити безпеку суб'єкта господарювання;

– організаційному, на якому вивчаються й визначаються структурні елементи процесу чи системи безпеки суб'єкта господарювання та зв'язків між ними;

– технологічному, на якому зводиться у єдиний процес всі елементи (функції, методи, засоби, принципи тощо), тобто здійснюється весь механізм забезпечення безпеки суб'єкта господарювання.

Між наведеними рівнями методології безпекознавства існують органічний зв'язок, залежність, підпорядкованість.

Для горизонтальної структури методології безпекознавства доцільно віднести такі її компоненти:

– *домінуючий безпековий світогляд* – це сукупність уявлень про життєдіяльність людей в умовах дії різних загроз та небезпек. Він впливає на формування типу домінуючого безпекового та наукового мислення;

– *тип безпекового мислення* – сукупність взаємозалежних і взаємообумовлених ідей, принципів, норм, форм пізнання й відображення безпекової дійсності;

– *безпекові парадигми* – усталені підходи до розуміння та вирішення теоретичних і практичних питань, пов'язаних із забезпеченням безпеки підприємства. Розрізняють дві парадигми безпеки: парадигма захищеності та парадигма самоствердження [41, с. 222–227]. Їх сутність полягає у такому: парадигми захищеності – «Я перебуваю у безпеці тому, що своєчасно виявляю та попереджую небезпеку», а парадигми самоствердження – «Я перебуваю у безпеці не тому, що не існує загроз, а тому, що Я сильний настільки, що вони не становлять для мене небезпеки». Ці парадигми у сучасному світі вже не є ефективними, прикладом чого можуть бути: СРСР, який дотримувався парадигми захищеності, та США, які застосовують парадигму самоствердження. Тому потрібна інтегруюча, тобто парадигма самозбереження та розвитку, сутність якої полягає у такому: «Я перебуваю у безпеці тому, що Я вмію протидіяти загрозам і небезпеці, зберігати цілісність та за допомогою цього створювати умови для розвитку, у зв'язку з чим Я сильний»;

– *методологічний підхід* – об'єднані домінуючим методом взаємозалежні методи, теорії та інші наукові знання про безпекову дійсність та її забезпечення;

– *методи* (від грецьк. *methodos* – шлях дослідження, теорія, вчення) – впорядковані способи пізнання й формування знання про безпекову реальність та забезпечення безпеки суб'єкта господарювання;

– *методика забезпечення безпеки* – сукупність конкретизованих, формалізованих, адаптованих до предмета і завдань забезпечення безпеки підприємства процедур, засобів, техніки і прийомів збирання, обробки й узагальнення інформації та протидії загрозам.

Наведені підходи до змісту методології, характеристики її структурних компонентів тощо є вченням, тобто теоретичними положеннями про:

1) пізнання, тобто процес активного, цілеспрямованого, категоріального відображення безпекової дійсності свідомістю суб'єктами безпеки під час організації безпеки організації;

2) загальне бачення діяльності, пов'язаної з забезпеченням безпеки підприємства та її логічної структури – основних її складових;

3) упорядкування діяльності, пов'язаної з забезпеченням безпеки організації в логічно структуровану, тобто в цілісну систему з чітко визначеними характеристиками та зв'язками. Логічна структура організації безпеки як діяльності передбачає такі компоненти: суб'єкт, об'єкт, предмет (функції), методи, засоби, форми, та принципи.

Отже, ***методологія безпеки організації*** – це вчення (сукупність теоретичних положень) про пізнання безпекової дійсності, загальне бачення безпекової діяльності та упорядкування її у систему.

Питання і завдання для самоконтролю

1. Розкрийте підходи до визначення сутності поняття «методологія».

2. Дайте визначення поняттям «діяльність», «безпекова діяльність». Поясніть чому діяльність є одночасно об'єктом і методом пізнання.

3. Розкрийте сутність продуктивної і репродуктивної діяльності.

4. Дайте визначення поняття «пізнання» та наведіть структуру процесу пізнання безпекової діяльності.

5. Охарактеризуйте емпіричне й практичне пізнання безпекової діяльності.

6. Розкрийте зміст наукового й буденного пізнання безпекової діяльності.

7. Поясніть роль фундаментальних наукових принципів та логічної організації діяльності у формуванні методології безпеки соціальної системи.

8. Розкрийте сутність та структуру методології безпеки організації, дайте її загальну характеристику.

9. Наведіть рівні методології безпеки соціальної системи та розкрийте їх зміст.

10. Наведіть компоненти методології безпеки соціальної системи та розкрийте їх зміст.

Тести

1. Методологія – складний феномен, через який відображається специфіка пізнавального процесу:

- а) наукової діяльності;
- б) практичної діяльності;
- в) наукової й практичної діяльності;
- г) репродуктивної діяльності.

2. Які з наведених визначень поняття «методологія» належать до методології наукової діяльності?

- а) сукупність прийомів дослідження, що застосовуються в тій або іншій науці;
- б) вчення про метод пізнання і реформування світу;
- в) система принципів і способів організації та формування теоретичної і практичної діяльності, а також вчення про цю систему;
- г) правильні відповіді а, б.

3. Які з наведених визначень поняття «методологія» належать до сучасних?

а) система принципів і засобів організації та формування теоретичної і практичної діяльності;

б) сукупність підходів, способів, прийомів та процедур, що застосовуються в процесі наукового пізнання та практичної діяльності для досягнення наперед визначеної мети;

в) вчення про структуру, логічну організацію, методи та засоби діяльності;

г) усі відповіді правильні.

4. Форма активного ставлення суб'єктів безпеки до безпекової дійсності, зміст якого полягає у проведенні в ній відповідних змін і перетворень на основі засвоєння та розвитку безпекової культури – це:

а) принцип безпекової діяльності;

б) критерій формування методології безпеки;

в) безпекова діяльність;

г) парадигма безпеки.

5. Діяльність, що спрямована на отримання нового результату чи нових знань і потребує відповідного впорядкування, логічної її організації тощо, – це:

а) репродуктивна діяльність;

б) продуктивна діяльність;

в) репродуктивна й продуктивна діяльність;

г) жодна відповідь не правильна.

6. Відображення дійсності за допомогою абстрактного мислення й дослідження, у процесі якого виокремлюються істотні властивості або сторони об'єкта, виявляються об'єктивні закономірності, зв'язки та тенденції його розвитку, недоступні для чуттєвого пізнання, – це:

а) теоретичне пізнання;

б) практичне пізнання;

в) емпіричне пізнання;

г) усі відповіді не правильні.

7. Які з поданих характерних ознак відображають зміст теоретичного пізнання у сфері безпеки:

а) встановлення реальності досліджуваних об'єктів у сфері безпеки суб'єкта господарювання;

б) абстрагування від безпосередньо спостережуваних характеристик, висування і обґрунтування гіпотез, які дають можливість пояснити причини, процеси або механізми, встановлених фактів виникнення загроз, порушення цілісності процесів й об'єктів;

в) розробка і застосування точних способів опису фактів тих чи інших загроз, а також залежностей між подіями, явищами, поведінкою людей тощо у сфері безпеки підприємства;

г) виявлення залежностей, між подіями, явищами, поведінкою людей тощо у сфері безпеки підприємства та конкретних умов, у яких вони виявляються.

8. Які з поданих характерних ознак відображають зміст емпіричного пізнання у сфері безпеки:

а) виявлення і вивчення залежностей, взаємодій, процесів, які дають змогу пояснити факти порушення цілісності процесів й об'єктів;

б) виявлення причин і зв'язків, які дають змогу пояснити факти виникнення й дії загроз;

в) виявлення, уточнення і класифікація загроз, їхніх якісних й кількісних характеристик;

г) формулювання теоретичних висновків у сфері безпеки організації.

9. За своїм змістом методологія безпеки соціальних систем – це:

а) загальне бачення безпекової діяльності та її логічної структури – основних її складових;

б) упорядкування безпекової діяльності в логічно структуровану, тобто в цілісну систему з чітко визначеними характеристиками та зв'язками.

в) пізнання, тобто процес активного, цілеспрямованого, категоріального відображення безпекової дійсності свідомістю суб'єктами безпеки під час організації безпеки організації.

г) усі відповіді правильні.

10. Вчення (сукупність теоретичних положень) про логічну структуру організації безпекової діяльності – це:

- а) методологічний підхід до безпеки соціальної системи;
- б) парадигми безпеки соціальної системи;
- в) методологія безпеки соціальної системи;
- г) домінуючий безпековий світогляд.

11. Сукупність взаємопов'язаних елементів, необхідних для протидії внутрішнім і зовнішнім загрозам з метою захисту корпоративних інтересів і загалом створення безпечних умов для розвитку та забезпечення цілісності процесів чи об'єктів організації, – це:

- а) організаційна структура системи;
- б) система;
- в) технологія;
- г) правильні відповіді а, в.

12. У таблиці 1 подані рівні та компоненти методології. Для її застосування на тому чи іншому рівні необхідно сформулювати відповідні його компоненти чи компонент, через які вона й реалізується.

Таблиця

Рівні методології	Компоненти методології
Світоглядний Концептуальний Організаційний Технологічний	а) домінуючий безпековий світогляд б) тип безпекового мислення в) безпекові парадигми г) методологічний підхід г) методи забезпечення безпеки організації д) методики забезпечення безпеки організації

У якому з поданих варіантів правильно запропоновано для кожного рівня методології відповідні компоненти?

- а) 1. а, б; 2. г; 3. в; 4. д, е;
- б) 1. а, б; 2. в; 3. г; 4. д, е;
- в) 1. а, в; 2. б; 3. в; 4. д, е;
- г) 1. а, б; 2. г; 3. в, д; 4. е.

13. Сукупність теоретичних положень про пізнання безпекової дійсності, загальне бачення безпекової діяльності та упорядкування її у систему це:

- а) домінуючий безпековий світогляд.
- б) парадигма безпеки соціальної системи;
- в) зміст поняття «методологія безпеки соціальної системи»;
- г) усі відповіді вірні.

Тема 8

СИСТЕМА БЕЗПЕКИ ОРГАНІЗАЦІЇ

*У Всесвіті все взаємопов'язано,
і будь-яка соціальна система, її діяльність
є лише маленькою його частинкою.
Їх потрібно пізнавати у взаємозв'язку
та здійснювати діяльність системно.
Хто володіє мистецтвом системного підходу,
той може розраховувати на успіх.
Особливо коли йдеться про безпеку,
котра як рідина може витекти із посудини,
якщо та має хоч найменшу тріщинку*

8.1 Структура та загальна характеристика системи безпеки організації

Безпекова діяльність – це складна та водночас інтегрована за різними напрямками діяльність, у зв'язку з чим потребує системного підходу. Інакше безпекову діяльність потрібно організувати та здійснювати у формі системи, яка є складною за структурою і зв'язками. Щоб сформувати її оптимальною і ефективно діючою, необхідно застосовувати моделювання.

Моделювання – це відображення будь-яким способом процесів, які відбуваються в реальному об'єкті [10, с. 10] або зразок, макет конструкції чого-небудь, відтворений у зменшеному або збільшеному вигляді.

Модель системи безпеки організації має вирішувати, окрім основного свого завдання – формування наукового системного підходу до забезпечення безпеки, – ще і завдання концентрації та маневрування силами і засобами згідно з визначеними цілями і завданнями з урахуванням змін у характері та інтенсивності загроз, що виникають [5, с. 97].

Серед науковців фактично немає єдиного підходу до створення моделі системи безпеки підприємницьких структур, тобто пропонується набір структурних елементів, які суттєво різняться між собою. Зокрема під системою безпеки підприємства розуміється:

1) система, що включає наукову теорію безпеки, політику і стратегію безпеки засоби і методи забезпечення безпеки і концепцію безпеки підприємства [13].

2) організована сукупність спеціальних органів, служб, засобів, методів заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства, держави від внутрішніх і зовнішніх погроз [24, с. 9];

4) сукупність об'єкта, засобів захисту, нормативної бази та організаційних структур її здійснення [18, с. 215];

5) комплекс принципових моделей забезпечення безпеки персоналу фірми, основних фондів, конфіденційної інформації,

елементами яких є: об'єкт безпеки, об'єкт загроз, джерела загроз, загрози та засоби захисту та ін. [7].

Основним інструментом формування будь-якої системи є організаційна діяльність, під якою розуміється:

1) внутрішня впорядкованість, узгодженість взаємодії більш або менш диференційованих та автономних частин цілого, що обумовлено його побудовою;

2) сукупність процесів та дій, які призводять до виникнення та удосконалення взаємозв'язків між частинами цілого;

3) об'єднання людей, які спільно реалізують певну програму чи мету та які діють на основі процедур та правил [23].

Організовувати діяльність – означає впорядковувати її у цілісну систему з чітко визначеними характеристиками, логічною структурою та процесом її здійснення [16, с. 32–40]. Тобто йдеться про формування таких елементів системи безпеки, які пов'язані між собою і створюють єдине ціле. Водночас вона має функціонувати на досягнення спільної мети, коли кожен з цих елементів виконує свою роль.

Під час формування системи безпеки організації необхідно дотримуватися певних концептуальних вимог:

– *по-перше*, система безпеки підприємства є унікальною на кожному підприємстві, оскільки залежить від рівня розвитку і структури виробничого потенціалу, ефективності його використання і спрямованості виробничої діяльності, кваліфікації кадрів, виробничої дисципліни, від стану навколишнього середовища, виробничих зв'язків підприємства, конкурентного середовища, ризикованості виробництва та ін.

– *по-друге*, система безпеки підприємства є самостійною, відособленою від аналогічних систем інших виробничих одиниць. Але її відособленість є відносною, тому що система безпеки підприємницької діяльності – це складний елемент безпеки більш високого рівня: міста, регіону, країни;

– *по-третє*, система безпеки підприємства є комплексною. Вона покликана забезпечити безпеку економічну, науково-технічну, кадрову, інтелектуальну, екологічну, інформаційну,

фізичну, техногенну, пожежну тощо. Тому до її складу повинні входити відповідні елементи, органи, сили і засоби [8, с. 134–138].

Крім цього, формуючи безпекову систему необхідно виходити з того, що вона як ієрархічна система має певні властивості. Основними з них є:

1) двоїстість якостей елементів в системі – елемент одночасно має індивідуальні та системні якості, чим складніша ієрархічна структура системи, тим вищі її індивідуальні властивості, тим чіткіше вони виступають в над системі, тим менше вона зв'язана з іншими елементами (системами) над системи. На більш низьких рівнях відбувається спрощення елементів (потрібна лише корисна функція);

2) диктат верхніх рівнів над нижніми – основний порядок ієрархії. Самий нижній рівень ієрархії – робочий орган або його робоча частина;

3) нечутливість верхніх рівнів до змін на нижніх, і навпаки – чутливість нижніх рівнів до змін на верхніх. Головне для надсистеми – виконання підсистемою своїх функцій;

4) виокремлення корисних функцій на рівнях ієрархії. Правильно організована ієрархічна структура виокремлює на кожному рівні корисну функцію, ці функції взаємно підсилюються на наступному рівні, при цьому шкідливі функції на кожному рівні або пригнічуються, або до них не додаються нові. Самий верхній рівень ієрархії виконує зазвичай лише стратегічні та узгоджувальні функції. При цьому, чим вищий рівень ієрархії, тим більш гнучкою є структура, менш жорсткі зв'язки між елементами, легше переставляти їх та замінювати. На нижніх рівнях більш жорстка ієрархія та зв'язки.

Системний підхід дозволяє формувати безпекову систему як цілісний соціальний організм, не концентруючи уваги на окремих її підсистемах та елементах. Бо навіть найкраще функціонування окремих із них ще не гарантує ефективного функціонування всієї системи в цілому, оскільки завжди існує взаємодія між її складовими. Разом з тим, необхідно брати до уваги, що будь-яка соціальна система може ефективно функціонувати за такої умови: 1) цілісності системи; 2) обмеженої автоном-

ності елементів системи та їх дій; 3) внутрішньої і зовнішньої активності системи.

Ці ж вимоги рівнозначно є справедливими й до системи безпеки організації. У процесі функціонування безпекова система виступає як цілісне утворення, у якому існує взаємозв'язок між її структурою та функціями. Безпекова функція реалізується структурою у процесі чого відбувається функціональний дійовий безпековий ефект завдяки поєднанню дій безпекових елементів системи (рис. 8.1).

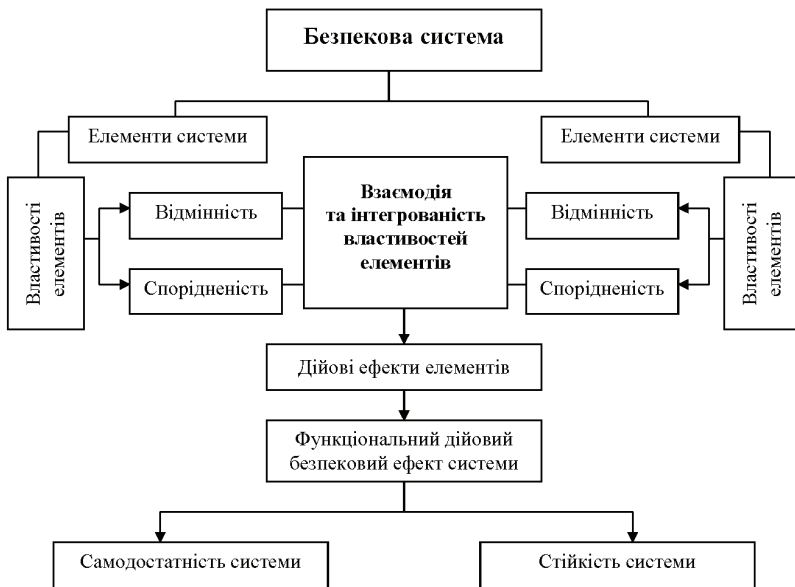


Рис. 8.1 Сутність функціонального дійового безпекового ефекту безпекової системи

Це поєднання базується на взаємодії та інтегрованості основних властивостей елементів: спорідненості та відмінності. В кінцевому результаті система набуває функціонального дійового безпекового ефекту у формі стійкості та самодостатності системи. У такий спосіб безпекова система ро-

бить те, що за жодних обставин не може зробити кожен її елемент окремо. Таким чином, діяльність безпекової системи є постійними відтворенням функціонального дійового безпекового ефекту.

Безпекова система може мати будь-яку кількість елементів. Але вони мають бути такими, що відповідають основній меті системи, а їх кількість такою, щоб вистачало для реалізації цієї мети.

Система безпеки організації – це сукупність взаємопов'язаних елементів, що має властивості, відмінні від властивостей структурного елемента, необхідних для протидії загрозам з метою захисту корпоративних інтересів і загалом створення безпечних умов для розвитку та забезпечення цілісності процесів, об'єктів та підприємства.

Безпекова діяльність, організована у формі системи, має охоплювати основні елементи, які дають можливість здійснювати її ефективно (рис. 8.2).

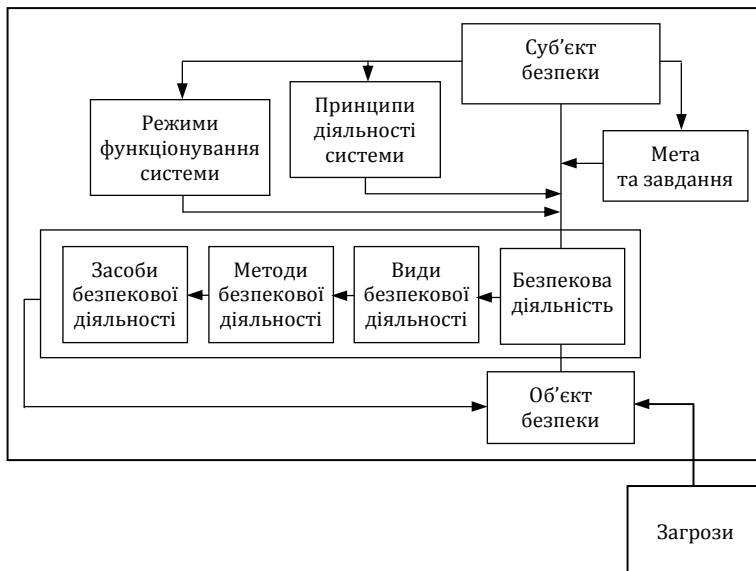


Рис. 8.2 Система безпеки організації

Безпекова діяльність як система поділяється на три блоки: *вхід, процес перетворень, вихід*. На вході система отримує те, що дозволить після відповідних перетворень забезпечити запланований результат. Водночас у реальній життєдіяльності організації є багато різних обмежень, які слід брати до уваги при організації й управлінні системою безпеки. Схематично цей процес відображено на рисунку 8.3.

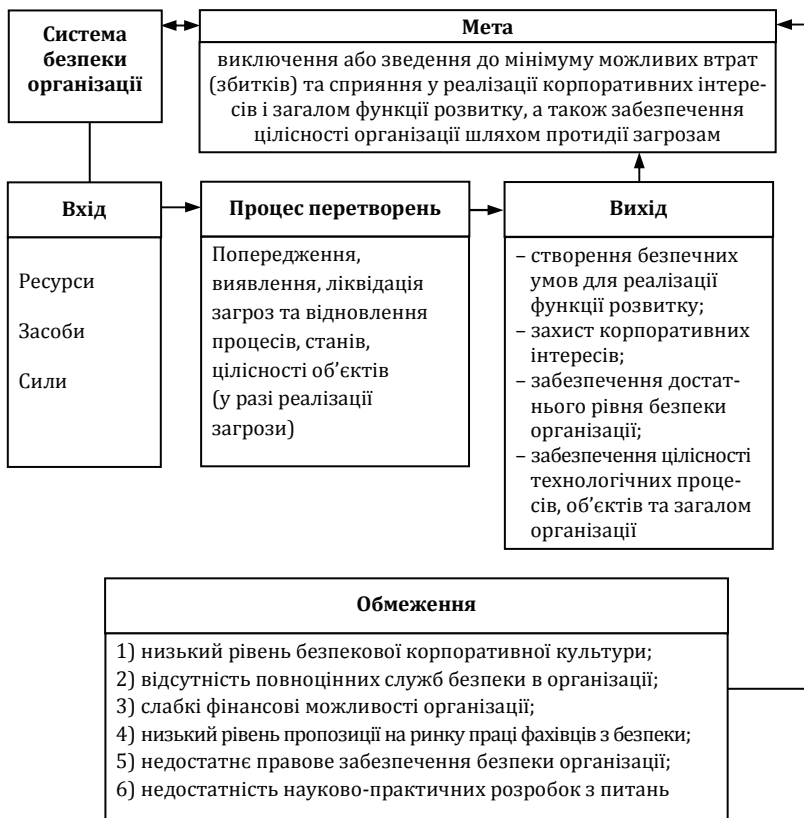


Рис. 8.3 Операційна модель системи безпеки організації

8.2 Цілі та завдання системи безпеки організації

Ціль – це не стільки те, що людина реалізує у своїй повсякденній діяльності, скільки те, що вона має реалізовувати, бажати і з чим повинна узгоджувати свою діяльність [22, с. 39].

Саме цілі є тим основним стрижнем безпекової діяльності, який спрямовує, інтегрує, організує і мобілізує всі необхідні засоби і методи, тобто виконує роль своєрідного компасу, спрямовують та раціоналізують її діяльність, а також підвищують ефективність управління нею. Від того, наскільки правильно вони визначені, залежить напрям і зміст забезпечення безпеки організації.

Основна ціль (мета) системи безпеки – це виключення або зведення до мінімуму можливих втрат (збитків) та сприяння у реалізації корпоративних інтересів і загалом функції розвитку, а також забезпечення цілісності соціальної системи шляхом протидії загрозам.

Формулюючи цілі системи безпеки організації, необхідно пам'ятати, що вони, як і сама система безпеки будь-якого підприємства, не є самостійним елементом, залежить від підприємства як самостійної соціально-економічної одиниці. Формування цілей є складним і взаємопов'язаним процесом, що подібний до форми ланцюга, де попередня ланка є визначальною для наступної. Вони формуються з урахуванням корпоративних інтересів з безпеки, включаючи так звані «пов'язані інтереси» (інтереси постачальників, партнерів, кредиторів, споживачів, держави тощо) та повинні мати комплексний характер та кількісне вираження для кожного напрямку діяльності. Наприклад, зменшення рівня травматизму на підприємстві на 1%; виключення штрафних санкцій з боку партнерів чи постачальників за невчасно виконанні зобов'язання на 2% тощо.

Для досягнення цілей система безпеки реалізує системні та комплексні завдання:

1. Визначення, попередження, виявлення та ліквідація загроз організації, а у разі їх реалізації, послаблення негативних наслідків від втрат, їх відшкодування та/або відновлення процесів чи цілісності об'єкта безпеки.

2. Протидія факторам і умовам, що можуть перешкоджати реалізації корпоративних інтересів та спричиняти з приводу цього внутрішні конфлікти.

3. Протидія факторам і умовам, що можуть перешкоджати реалізації пов'язаних інтересів (інтересів постачальників, партнерів, кредиторів, споживачів, держави тощо), визначених законодавством, угодами, стандартами якості тощо.

Загальні завдання слід деталізувати для функцій управління, а також для конкретних функцій розвитку (сфер діяльності) соціальної системи. Кожна з них має свою систему безпечових завдань (рис. 8.4).

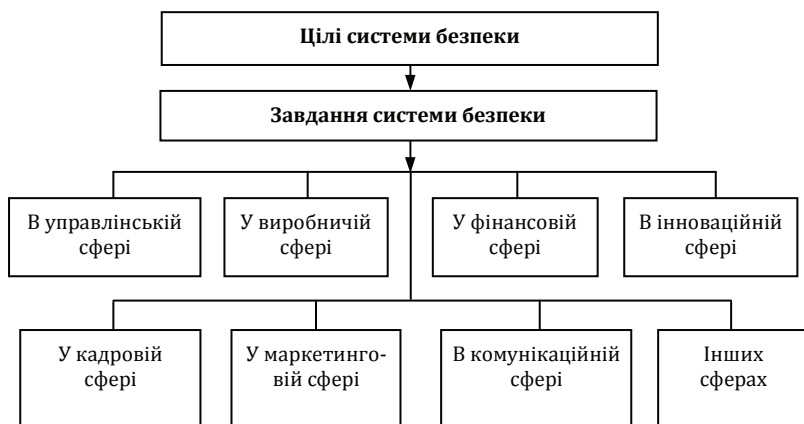


Рис. 8.4 Схема структури завдань системи безпеки організації

Варто зауважити, що формулювати цілі та завдання для кожного структурного елементу (видових функцій розвитку і управління) соціальної системи необхідно якомога конкретніше. Водночас необхідно дотримуватися комплексного і системного підходів, що закладені у загальних завданнях. Тобто

потрібно дотримуватися таких вимог: по кожній функції у завданнях мають бути механізми протидії (визначення, попередження, виявлення та ліквідація) загрозам та відшкодування збитків та/або відновлення процесів чи цілісності об'єкта безпеки, виходячи з корпоративних та пов'язаних з ними інтересів. Наприклад, такими завдання у сфері фінансової діяльності організації можуть бути:

1) створення та підтримання на необхідному рівні нормативно-правового забезпечення фінансово-господарської діяльності організації;

2) встановлення індикаторів з фінансової безпеки організації;

3) створення та підтримання системи постійного моніторингу кількісних показників фінансової безпеки;

4) створення та підтримання системи реагування на загрози у разі погіршення показників фінансової безпеки до граничних значень;

5) створення механізму відшкодування можливих чи отриманих збитків.

Формування завдань з безпеки організації у такий спосіб дасть змогу уникнути виконання несистемних завдань і зайвих витрат.

8.3 Принципи та режим функціонування системи безпеки організації

Принципи забезпечення безпеки – це основні орієнтири, яких повинні дотримуватися суб'єкти безпеки організації у безпековій діяльності. Зазначені орієнтири створюють механізм «стримань та противаг» у використанні сил і засобів та методів для реалізації завдань і досягнення цілей. Тобто, принципи є своєрідним компасом, за яким слід звіряти рішення. Основними з них є:

1. **Принцип правомірності**, що зобов'язує суб'єктів безпеки реалізовувати функцію безпеки, відповідно до верховенства права в межах чинного законодавства.

2. **Принцип системності** – передбачає вимоги, за яких в організації безпекової діяльності немає «важливих» та «неважливих» елементів. А відтак мають бути включені всі, які дадуть змогу протидіяти загрозам та забезпечувати цілісність процесів і об'єктів й сукупно сформулюють систему безпеки організації.

3. **Принцип достатності** – спрямовує застосовування таких засобів і заходів активного та пасивного захисту, які були б достатніми щодо протидії загрозам чи небезпеці, що мінімізує витрати.

4. **Принцип гнучкості** – дає змогу суб'єкту безпеки застосовувати моделі системи безпеки залежно від характеру і рівня розвитку загрози чи небезпеки. Це надає мобільності в реалізації функції безпеки соціальної системи і підвищує її ефективність.

5. **Принцип своєчасності** – вимагає від суб'єкта безпеки діяти оперативно, щоб вчасно ліквідувати загрозу. Крім того, система безпеки організації повинна мати механізми і можливості ухвалювати рішення і діяти на випередження розвитку загрози чи небезпеки, що дозволить уникнути збитків або звести їх до мінімуму.

6. **Принцип спеціалізації** – передбачає залучення до протидії загрозам підготовлених фахівців з конкретного виду діяльності чи спеціалізовану структуру у сфері безпеки, а також організацію професійної підготовки відповідальних осіб за організацію та безпосереднє виконання видових функцій безпеки.

7. **Принцип поєднання гласності й конфіденційності** – дає можливість створити в організації систему безпеки, яка буде зрозумілою і потрібною всьому менеджменту підприємства, що в подальшому дозволить своєчасно виявляти потенційні і реальні загрози. Водночас окремі безпекові заходи мають бути відомі тільки керівникові та співробітнику, який їх реалізує. Принцип конфіденційності дозволяє уникнути можливого витоку інформації та запобігти відповідним контрзаходам з боку конкурентів.

8. Принцип взаємодії – спонукає усі структурні одиниці організації та осіб, які забезпечують процес безпеки, до чітко скоординованої спільної діяльності. Крім того, система безпеки організації також не повинна бути закритою і орієнтованою лише на власні сили і засоби. Має бути налагоджена взаємодія з органами влади, правоохоронними та контрольними органами.

9. Принцип централізації управління – передбачає чітку ієрархічну структуру системи безпеки організації, підпорядкованість її власнику або керівнику.

Система безпеки організації залежно від ситуації та її розвитку може функціонувати в трьох режимах:

- 1) повсякденному;
- 2) підвищеної готовності;
- 3) надзвичайного стану.

Повсякденний режим – це звичайний робочий режим, коли всі суб'єкти системи безпеки, окрім кризової групи, виконують свої функції, реалізують заходи, спрямовані на попередження виникнення загроз, їх виявлення та розробку відповідних типових планів дій на випадок реалізації тих чи інших загроз. Залежно від ситуації, що складається, плани можуть бути таких видів:

- план дій у разі загрози вибуху;
- план дій у разі захоплення заручників, або викрадення працівників організації;
- план дій у разі вимагання;
- план дій у разі нападу на приміщення організації;
- план дій у разі нападу на інкасаторів та ін.

Типові кризові плани є документами конфіденційного характеру, доступ до яких повинен бути у вузького кола осіб. Складаються подібні плани у двох-трьох примірниках. Один зберігається у керівника організації, другий – у начальника служби безпеки, третій може знаходитися у заступника керівника, який виконує його обов'язки.

Розробляючи такі плани, необхідно зважати на те, що це не перелік заходів, а послідовна лінія поведінки організації в конкретній кризовій ситуації, спрямована на забезпечення безпеки.

Режим підвищеної готовності – це функціонування системи безпеки у разі виявлення конкретних загроз.

Із діями, що проводяться у повсякденному режимі, здійснюються ще низка:

- уточнюються і удосконалюються типові плани дій з урахуванням виду загрози, її інтенсивності та масштабності;
- підвищується готовність сил безпеки, які можуть бути задіяні для припинення дії загрози;
- можливий початок роботи кризової групи.

Режим надзвичайного (кризового) стану – це функціонування системи безпеки за наявності реальної дії загроз. У цьому випадку:

- оперативним управлінням організацією займається кризова група;
- рада з безпеки розпочинає працювати в постійному режимі;
- забезпечується повна готовність системи безпеки, особливо служби безпеки, функціональних і лінійних керівників та персоналу організації до безпосереднього припинення дії загрози;
- залучаються зовнішні сили безпеки (державна служба охорони, органи внутрішніх справ) та сили підтримки (структури міністерства надзвичайних ситуацій тощо).

8.4 Суб'єкти, сили та об'єкти безпеки

Участь у безпековій діяльності беруть відповідні суб'єкти на національному рівні та на мікрорівні, тобто на рівні окремої організації.

Суб'єкт безпекової діяльності – це фізична (посадова) або юридична особа, яка бере участь в управлінні, або лише в організації безпекової діяльності соціальної системи.

Держава через відповідні інституції, механізм, закони, підзаконні акти впливає на безпеку соціальних систем на націо-

нальному і на мікрорівні. На загальнонаціональному та регіональному рівні основними інституціями є: Президент України, Верховна Рада України, Кабінет міністрів України, Рада національної безпеки й оборони України, центральні та регіональні органи виконавчої влади, суди, органи прокуратури, місцеві державні адміністрації та місцеві ради. Всі ці суб'єкти безпеки беруть участь у безпековій діяльності держави, а також у забезпеченні безпеки соціальних систем на мікрорівні у межах своїх повноважень.

З погляду безпеки організаційні механізми держави потрібні для того, щоб:

- 1) попереджувати загрози та небезпеки;
- 2) вирішувати конфлікти учасників ринку;
- 3) ліквідовувати умови, що сприяють учиненню економічних правопорушень та злочинів;
- 4) впроваджувати мінімально необхідні й обов'язкові для всіх учасників ринку правила, критерії та стандарти;
- 5) впорядковувати механізми взаємодії для захисту інтересів учасників економічних відносин на ринку;
- 6) застосовувати заходи впливу та примусу тощо.

У підсумку роль держави у забезпеченні безпеки організації полягає у створенні таких механізмів і можливостей, які б забезпечували самодостатність та стійкість соціальних систем усіх рівнів.

Водночас держава, яка неспроможна сформувати такі механізми і можливості, виконує негативну роль у забезпеченні безпеки соціальних систем, тобто перетворюється з фактора забезпечення безпеки на джерело загрози.

На мікрорівні послуги з безпекової діяльності надають Державна служба охорони (ДСО) та приватні структури з безпеки.

ДСО у забезпеченні безпеки організацій належить особливе місце. Воно обумовлена тим, що ДСО є єдиною в Україні централізованою професійною охоронною структурою, що володіє правом на надання замовникам озброєної охорони. Крім того, ДСО також є представником держави на ринку охоронних послуг України [9].

Роль ДСО на ринку охоронних послуг України обумовлена наявністю в її розпорядженні найбільш потужних сил і засобів, законодавчому захисті її діяльності, а також тим, що саме ДСО визначає «правила гри» на ринку охоронних послуг.

Приватні структури безпеки надають широкий спектр послуг: правовий і економічний захист усіх форм власності, моніторинг фінансової спроможності партнера, надання інформації про конкурентів, моніторинг боргових зобов'язань, оснащення різними системами сигналізації, технічний захист від прослуховування приміщень, телефонних розмов, несанкціонованого доступу до комп'ютерних мереж, антитерористичне обладнання для виявлення і знешкодження вибухових пристроїв, рентген-системи для огляду людей, кореспонденції, металошукачі та ін.

Приватні структури з безпеки, які можуть брати участь у забезпеченні безпеки підприємства, за напрямками діяльності поділяються на такі основні види:

- 1) охоронні агентства;
- 2) детективні агентства (приватні детективи);
- 3) аналітичні агентства;
- 4) консалтингові агентства.

Кожна з наведених структур бере участь у забезпеченні безпеки організацій шляхом виконання тих чи інших видів діяльності, що притаманні їм та визначені в статутних документах.

Основним суб'єктом забезпечення безпеки є саме підприємство. Ефективність безпекової діяльності залежить від дієвості, взаємодії та оптимальної структури внутрішніх суб'єктів безпеки. Для великих організацій є оптимальним, коли до складу суб'єктів безпеки безпосередньо входять:

- 1) відповідальний керівник системи;
- 2) рада з питань безпеки;
- 3) кризова група;
- 4) керівники лінійних і функціональних підрозділів організації;
- 5) служба безпеки.

Всі ці суб'єкти здійснюють безпекову діяльність у межах делегованих їм повноважень та функцій, які передбаченні у внутрішніх документах соціальної системи: статуті, положеннях про структурний підрозділ, посадових обов'язках фахівців тощо.

Відповідальний керівник системи безпеки організації – головний керівник або його заступник. Він спрямовує діяльність системи безпеки, відтак повинен добре знати об'єкти безпеки і загалом сферу безпеки організації.

Рада з безпеки організації – це колегіальний орган при керівникові системи безпеки. Рада виконує консультативні функції шляхом аналізу і оцінки ситуації у сфері безпеки та розробки проектів відповідних документів. Її пропозиції та рішення мають рекомендаційний характер.

Кризова група – група з ключових фігур організації, якій делегуються повноваження щодо оперативного управління у кризових (надзвичайних) ситуаціях. Кризові ситуації виникають у процесі або після здійснення зовнішніх чи внутрішніх загроз (теракт, пожежа, рейдерські атаки, крадіжка коштів у особливо великих розмірах, викрадення ключових фігур організації тощо) і можуть виявлятися і розвиватися по-різному: повільно або миттєво, спонтанно або ретельно сплановано конкурентами чи зловмисниками.

До складу кризової групи обов'язково повинні входити: головний керівник, юрист, фінансист, керівник служби безпеки. Ці особи, як правило, через своє службове становище, мають спеціальні знання, досвід, реальні можливості впливати на обставини, в яких виникає і розвивається кризова ситуація. Водночас забезпечується вплив на щоденну діяльність організації.

Кризова група вирішує такі завдання:

- 1) проводить оцінку ситуації, що формується чи вже виникла;
- 2) ухвалює рішення та забезпечує на їх виконання невідкладні заходи з безпеки;
- 3) забезпечує оперативну взаємодію з правоохоронними органами.

Керівники лінійних і функціональних підрозділів організації беруть участь у забезпеченні безпеки шляхом створення відповідних умов та виконання загальних заходів безпеки. Основними їх функціями є:

- 1) участь у визначенні складу відомостей, що становлять комерційну таємницю і конфіденційну інформацію підприємства;
- 2) організація виконання заходів безпеки у своїх підрозділах;
- 3) економічний та фінансовий контроль клієнтів і партнерів під час проведення операцій і угод;
- 4) реалізація заходів безпеки у кадровій роботі;
- 5) організація заходів захисту інтелектуальної власності, інформації з обмеженим доступом та технологій підприємства під час проведення операцій, угод, ділових переговорів і зустрічей;
- 6) організація та підтримка відповідних режимів безпеки у роботі підрозділів підприємства;
- 7) економічні і технологічні заходи мінімізації ризиків у діяльності підприємства;
- 8) моніторинг комерційних операцій на предмет реальних або виникнення потенційних загроз;
- 9) організація навчання працівників підприємства, роботи з профілактики злочинів, порушень правил роботи та негативних вчинків;
- 10) проведення внутрішніх перевірок і ревізій.

Служба безпеки (СБ) організації є самостійним функціональним структурним підрозділом, безпосереднє управління якою покладається на її начальника. Основне призначення служби безпеки полягає у виключенні можливих збитків та забезпечення цілісності процесів чи об'єктів і загалом організації шляхом протидії загрозам.

Законів прямої дії, що регламентують діяльність, права і обов'язок служби безпеки суб'єктів господарської діяльності, сьогодні в Україні не прийнято. Відтак служба безпеки створюється і функціонує відповідно до локальних нормативних актів конкретної організації. Організаційно вона може бути предста-

влена у вигляді: департаменту безпеки, управління, служби, відділу тощо.

Формуючи службу безпеки в організації необхідно дотримуватися чітких вимог:

1) служба безпеки має підпорядковуватися власнику, або головному керівникові;

2) в основних організаційних нормативно-правових документах мають бути закріплені відповідні функції, повноваження та обов'язки, які б дозволяли ефективно взаємодіяти її з внутрішніми підрозділами та зовнішніми структурами з безпеки;

3) розширення сфери впливу має відбуватися через збільшення кількості відповідних функцій, а посилення впливу через наділення її відповідними повноваженнями.

Служба безпеки організації має відповідну структуру, конфігурація якої може бути різною, з урахуванням загроз та фінансових, технічних, кадрових та інших можливостей.

Є два підходи до формування організаційної структури служби безпеки підприємства:

1) створення служби безпеки, структура якої зорієнтована на виконання всіх функцій, необхідних для забезпечення безпеки організації, що делегуються їй як структурному підрозділу;

2) створення служби безпеки, структура якої зорієнтована на виконання частини функцій, і для залучення на умовах угоди інших сил безпеки (ДСО, приватних структур безпеки) для виконання решти функцій, необхідних для забезпечення безпеки організації у межах функцій, передбачених для неї як структурного підрозділу.

Функції СБ розробляються з урахуванням потенційних і реальних загроз конкретним об'єктам безпеки організації, забезпечення цілісності процесів та об'єктів організації. Основними функціями служби безпеки підприємства можуть бути:

1) здійснення управління власними структурними підрозділами, організація взаємодії між ними та підрозділами служб безпеки суб'єктів господарювання та інших юридичних

осіб інших об'єктів з метою забезпечення функціонування та стійкого розвитку об'єкта;

2) проведення моніторингу загроз і небезпек, виявлення факторів та джерел, здійснення превентивного впливу на них;

3) вироблення механізму мінімізації загроз і небезпек;

4) здійснення комплексу заходів, що забезпечують безпеку об'єкта: інформаційно-аналітичне, нормативно-правове, матеріально-технічне, психологічне, ідеологічне, організаційне та інше забезпечення;

5) сприяння у здійсненні державного контролю за діяльністю служб безпеки суб'єктів господарювання та інших юридичних осіб інших об'єктів;

6) здійснення конкретних заходів реагування на загрози і небезпеки щодо об'єкта;

7) участь у формуванні системи освіти в сфері безпеки;

8) організаційно-правове та інформаційно-аналітичне супроводження судових розглядів, що стосуються інтересів об'єкта;

9) інформування уповноважених державних органів і громадськості про порушення прав об'єкта;

10) надання допомоги у процесі підбору та вивчення осіб, які приймаються на роботу;

11) вивчення ділової надійності й фінансової самостійності партнерів об'єкта;

12) сприяння в організації незалежної експертизи щодо якості товару, продукції;

13) ведення реєстру надійних партнерів;

14) організація, проведення навчально-практичної і консультаційної діяльності персоналу об'єкта в галузі безпеки;

15) захист законних прав та інтересів, зокрема й матеріальних, персоналу об'єкта;

16) збір, аналіз, оцінка і прогнозування даних, що характеризують стан обстановки зсередини і ззовні об'єкта безпеки;

17) своєчасне виявлення можливих прагнень до об'єкта з боку джерел зовнішніх загроз безпеці;

18) недопущення промислового шпигунства, виявів злочинності всіх форм та протиправних намірів окремих громадян на об'єкті;

19) протидія несанкціонованому технічному проникненню на об'єкт;

20) виявлення, попередження та припинення можливої протиправної діяльності з боку співробітників об'єкта на шкоду його безпеці;

21) захист співробітників об'єкта від насильницьких та майнових посягань під час виконання службових обов'язків;

22) збереження матеріальних цінностей і відомостей об'єкта;

23) добування необхідної інформації для вироблення стратегічних і тактичних рішень, пов'язаних із управлінням діяльністю об'єкта;

24) фізична і технічна оборона будівель, споруд, території і транспортних засобів, які належать об'єкту;

25) протидія недобросовісній конкуренції;

26) забезпечення дотримання комерційної таємниці персоналом об'єкта, вжиття заходів, згідно з чинним законодавством, за фактом розголошення комерційної таємниці;

27) збір інформації про факти неправомірного використання товарних знаків підприємства;

28) збір інформації про проведення ділових переговорів;

29) захист життя та здоров'я персоналу від протиправних посягань;

30) забезпечення безпеки в місцях проведення об'єктом представницьких, конфіденційних та інших заходів;

31) підтримання взаємодії з правоохоронними та контрольними органами, створення сприятливих умов для виконання покладених на них законом обов'язків;

32) здійснення профілактичних заходів із протидії виявам тероризму на об'єкті [11, с. 396–398].

У процесі виконання зазначених та інших функцій, а також загальних і спеціальних заходів з безпеки, що впливають з них, взаємодіє практично з усіма суб'єктами і силами підприємства, а також, у міру необхідності, з іншими (зовнішніми) суб'єктами і

силами системи безпеки. Така взаємодія щодо протидії загрозам, забезпечення цілісності процесів і об'єктів дає змогу створювати умови для стійкого функціонування і розвитку організації.

Принципово важливим для забезпечення безпеки організації є використання механізмів взаємодії системи безпеки організації та системи безпеки держави. Наприклад, суттєвою допомогою для безпеки організації була б інформація про протиправні дії транснаціональних корпорацій, про рейдерські захоплення, про проникнення в управлінські структури представників організованих злочинних угруповань тощо. Подібна допомога відповідним структурам системи безпеки держави могла б бути з боку служб безпеки організацій, наприклад, допомога у розшуку відповідних осіб, надання інформації про «відмивання» коштів, здобутих злочинним шляхом тощо. Відтак системи безпеки організації і держави повинні взаємодіяти і в такий спосіб сприяти один одному у виконанні властивих їм функцій та вирішенні обраних завдань. Практика такої взаємодії існує в США, низці європейських країн та ін.

У процесі забезпечення безпеки беруть участь відповідні сили безпеки.

Сили безпеки – це фізичні особи, які безпосередньо виконують заходи безпеки.

Сили безпекової діяльності можна поділити на такі основні групи:

- 1) особовий склад служби безпеки підприємства;
- 2) співробітники підприємства;
- 3) організації і особи, які забезпечують безпеку на умовах договору;
- 4) працівники державних структур.

Фактично всі зазначені категорії беруть повноцінну участь у забезпеченні безпеки соціальної системи, хоча й по-різному. Особовий склад служби безпеки підприємства безпосередньо задіяний у виконанні завдань із забезпечення кожного напрямку безпеки. Співробітники підприємства забезпечують безпеку шляхом дотримання відповідних адміністративних режимів і нормативно-правових актів з безпеки на

власному робочому місці. Працівники приватних спеціалізованих структур з безпеки та державних структур, зокрема й правоохоронних органів України, виконують спеціальні заходи безпеки залежно від виду і форми загрози та у межах своїх обов'язків та повноважень.

Безпека соціальної системи організується не взагалі, а за конкретними об'єктами. Під *об'єктом безпеки* розуміється все те, на що спрямована діяльність суб'єктів і сил безпеки з метою захисту їх від загроз. Практика свідчить, що найбільшу зацікавленість у недобросовісних конкурентів та зловмисників до ефективно господарюючих організацій, викликають такі об'єкти:

1) персонал (власники організації, їх приватне майно; керівництво і вищий менеджмент організації; особи, які мають доступ до його таємниць організації, інші працівники);

2) фінансові ресурси (національна й іноземна валюта, комерційні операції та угоди, коштовності, фінансові документи, акції, облигації тощо);

3) матеріальні ресурси (будівлі, сховища, обладнання, транспорт, засоби і системи інформатизації, сировина, готовий товар, комунікації: водо- і газопостачання, каналізація, електричні і телефонні мережі, системи вентиляції і кондиціонування, протипожежна і охоронна сигналізації тощо);

4) інформаційні ресурси з обмеженим доступом (відомості, що є комерційною таємницею і конфіденційною інформацією в різних сферах діяльності організації: особливості та інноваційні секрети, інфраструктура бізнесу, менеджмент, маркетинг і цінова стратегія, фінансові звіти і прогнози, програми розвитку, персонал, система безпеки фірми, корпоративні зв'язки тощо);

5) корпоративні права (майнові та немайнові права акціонера – власника акцій товариства, які впливають з права власності на акції, що включають право на участь в управлінні акціонерним товариством, право голосу, право на отримання інформації про діяльність юридичної особи, отримання дивідендів та активів акціонерного товариства у разі його ліквідації відповідно до закону, а також інші права та правомочності, передбачені законом чи статутними документами);

б) імідж організації (психологічний портрет організації, який беруть до уваги споживачі, постачальники, конкуренти, злочинці та ін. під час формування власного ставлення до неї та ухвалення рішень).

Питання та завдання для самоконтролю

1. Що таке система безпеки організації та які є наукові підходи до визначення її сутності?

2. Поясніть сутність та роль моделювання у формуванні структури системи безпеки організації.

3. Розкрийте сутність основних вимог до формування системи безпеки організації та обґрунтуйте чому варто їх дотримуватися?

4. Наведіть структуру системи безпеки організації та дайте загальну її характеристику.

5. Розкрийте структуру процесу функціонування системи безпеки організації.

6. Що таке цілі системи безпеки організації та який їх вплив на її функціонування.

7. Розкрийте структуру та сутність завдань системи безпеки на конкретному прикладі.

8. Яких принципів необхідно дотримуватися, щоб система безпеки функціонувала ефективно? Розкрийте їх застосування на конкретному прикладі.

7. Охарактеризуйте режими функціонування системи безпеки організації.

8. Які є основні суб'єкти безпекової діяльності на національному рівні та яке їх основне завдання у цьому процесі?

9. Яке основне призначення внутрішніх суб'єктів безпекової діяльності: відповідального керівника системи безпеки, ради з питань безпеки, кризової групи у забезпеченні безпеки соціальної системи?

10. Розкрийте роль та основні функції керівників лінійних і функціональних підрозділів організації у системі її безпеки.

11. Що таке Служба безпеки організації? Яких вимог до її створення та підходів до формування організаційної структури необхідно дотримуватися?

12. Наведіть основні функції служби безпеки організації.
13. Розкрийте роль Державної служби охорони у забезпеченні безпеки соціальної системи.
14. Яке значення приватних (недержавних) структур з безпеки у забезпеченні безпеки соціальної системи.
15. Що таке сили забезпечення безпеки організації та яке їх призначення?
16. Що таке об'єкт безпеки, які є види об'єктів безпеки? Охарактеризуйте їх.

Тести

1. Виключення або зведення до мінімуму можливих втрат (збитків) або упущення вигоди та сприяння в реалізації корпоративних інтересів і загалом функції розвитку, а також забезпечення цілісності організації шляхом протидії загрозам – це:
 - а) завдання системи безпеки організації;
 - б) місія організації у сфері безпеки;
 - в) основна мета системи безпеки організації;
 - г) правильні відповіді а і б.
2. Яке з наведених не є завданням системи безпеки організації?
 - а) визначення, попередження, виявлення та ліквідація загроз організації, а у разі їх реалізації, послаблення негативних наслідків від втрат, їх відшкодування та/або відновлення процесів чи цілісності об'єкта безпеки;
 - б) протидія факторам і умовам, що можуть перешкоджати найманим працівникам, топ-менеджерам, акціонерам і власникам організації реалізовувати власні корпоративні інтереси та виконувати обов'язки щодо підприємства, а також викликати конфлікти з приводу реалізації корпоративних економічних інтересів;
 - в) визначення механізмів та створення умов для реалізації корпоративних інтересів;
 - г) протидія факторам і умовам, що можуть перешкоджати реалізації пов'язаних інтересів (інтересів постачальників, партнерів, кредиторів, споживачів, держави тощо), визначених законодавством, угодами, стандартами якості тощо.

3. Які з наведених елементів не є об'єктом безпеки організації?

- а) персонал;
- б) фінансові ресурси;
- в) інформаційні ресурси, які не мають обмежень у доступі до них;
- г) імідж організації.

4. Який з поданих принципів не належить до принципів функціонування системи безпеки?

- а) плановість;
- б) правомірність;
- в) структурність;
- г) поєднання гласності та конфіденційності.

5. Режим функціонування системи безпеки, за якого всі суб'єкти системи безпеки, окрім кризової групи, виконують свої функції, реалізують заходи, спрямовані на попередження виникнення загроз, їх виявлення та розробку відповідних типових планів дій на випадок реалізації тих чи інших загроз, – це:

- а) режим підвищеної готовності;
- б) повсякденний режим;
- в) режим надзвичайного (кризового) стану;
- г) правильні відповіді а, б.

6. До концептуальних вимог, яких необхідно дотримуватися під час формування системи безпеки організації, належать:

- а) унікальність;
- б) комплексність;
- в) відносна самостійність;
- г) усі відповіді правильні.

7. Основні орієнтири, яких повинні дотримуватися суб'єкти безпеки організації у безпековій діяльності, – це:

- а) методи;
- б) принципи;
- в) засоби;
- г) функції.

8. Які з наведених дій є властивими для функціонування системи безпеки у режимі підвищеної готовності:

а) рада з безпеки розпочинає працювати в постійному режимі;

б) забезпечується повна готовність системи безпеки, особливо служби безпеки, функціональних і лінійних керівників та персоналу організації до безпосереднього припинення дії загрози;

в) залучаються зовнішні сили безпеки (державна служба охорони, органи внутрішніх справ) та сили підтримки (структури міністерства надзвичайних ситуацій тощо).

г) уточнюються і удосконалюються типові плани дій з урахуванням виду загрози, її інтенсивності та масштабності.

9. Для забезпечення безпеки соціальних систем держава як суб'єкт безпеки створює організаційні механізми для того, щоб:

а) вирішувати конфлікти учасників ринку;

б) ліквідовувати умови, що сприяють учиненню економічних правопорушень та злочинів;

в) впроваджувати мінімально необхідні й обов'язкові для всіх учасників ринку правила, критерії та стандарти;

г) усі відповіді правильні.

10. Які з поданих нижче суб'єктів не входить безпосередньо у склад суб'єктів безпеки великих організацій?

а) приватна охорона структура;

б) рада з питань безпеки;

в) кризова група;

г) керівники лінійних і функціональних підрозділів організації.

11. Формуючи службу безпеки в організації необхідно дотримуватися чітких вимог:

а) служба безпеки має підпорядковуватися власнику, або головному керівникові;

б) в основних організаційних нормативно-правових документах мають бути закріплені відповідні функції, повноваження та обов'язки, які б дозволяли ефективно взаємодіяти її з внутрішніми підрозділами та зовнішніми структурами з безпеки;

в) розширення сфери впливу має відбуватися через збільшення кількості відповідних функцій, а посилення впливу через наділення її відповідними повноваженнями.

г) усі відповіді правильні.

12. До суб'єктів безпекової діяльності можна віднести таку групу:

а) особовий склад служби безпеки підприємства;

б) співробітники підприємства;

в) організації й особи, які забезпечують безпеку на умовах договору;

г) керівники структурних підрозділів.

Тема 9

ДІАГНОСТИКА СТАНУ БЕЗПЕКИ СОЦІАЛЬНОЇ СИСТЕМИ

*Щоб змінити стан речей
є лише один спосіб –
отримати об'єктивну інформацію.
Це можливо лише за умови
застосування сучасних методик діагностики*

9.1 Концептуально-методичний підхід до діагностики стану безпеки організації

Безпека як складне соціальне явище й феномен розглядається вченими з різних боків, зокрема й як стан соціальної системи у межах граничних значень. Стан соціальної системи відображає результати її діяльності (безпекової, розвиткової та управлінської) та залежить від її ефективності. Розуміння безпеки організації як її стану у межах граничних значень, тобто стану, який не порушує меж, за якими починається небезпека, потребує відповідних підходів та методик його діагностики.

Діагностика стану безпеки організації – це вивчення наслідків впливу загроз на діяльність організації та об'єкти безпеки в умовах неповної інформації на предмет встановлення рівня її безпеки.

Стан безпеки системи можна визначити через відповідні критерії та показники. Під критерієм оцінювання безпеки необхідно розуміти ознаку, за якою визначається стан безпеки соціальної системи.

Кожен критерій має якісне чи кількісне вираження – показник, що свідчить про стан системи. Розглядаючи питання показників, слід чітко розмежовувати показники, які використовуються для розрахунку під час оцінювання чи визначення стану безпеки, та показник критеріїв безпеки, що має граничне значення. Показник з граничним значенням – це своєрідний індикатор безпеки, котрий демонструє в безпеці чи небезпеці перебуває соціальна система. Для оцінки стану чи рівня безпеки підприємства слід використовувати індикатори безпеки, тобто критерії з граничним показником. Оцінюючи стан безпеки, потрібно завжди бачити межу, яка розділяє його на два поля: безпечне і небезпечне через якісний чи кількісний показник з відповідними граничним значенням, тобто через індика-

тори безпеки. Безпечний стан системи є тоді, коли основні індикатори безпеки знаходяться в межах граничних значень, тобто ще зберігаються можливості для розвитку.

У навчально-науковій літературі наведені різні підходи та методики визначення стану економічної безпеки організації. Проте вони не мають комплексного характеру та здебільшого є громіздкими у розрахунках чи зборі відповідної інформації.

Формуючи методичний підхід до діагностики безпеки організації, необхідно зважати, що її життєдіяльність забезпечується корінними функціями – функцією розвитку, функцією безпеки та функцією управління. Тому об'єктивно в реальному житті виокремити і оцінити функцію безпеки практично неможливо. Як слушно зазначає Г. А. Мінаєв, сутність безпекоменеджменту полягає у тому, що логіка супротиву силам тяжіння загроз, логіка безпечного розвитку соціальної системи виводиться з пізнання її як цілісного організму, чого раніше не робилось [14, с. 31]. А процес управління організацією супроводжується процесом оцінки чинників та умов, що є відповідальними за реалізацію функцій розвитку і функцій безпеки [14, с. 29].

Діагностувати й визначати рівень безпеки соціальної системи потрібно комплексно, керуючись основними положеннями. Вони зводяться до такого:

1. Оцінюючи стан (рівень) безпеки соціальної системи оцінюватимемо наслідки вже вжитих дій і заходів, тобто минуле. Проте функція «оцінки минулого» дає змогу відповісти на питання, як результати, досягнуті у минулому, та процеси функціонування вплинули на подальшу економічну ефективність. «Оцінка минулого» дозволяє зробити висновок про майбутню ефективність на підставі переваг, отриманих у минулому [1, с. 47–50]. Тобто, оцінюватиметься результат виконання функції безпеки, розвитку та управління. Також діагностуватиметься безпосередній і опосередкований вплив безпекової діяльності на стан безпеки організації безпекової корпоративної культури. Своєю чергою, стан безпеки організації також має зворотній вплив на згадані елементи.

2. У сучасній ринковій економіці перспективи розвитку мають ті організації, які є цікавими для інвестора. Відтак інвестор визначає рівень зацікавленості через ступінь захисту у цьому підприємстві інтересів інвестора та корпоративних інтересів. З погляду організації – це інтереси безпеки, адже, не створивши необхідних умов і механізмів для їх реалізації, підприємство може зазнати значних збитків через штрафні санкції, компенсацію за завдані моральні збитки, реклаमाції споживачів і відкликання у зв'язку з цим товару з ринку тощо. Саме ці та подібні показники, тобто показники безпеки, сьогодні є пріоритетними під час укладання угод, залучення інвестицій тощо.

3. Для розробки методики діагностики (оцінки) стану безпеки потрібно використовувати комплексні якісні й кількісні критерії та показники до кожного з них, які б відображали протидію основним реальним чи потенційним загрозам з чітким розмежуванням безпечного і небезпечного стану, процесу чи тенденції.

4. Основними елементами систематичного моніторингу й оцінки рівня безпеки соціальної системи на практиці є фахівець-експерт, рівень його професійних знань і вмінь та просто-та, коректність й інформативність методик, якими він користується. Це дає змогу фахівцям-експертам використовувати суб'єктивно-об'єктивний підхід. Експертами мають бути провідні фахівці та керівники організації. Саме вони найбільш обізнані з основними загрозами підприємству, особливо внутрішніми. Можна залучати і зовнішніх експертів, які працюють або досліджують галузь, в якій функціонує підприємство.

5. Для діагностики необхідно обрати такі індикатори безпеки, які комплексно давали б можливість оцінити стан безпеки організації та відображали її властивості, а саме:

а) *самодостатність соціальної системи* – це наявність у розпорядженні суб'єктів управління відповідних ресурсів та уникнення залежності від джерел їх походження, що може становити загрозу, а також їх використання на рівні, необхідному для збереження параметрів життєдіяльності системи;

б) *стійкість соціальної системи* – це наявність необхідних умов, елементів та системних зв'язків між ними як мінімум на рівні, достатньому для стримування дії дестабілізуючих факторів.

Саме показники самодостатності та стійкості системи організації визначають її здатність протидіяти загрозам. Водночас необхідно пам'ятати:

- не може існувати єдиного незмінного переліку індикаторів безпеки підприємства, оскільки кожне підприємство, а також особливості його підприємницької діяльності є унікальними та індивідуальними [6, с. 9];

- до показників індикаторів рівня безпеки підприємства можна віднести ті, які кількісно відображають рівень загрози, наділені значним рівнем чутливості та, відповідно, здатні попереджати про можливість настання небезпеки [3, с. 80];

- в) індикатори безпеки мають бути такими, що не потребують додаткових звітів в організації та є простими у використанні під час ухвалення управлінських рішень.

9.2 Критерії діагностики стану та визначення рівня безпеки організації

Для діагностики стану безпеки організації необхідно використовувати лише основні та водночас комплексні критерії, які б відображали її властивості як соціальної системи, а саме самодостатність та стійкість.

Такими основними комплексними критеріями, які мають бути обов'язковими для діагностики стану безпеки організації, є:

- а) збиток організації;
- б) платоспроможність організації;
- в) встановлення протиправного контролю над організацією або її активами.

Додатково до цих критеріїв можна використовувати й інші. Це надасть змогу ширше й глибше проаналізувати стан соціальної системи з погляду безпеки. Це залежить від виду

діяльності, розмірів, організаційної форми соціальної системи та інших чинників.

Наведені критерії діагностики стану безпеки організації та визначення його рівня дають достатньо інформації для того, щоб зрозуміти який стан безпеки в організації та які рішення необхідно ухвалювати.

Критерій збитку комплексно характеризує стан економічної безпеки. Такий підхід підтверджується працями В. М. Геєця, Т. С. Клебанової, М. О. Кизим, які зазначають, що загроза економічній безпеці може бути визначена як деякий збиток, інтегральний показник якого характеризує ступінь зниження економічного потенціалу за визначений проміжок часу [15, с. 128]. Його величина залежить від деструктивних граничних змін в акціонерному товаристві, які спричинені реалізацією тих чи інших загроз. Проте визначити чисті збитки, пов'язані з реалізацією загроз, на практиці доволі складно, оскільки в організації окремо такий облік не ведеться. Обліковуються всі витрати, які були необхідні для проведення всієї діяльності, зокрема й заходів з безпеки, за результатами якої отримується певний дохід. Витрати характеризують якість і ефективність виконання робіт, завдань, операцій тощо з усіх видових функцій розвитку, безпеки та управління.

Водночас під доходом слід розуміти збільшення економічного зиску у вигляді надходження активів або зменшення зобов'язань, що призводить до збільшення власного капіталу (окрім зростання капіталу за рахунок внесків власників). Під витратами розуміється зменшення економічного зиску у вигляді вибуття активів або збільшення зобов'язань, що призводить до зменшення власного капіталу (за винятком зменшення капіталу за рахунок його вилучення або розподілу між власниками). Отже, що більше реалізується тих чи інших загроз, то більші загальні витрати організації. Вони можуть бути незначними, якщо система безпеки ефективна, і навпаки, – значні, що можуть дестабілізувати діяльність підприємства. У другому випадку загальні витрати значно збільшуються.

Зрозуміло, що витрати компенсуються доходами. Якщо доходи їх не покривають, то організація за результатами діяльнос-

ті матиме збиток. У цьому разі, з погляду безпеки, дуже важливим є питання їх дестабілізуючого впливу на діяльність організації, тобто потрібно знати, до якої межі збиток ще залишає можливості для розвитку.

Граничним показником збитку може бути, наприклад, в акціонерному товаристві – співвідношення власного капіталу до мінімального розміру статутного капіталу. Водночас згідно з Законом України про «Акціонерні товариства» власний капітал не повинен бути меншим за мінімальний розмір статутного капіталу акціонерного товариства. У разі, коли він менший, акціонерне товариство зобов'язане упродовж десяти місяців усунути таку невідповідність або ухвалити рішення про самоліквідацію.

Можна застосовувати й інші методичні підходи до оцінювання стану безпеки організації за критерієм збитковості. Вони описані в науково-практичній літературі.

Для оцінки стану безпеки за цим критерієм доцільно використовувати такі характерні ознаки:

1) збиток небезпечний, якщо організація практично не має можливості для його відшкодування;

2) збиток критичний, якщо організація ще має можливість для його відшкодування шляхом залучення позичкового капіталу;

3) збиток значний, якщо організація ще має можливості для його відшкодування шляхом збільшення власного та залучення позичкового капіталу;

4) збиток незначний, якщо організація має можливість для його відшкодування шляхом збільшення власного капіталу.

Критерій платоспроможності для діагностики стану безпеки організації є найінформативнішим і простим у застосуванні, що на практиці має велике значення. Під час оцінювання загального стану безпеки підприємства визначальною є його фінансова сфера, оскільки «...саме фінансова сфера діяльності підприємства інтегрує в собі результати діяльності всіх життєво важливих для підприємства сфер» [15, с. 132].

Тому «лакмусовим папірцем», де відображаються результати діяльності організації з усіх основних видових функцій і

розвитку, і безпеки, є фінансовий критерій у вигляді показника обігових коштів, за яким можна визначити рівень платоспроможності та ознаки банкрутства.

У процесі діяльності підприємству через різні обставини не вистачає власних обігових коштів. Користуючись цим критерієм, спочатку можна побачити цілісну картину стану, і у разі, коли інформація є тривожною, потрібно провести аналіз і виявити реальні загрози. Їх може бути багато, наприклад: спад обсягів реалізації товарів у зв'язку із дискредитацією організації на ринку чи піддробкою товару; затримка оплати за відвантажений товар; накладення штрафних санкцій контрольними органами через порушення чинного законодавства; зменшення обсягів виробництва через проблеми у постачанні сировини чи напівфабрикатів, або технологічною аварією; завищені планові показники доходів тощо. У такому разі підприємство бере середні і довгострокові кредити. Це нормальний процес, характерний для ринкового господарювання, до того ж він є ще доволі безпечним, оскільки в організації зберігаються можливості для розвитку. Проте, коли підприємство бере короткострокові кредити, то це свідчить про те, що організація зазнала суттєвих втрат (збитків) у різній формі, а це вже перший крок до банкрутства, що становить небезпеку. Ще гірша ситуація, коли організація не вистачає ані власних, ані позикових коштів. Це є реальна небезпека життєдіяльності організації, оскільки за таких умов воно перебуває на стадії банкрутства. Отже, відсутність платоспроможності організації є підставою для провадження справи про банкрутство і згодом про його ліквідацію.

Оцінка стану безпеки організації за цим критерієм зводиться до того, щоб з'ясувати її фінансову міцність через показник банкрутства та залучення кредитних коштів, у зв'язку з нестачею власних коштів, для виконання відповідних фінансових зобов'язань.

Основними характерними ознаками, на які необхідно зважати під час аналізу та оцінювання стану безпеки організації за критерієм її платоспроможності, є:

а) організація перебуває на стадії банкрутства;

б) нестача обігових коштів компенсується короткостроковими кредитами;

в) нестача обігових коштів компенсується середньостроковими кредитами;

г) нестача обігових коштів компенсується довгостроковими кредитами.

Для оцінки стану безпеки організації за цим критерієм можна використовувати різні методики, що описані в літературі.

Використання **критерію встановлення протиправного контролю над організацією або її активами** є обов'язковим під час оцінювання стану безпеки. Ефективно господарює і конкурентноздатне підприємство є цікавим на ринку не тільки для інвесторів. В умовах українського бізнес-середовища, де домінують тіньові і корупційні відносини, такі підприємства викликають зацікавленість у недобросовісних конкурентів та кримінальних структур. Використовуючи прогалини у нормативно-правовому забезпеченні діяльності організацій та чинного законодавства, вони намагаються встановити над організацією чи її активами контроль всупереч її волі та протиправними методами. Зрозуміло, що за умови встановлення такого контролю над підприємством чи його активами реалізація корпоративних інтересів та прав значно ускладнюється. Виявити таку небезпеку можна шляхом проведення аналітично-пошукової та детективної діяльності. Виявлення перших ознак встановлення такого контролю необхідно кваліфікувати як початок реалізації реальних загроз, що обов'язково можуть спричинити небезпеку для організації, наприклад у формі рейдерського захоплення. Для цього потрібно володіти відповідною інформацією та діяти за такими ознаками:

а) над організацією чи її активами є реальний контроль всупереч її волі та протиправними методами;

б) є реальні спроби встановлення над організацією чи її активами контроль всупереч її волі та за допомогою протиправних методів;

в) відсутність будь-яких реальних спроб встановити над організацією чи її активами контроль всупереч її волі та протиправними методами;

г) відсутність реальних чи потенційних намірів встановити над організацією чи її активами контроль всупереч її волі та протиправними методами.

Оцінюючи стан безпеки організації через наведені критерії, потрібно зважати на принципове положення: безпека є тоді, коли загальний показник стану безпеки та окремі його індикатори: збиток, платоспроможність і встановлення протиправного контролю над організацією або її активами будуть не нижче граничного, тобто самодостатність та стійкість соціальної системи є такими, за яких зберігаються умови і можливості для розвитку. Індикатори безпеки (критерії та їх граничні показники) мають кількісне й якісне вираження. Щодо цього питання у науковій літературі є різні методичні підходи та методики до формування індикаторів безпеки та їх розрахунків. У розділі підручника «Практикум» викладено авторську методику діагностики та визначення рівня безпеки організації.

Важливим у діагностиці є питання організаційні та технологічні. Йдеться про певні правила, вимоги, якими встановлюється алгоритм, тобто порядок підготовки до діагностики та її проведення. Основними з них є:

1. Для оцінювання стану безпеки організації власником чи керівником призначається керівник експертної групи та формується склад експертної групи з числа її керівників та провідних за напрямками фахівців. Обов'язково необхідно включати керівника служби безпеки та фахівців цієї структури.

Доцільно, щоб така експертна група функціонувала як робоча група на постійній основі. Це дає можливість планомірно аналізувати ситуацію й оцінювати рівень безпеки. Крім того, систематична робота такої експертної групи сприяє підвищенню рівня знань експертів, формуванню відповідних вмінь та навиків, що, своєю чергою, значно покращує якість аналізу ситуації та її оцінки.

2. Експертною групою проводиться оцінювання стану безпеки соціальної системи за визначеними індикаторами та методикою. Результати оцінки аналізуються та визначаються

слабкі місця соціальної системи й подаються керівникові організації чи власникові у встановленій формі.

3. Діагностика проводиться систематично, у терміни, визначені власником чи керівником організації. Це дозволить вчасно реагувати на загрози, усувати вузькі місця в системі безпеки та підтримувати її ефективність не нижче допустимого рівня.

Інформація про стан безпеки організації, з одного боку, в практичній управлінській діяльності спонукає власників і топ-менеджерів оперативніше ухвалювати більш виважені й ефективніші рішення, а з іншого, – виконує роль своєрідного інвестиційного індикатора.

Питання й завдання для самоконтролю

1. Обґрунтуйте, за яких умов стан соціальної системи можна вважати безпечним та чому саме індикатори безпеки використовуються для його встановлення?

2. Що таке діагностика та яких основних положень діагностики стану безпеки організації необхідно дотримуватися?

3. Наведіть та охарактеризуйте алгоритм діагностики стану безпеки організації.

4. Розкрийте сутність та наведіть основні ознаки оцінки стану безпеки організації за критерієм збитку.

5. Розкрийте сутність та наведіть основні ознаки оцінки стану безпеки організації за коефіцієнтом її платоспроможності.

6. Розкрийте сутність та наведіть основні ознаки, якими необхідно керуватися для оцінки стану безпеки організації за критерієм встановлення протиправного контролю над нею або її активами.

Тема 10

УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЇ

*Управління – це як гра на скрипці,
одночасно це наука й мистецтво,
взяті у глибокій єдності.
Одне й інше людство шукає багато років*

10.1 Безпекова філософія та структура системи управління безпековою діяльністю

Управління як корінна функція соціальної системи виконує інтегруючу роль у забезпеченні її життєдіяльності, оскільки інтегрує через управлінські технології в єдиний процес функції розвитку і безпеки. Водночас в основі управління є безпекова філософія, ядром якої є безпекова культура.

Безпекова філософія управління організацією – це спосіб управлінського мислення та безпекова поведінка у відносинах, які необхідні для збереження цілісності організації.

Основний зміст безпекової філософії управління організацією полягає у збереженні цілісності соціальної системи, створенні внутрішніх і зовнішніх умов, що гарантують їй безпеку, стійкий і поступальний розвиток та реалізацію корпоративних інтересів. Безпекова філософія управління організацією кардинально змінює його цілеспрямовання порівняно з традиційним. Його основною метою є забезпечення в об'єкті управління умов, необхідних для реалізації функцій безпеки і розвитку і на цій основі досягнення запланованого результату.

Управління організацією – це цілеспрямований вплив на об'єкт управління та створення у ньому внутрішніх і зовнішніх умов, необхідних для збереження цілісності соціальної системи, її безпеки, розвитку та реалізації корпоративних інтересів.

У практичній площині безпекова філософія управління організацією реалізується у формі управління функцією безпеки, яке пронизує усі видові функції розвитку та безпеки.

Управління функцією безпеки організації з погляду системного підходу слід розглядати як систему, яка складається з трьох підсистем: керуючої, результуючої та забезпечувальної, з них останні дві входять до керованої підсистеми [51]. Для ефективного управління дуже важливо щоб цій системі були делеговані відповідні повноваження. Під повноваженнями необхідно

розуміти обмежене право розпоряджатися людьми і ресурсами організації або структурного підрозділу для вирішення завдань. Масштаби делегування повноважень залежать від ієрархії управління, посади суб'єкта управління та від того, до якої підсистеми він належить: керуючої, результуючої чи забезпечувальної. Загалом повноваження повинні забезпечити право на ухвалення рішень, організування діяльності, безпосереднє виконання прийнятих рішень та іншої роботи, пов'язаної з ним, а також право на здійснення контролю за діяльністю та її результатами. Наявність таких повноважень у системі управління функцією безпеки організації та їх ефективне застосування дає змогу розпочати діяльність з протидії загрозам і успішно її завершити. Основними видами повноважень мають бути: розпорядчі, організаційні, виконавські та контрольні (рис. 10.1) [51].



Рис. 10.1 Структура системи управління функцією безпеки організації

Формуючи систему управління функцією безпеки організації, слід виходити з того, що вона має складатися з усіх необхідних і одночасно достатніх елементів, між якими має бути налагоджена взаємодія, а також вибудована відповідна ієрархічна структура управління. Водночас обов'язковою умовою є формування ефективних механізмів взаємодії суб'єктів управ-

ління системою безпеки із зовнішнім середовищем, оскільки воно може створювати умови для його розвитку і загрози. Отже, для системи управління функцією безпеки організації властиві такі характеристики: взаємодія із зовнішнім середовищем, наявність необхідних і достатніх компонентів та їх взаємодія, ієрархія структури. Нехтування хоча б однією з них робить систему управління малоефективною або/та затратною.

До керуючої підсистеми належать: керівники і менеджери всіх рівнів, зокрема й начальник служби безпеки.

Керуюча підсистема здійснює свою діяльність через виконання загальних (видових) функцій управління: планування, організування, мотивування, контролювання, внаслідок чого виробляються конкретні методи впливу на результуючу і забезпечувальну підсистеми. Для виконання видових функцій управління, керуюча підсистема отримує певну інформацію від результуючої і забезпечувальної підсистем і зовнішнього середовища. На основі цієї інформації ухвалюються рішення, зокрема про те, як повинні працювати відділи, служби, в тому числі й служба безпеки, а також структури чи фахівці з безпеки, що працюють на умовах договору, які входять до цих підсистем для забезпечення безпеки організації. Керуючій підсистемі делеговані повноваження розпорядчого, організаційного та контрольного характеру.

Результуюча підсистема складається зі служби безпеки, структур чи фахівців з безпеки, що працюють за угодами, а також фахівців, у яких забезпечення безпеки є їх функціональними обов'язками, але не є основною діяльністю, які організують або безпосередньо забезпечують безпеку організації або беруть у цьому процесі участь. Сукупно результуюча підсистема продукує й надає послуги з безпеки та виконує делеговані їй видові функції з безпеки. Для цього вона використовує різні види ресурсів та відповідні засоби: організаційні, технічні, технологічні, психологічні, інформаційні тощо. Їй делеговані повноваження організаційного, виконавчого та контрольного характеру.

Забезпечувальна підсистема не пов'язана з безпековою діяльністю, але створює належні умови для цього процесу та

забезпечує матеріально-технічними і фінансовими ресурсами. До неї входять певні відділи та служби і посадові особи організації. Їй делеговані повноваження лише виконавчого характеру.

Необхідно зазначити, що система управління функцією безпеки має певні особливості, які полягають у тому, що є підрозділи, чи фахівці, які одночасно здійснюють діяльність, пов'язану з функцією розвитку і виконують загальні заходи з безпеки. З огляду на це, вони входять до різних підсистем.

10.2 Сутність, структура та загальна характеристика технології управління безпековою діяльністю

Управління системою безпеки через здійснюється з використанням управлінської технології.

Управлінська технологія – поєднання менеджерських знань, вмінь, використання інформаційної техніки та процесу управління, що необхідні для здійснення бажаних змін в інформації і людях.

Професійні знання та вміння менеджера формуються під час навчання у вищих навчальних закладах, шляхом самоосвіти та безпосередньо під час роботи на керівній посаді або при виконанні управлінських функцій. Менеджеру насамперед потрібно мати відповідну освітню і практичну базу, необхідну для ефективної управлінської праці в будь-якій організації, особливо для управління функцією безпеки. На структуру менеджерських знань і вмінь впливає безпекова філософія управління, що дає змогу:

а) бачити діяльність організації загалом, роль функції безпеки у її життєдіяльності, системно адаптовувати її до впливів внутрішнього і зовнішнього середовища, з огляду на конкретну ситуацію, у тому числі й наявності тих чи інших загроз;

б) кваліфіковано аналізувати проблеми, пов'язані з потенційними чи реальними загрозами;

в) вміло готувати і ухвалювати рішення, передбачаючи водночас їх можливі наслідки;

г) фахово виконувати процедурні дії (заохочувати і карати, цінувати час своїх підлеглих, делегувати повноваження і завдання тощо);

г) ефективно передавати свої ідеї: розробки, накази, розпорядження в усній і письмовій формі та вміло будувати свої стосунки і спілкування з колегами в середині організації і за її межами.

Інформаційна (управлінська) техніка доволі широко використовується в управлінській діяльності, зокрема засоби розмноження документів, засоби отримання, обробки, передачі і розповсюдження інформації (телефон, факс, ксерокопіювальна техніка, комп'ютер тощо).

Управлінський процес є основою технології управління, сутність якого схематично відображено на рисунку 10.2.

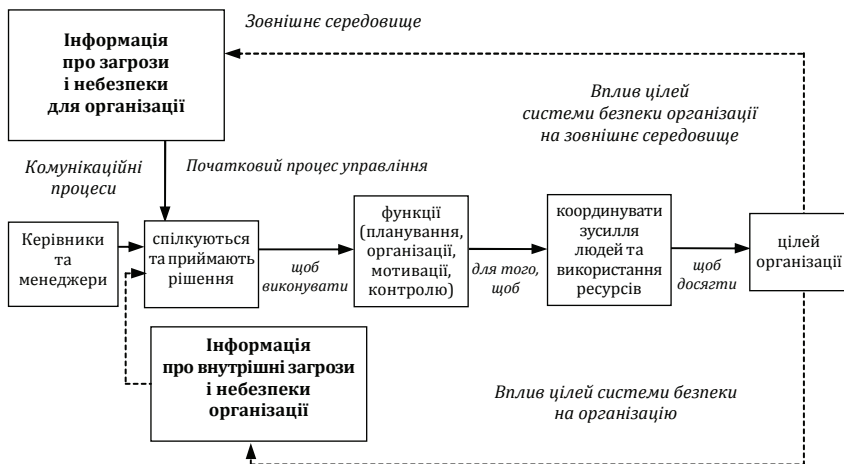


Рис. 10.2 Процес управління безпековою діяльністю організації

Менеджери виконують міжособові й інформаційні ролі, а також такі, що пов'язані з ухваленням рішень з метою ефективного виконання основних (видових) функцій та формування методів управління [50].

Міжособові ролі впливають із повноважень керівника, дозволяючи йому здійснювати керівництво підлеглими, та мати вплив на колег й інших людей, які йому не підпорядковані, але від яких певною мірою залежить ефективність функціонування системи безпеки організації. Основою керівництва є влада і повноваження. Керівництво пронизує всі видові функції управління і є необхідною умовою для ефективного їх виконання.

Інформаційні ролі передбачають формування менеджером комунікаційного процесу всередині системи безпеки і з зовнішнім середовищем. Слід зауважити, що складовими комунікаційного процесу є збір інформації, її аналіз та передання відповідним споживачам: керівництву, підлеглим та іншій цільовій аудиторії. Інформація використовується для ухвалення рішень, виконання видових функцій управління та видових функцій безпеки організації.

Ролі, пов'язані з прийняттям рішень, вимагають від менеджера різних альтернативних дій і вибору найоптимальнішої з них для тієї чи іншої ситуації, особливо коли вона спричинена дією загроз. Управлінські рішення приймаються для кожної функції на підставі певної інформації.

Отже, комунікації та ухвалення рішень є свого роду процесом, який пронизує і пов'язує загальні (видові) функції управління. Тобто вони є складовою кожної видової (загальної) управлінської функції.

Ролі взаємозалежні і взаємодіють для створення єдиного цілого, тобто керівник, маючи повноваження, владу і певну інформацію, може і зобов'язаний ухвалити рішення.

Крім того, менеджер виконує певні видові (загальні) функції управління. Під функціями менеджменту слід розуміти відносно відособлені напрями управлінської діяльності (трудові процеси в сфері управління), які забезпечують управлінську дію. Вони відображають суть і зміст управлінської діяльності на всіх рівнях управління.

В управлінському процесі системою безпеки організацією задіяні чотири основних функції:

а) планування;

- б) організування;
- в) мотивування;
- г) контролювання.

Виконання видових функцій управління завершується розробкою відповідних методів (способів) впливу на окремого працівника, групу, напрям діяльності і загалом на функцію безпеки. Тобто, йдеться про те, що виконання функцій – це розробка того чи іншого методу впливу. Їх є дуже багато, у зв'язку з чим доцільно їх об'єднати у три групи:

- а) економічні;
- б) адміністративні;
- в) соціально-психологічні.

10.3 Сутність та характеристика функцій управління

Планування – це відособлений вид управлінської діяльності, який визначає перспективу розвитку і майбутнього стану системи безпеки організації, а також створює умови для спрямування зусиль всіх її суб'єктів та сил безпеки на досягнення місії та загальних цілей. Планування передбачає, які повинні бути цілі системи безпеки, що слід робити суб'єктам та силам безпеки, щоб їх здійснити.

Планування – це не окрема одноразова дія, а постійний процес, який визначає стратегію дій, спрямованих на забезпечення безпеки, послідовність вирішення завдань, проведення заходів з безпеки.

Під час планування тією чи іншою мірою виконуються функції – організування, мотивування та контролювання, формуються умови, а також конкретні завдання для кожної з функцій безпеки. В управлінській практиці використовують два види планування: **стратегічне та тактичне**.

У процесі стратегічного планування встановлюються цілі системи безпеки, проводиться аналіз і оцінка потенційних і

реальних загроз. Суть стратегічного планування полягає у виробленні стратегії забезпечення безпеки організації.

Планування в організації має бути інтеграційним процесом, процесом розробки концепції безпеки. На думку Г. А. Мінаєва, стратегія розвитку організації, яка не містить елементів, що забезпечують умови для реалізації функції безпеки, не є життєздатною [33, с. 303]. У процесі стратегічного планування беруть участь менеджери всіх рівнів управління та напрямів діяльності, зокрема керівник служби безпеки, виконуючи конкретні завдання. Так, керівники вищої ланки безпосередньо розробляють стратегічний план, а керівники середньої і низової ланок надають відповідну інформацію і забезпечують зворотній зв'язок.

Для реалізації стратегічного плану використовується тактичне планування, яке є логічним продовження стратегічного. Воно покликане сформулювати механізми реалізації обраної стратегії і має два різновиди: поточне і оперативне.

Поточне планування передбачає формування завдань, заходів та умов, необхідних для забезпечення безпеки організації на річний період у напрямку обраної стратегії розвитку. У поточному плані необхідно визначити, що, як, де, коли робити, хто відповідальний, скільки коштів необхідно для того чи іншого виду діяльності та загалом для організації.

Оперативне планування передбачає формування деталізованих, нетривалих планів з конкретних питань діяльності системи безпеки, спрямованих на реалізацію поточних планів. Вони, як правило, є основою для виконання функціональних обов'язків конкретними працівниками.

Необхідно зазначити, що планування здійснюється на підставі відповідної інформації про стан внутрішнього і зовнішнього середовищ та про потенційні й реальні загрози безпеці організації. Ця інформація отримується завдяки виконанню системою безпеки організації інформаційно-оперативної функції, яка, своєю чергою, передбачає використання методів і засобів видових функцій управління та безпеки, особливо аналітично-пошукової, детективної та охоронної діяльності.

Внаслідок планування в організації створюється значна кількість різних за формою, спрямуванням та тривалістю дії планів: *концепція безпеки організації, стратегічний план розвитку, план реалізації стратегії (річний план), кризовий план, план дій у надзвичайних ситуаціях та ін.*

Ефективність діяльності системи безпеки значною мірою залежить від того, який організаційний вплив на неї здійснюється, тобто наскільки фахово виконується функція менеджменту – організування.

Організування – це процес формування структури управління, встановлення зв'язків та відносин, що дає змогу ефективно працювати для досягнення цілей. Цей процес має два аспекти:

- формування організаційної структури відповідно до цілей і стратегій;

- встановлення завдань, повноважень, відносин, які зв'язують вищі рівні з нижчими і забезпечують можливість розподілу і координації та виконання завдань з безпеки.

Формування організаційної структури системи безпеки здійснюється шляхом організаційного проектування, на основі стратегічного плану розвитку та концепції безпеки. Організаційне проектування здійснюється зверху до низу і охоплює такі етапи:

- закріплення видів безпекової діяльності за лінійними та штабними (функціональними) підрозділами.

- встановлення зв'язків між різними підрозділами.

- визначення посадових обов'язків, та/або безпекових завдань у посадових обов'язках, закріплення їх за конкретними посадовими особами.

У процесі організаційного проектування формується організаційна структура системи управління функцією безпеки організації.

Засобом, за допомогою якого встановлюються відносини і повноваження, є делегування, тобто передача завдань і повноважень особі, яка бере на себе відповідальність за їх виконання. Делегування – це спосіб добитися виконання роботи іншими людьми. Тому делегування – акт, який перетворює звичайного працівника на керівника.

Своєю чергою, відповідальність – це обов’язок працівника виконувати поставлені завдання і забезпечувати їх задовільне вирішення. Фактично відповідальність як така, не може бути повністю делегована керівником підлеглому. Йому передається функціональна відповідальність, а управлінська залишається за керівником.

Повноваження – це обмежене право використовувати ресурси організації і спрямовувати зусилля підлеглих працівників на виконання визначених завдань. Повноваження делегуються посаді, а не особі.

У середині організації за допомогою правил та посадових інструкцій визначаються межі повноважень. Що вища посада, то більше повноважень має особа, яка її обіймає. У менеджменті розрізняються лінійні та функціональні повноваження. Лінійні повноваження передаються безпосередньо начальником підлеглому і далі іншим підлеглим. Вони дають узаконену владу. Керівник у межах лінійних повноважень може вирішувати проблеми без погодження з вищими керівниками, з огляду на настанови, закони, звичаї. Делегування лінійних повноважень створює ієрархію рівнів управління системою безпеки організації.

Функціональні повноваження делегуються керівникові для управління певною функцією (фінансами, кадрами, маркетинговою діяльністю, виробництвом, охоронною діяльністю, юридичною діяльністю тощо). Він може і запропонувати, і заборонити ті чи інші дії у сфері своєї компетенції. Лінійні повноваження керівники організації реалізують через функціональні, що можуть реалізовуватися у формі: рекомендаційних повноважень; обов’язкових узгоджень; паралельних повноважень.

З розглянутих повноважень виникають відповідні управлінські відносини.

Управлінські відносини – це зв’язок людей за їх правами, обов’язками та підпорядкуванням один одному в спільній трудовій діяльності. Розрізняють: відносини субординації та відносини координації.

Відносини субординації – це службове підпорядкування молодшого за посадою старшому, виконання правил службової

дисципліни. Відносини субординації складаються між структурними підрозділами системи управління, між керівниками і підлеглими різного рівня.

Відносини координації виникають між органами, структурними підрозділами, керівниками і підлеглими одного рівня за спільної участі у вирішенні завдання з питань безпеки. Координація здійснюється як розпорядча діяльність, за допомогою якої організовується взаємодія виконавців, узгодження дій об'єктів управління і визначається порядок докладання спільних зусиль.

Для успішної реалізації плану та просування організації до цілі слід координувати роботу і вимагати від людей її виконання. Для цього необхідно розуміти і використовувати механізми мотивації людської поведінки.

Мотивування – вид управлінської діяльності, що забезпечує процес спонукання до діяльності для досягнення особистих цілей і цілей організації.

Для мотивування працівників потрібно користуватися запропонованою моделлю механізму мотивації, яка ґрунтується на:

- потребах від яких залежить мотив у працівника до роботи;
- зусиллях, які докладатиме працівник, враховуючи складність завдань;
- винагородах, які отримує працівник за роботу, особливо наскільки вона є для нього справедливою (рис. 10.3).

Використовуючи цю модель, можна передбачити яку віддачу слід очікувати від працівників за тих умов, що у ній створені, а також зрозуміти, як чого найбільшою мірою створюється несприятливе мотиваційне середовище.

Залежно від того, яке мотиваційне середовище в організації, як його оцінює працівник (за цією моделлю), таку він і обирає стратегію або тип поведінки: ініціативний, виконавський, споживацький, відсутній.

Перших два сприяють розвитку корпоративних відносин в організації, а останні можуть створювати загрози для його безпеки.

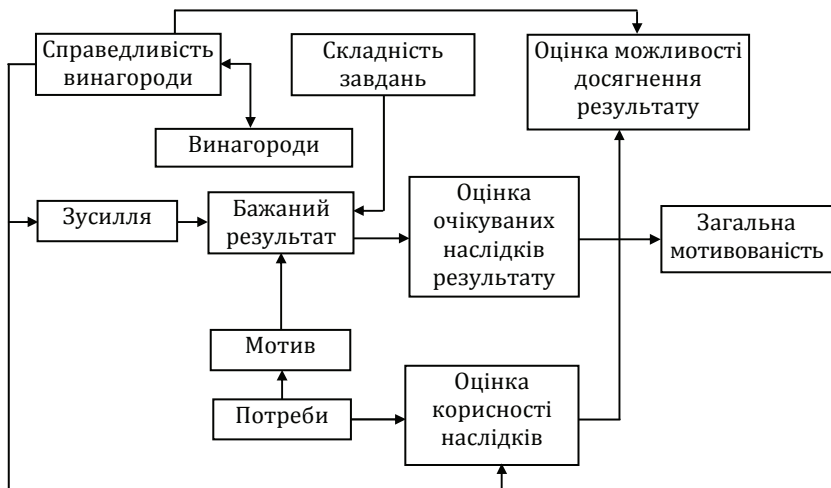


Рис. 10.3 Модель механізму мотивування

Модель механізму мотивації демонструє, що вмотивованість працівника залежить від того, наскільки він упевнений, що за досягнення конкретних результатів він отримає цінну для нього винагороду. Цю впевненість необхідно забезпечити тільки за допомогою прийнятої в організації системи стимулювання, яка б виключала свавілля керівників і невизначеність у способах заохочень, діяла б незалежно від чийх-небудь бажань і настроїв та була б відомою всім членам колективу.

У процесі управління системою безпеки контроль здійснюється з моменту її створення. Без контролю виникає хаос і об'єднати діяльність окремих людей та будь-яких груп стає неможливо.

Контроль – це процес відстеження і вибір напрямів для здійснення необхідних коректив у діяльності організації з метою досягнення очікуваних безпекових результатів.

Саме тому контроль як основний елемент процесу управління не слід розглядати відірвано від планування, формування організаційних структур, мотивації. Фактично всі вони є невід'ємною частиною системи контролю в будь-якій організації. Це стане більш зрозумілим, коли розглянемо основні види контролю: попередній, поточний, завершальний.

Попередній контроль реалізується через правила, процедури, поведінку тощо до фактичного початку роботи. Його основні важелі закладені у процесі реалізації таких функцій менеджменту, як планування, організування взаємодії.

Поточний контроль здійснюється у процесі проведення роботи безпосередньо начальником і передбачає отримання даних про фактичні результати. Регулярна перевірка роботи підлеглих, обговорення проблем, що виникають, пропозиції щодо вдосконалення роботи дають змогу усувати відхилення від планів та інструкцій, тобто ним забезпечується зворотній зв'язок під час роботи.

Завершальний контроль використовується після виконання безпекових завдань (роботи). Фактичні результати порівнюються із запланованими, чи відразу після закінчення роботи, що контролювалася, або після закінчення визначеного терміну. Порівнюючи фактичні результати із запланованими, керівництво має можливість оцінити, наскільки реальними були складені плани. Крім того, завершальний контроль сприяє формуванню мотиваційного середовища в організації, якщо її керівництво пов'язує мотиваційні винагороди з отриманням визначеного результату.

Процес контролю передбачає три етапи:

- а) розробка стандартів;
- б) зіставлення з ними реальних результатів;
- в) вжиття необхідних корегуючих заходів.

На кожному етапі реалізується комплекс різних дій.

Контроль можна проводити у різних формах. Останнім часом набуває широкого застосування контроль у формі аудиту безпеки. Його можна розділити на внутрішній і зовнішній, а за масштабами на аудит: безпеки всієї організації; безпеки окремих приміщень та будинків; обладнання і технічних засобів; окремих видів і напрямів діяльності (фінансової, інформаційної тощо).

Проведення аудиту дає змогу оцінити:

- 1) дотримання законодавства з питань безпеки соціальної системи;
- 2) виконання вимог стандартів і норм з безпеки, запроваджених в організації;
- 3) наявність вузьких місць у системі безпеки організації;

4) стан безпекової культури у менеджерів і фахівців організації;

5) можливі економічні збитки у будь-якій сфері діяльності організації.

Отже, видові (загальні) функції управління: планування, організування, мотивування та контролювання потрібні для того, щоб практично виконувати видові функції розвитку та безпеки, інтегруючи їх у цілеспрямовану діяльність, і на цій основі забезпечувати безпеку і розвиток соціальної системи.

Питання та завдання для самоконтролю

1. Що таке управління організацією та який зміст його безпекової філософії?

2. Яка структура системи управління безпековою діяльністю? Дайте їй характеристику.

3. Розкрийте сутність та структуру технології управління безпековою діяльністю організації, дайте їй загальну характеристику.

4. Розкрийте сутність та структуру процесу управління безпековою діяльністю організації, дайте йому загальну характеристику.

5. Розкрийте сутність планування як загальної функції управління безпековою діяльністю організації.

6. Розкрийте сутність організування як загальної функції управління безпековою діяльністю організації.

7. Розкрийте сутність мотивування як загальної функції управління безпековою діяльністю організації

8. Розкрийте сутність контролю як загальної функції управління безпековою діяльністю організації.

Тести

1. Що є в основі управління соціальною системою з погляду безпеки?

- а) безпекова філософія;
- б) наявність корпоративних інтересів;
- в) безпекова парадигма;
- г) правильні відповіді б, в.

2. Спосіб мислення та безпекова поведінка у відносинах, які необхідні для збереження цілісності організації:

- а) функції розвитку;
- б) безпекова філософія управління організацією;
- в) функції безпеки;
- г) правильні відповіді а і в.

3. Цілеспрямований вплив на об'єкт управління та створення у ньому внутрішніх і зовнішніх умов, необхідних для збереження цілісності соціальної системи, її безпеки, розвитку та реалізації корпоративних інтересів, – це ...

- а) управління організацією;
- б) безпекова філософія управління;
- в) процес управління;
- г) корпоративна культура.

4. Які з наведених повноважень не належать до повноважень системи управління безпековою діяльністю?

- а) розпорядчі;
- б) організаційні;
- в) виконавські;
- г) мотиваційні.

5. Поєднання менеджерських знань, вмінь, використання інформаційної техніки та процесу управління, що необхідні для здійснення бажаних змін в інформації і людях, – це ...

- а) управлінська технологія;
- б) управлінський процес;
- в) методологія;
- г) методика управління.

6. Яка з поданих функцій не належить до основних (видових) управлінських:

- а) планування;
- б) організування;
- в) мотивування;
- г) інформування.

7. Відособлений вид управлінської діяльності, який визначає перспективу розвитку і майбутнього стану системи безпеки органі-

зації, а також створює умови для спрямування зусиль всіх її суб'єктів та сил безпеки на досягнення місії та загальних цілей – це функція:

- а) координування;
- б) планування;
- в) мотивування;
- г) організування.

8. Розроблена концепція безпеки організації – це результат виконання планування:

- а) тактичного;
- б) стратегічного;
- в) оперативного;
- г) поточного.

9. Процес формування структури управління, встановлення зв'язків та відносин, що дає змогу ефективно працювати для досягнення цілей, – це функція:

- а) контролювання;
- б) планування;
- в) мотивування;
- г) організування.

10. Який з наведених видів діяльності не належить до функції організування?

а) закріплення видів безпекової діяльності за лінійними та штабними (функціональними) підрозділами.

б) встановлення зв'язків між різними підрозділами.

в) визначення посадових обов'язків, та/або безпекових завдань у посадових обов'язках, закріплення їх за конкретними посадовими особами;

г) формування плану дій у надзвичайних ситуаціях.

11. Вид управлінської діяльності, що створює мотиваційне середовище, яке спонукає до діяльності для досягнення цілей організації, – це функція:

- а) контролювання;
- б) планування;
- в) мотивування;
- г) організування.

12. Який з поданих елементів не входить до моделі механізму мотивування працівників:

- а) потреби, від яких залежить мотив у працівника до роботи;
- б) зусилля, які докладатиме працівник, враховуючи складність завдань;
- в) винагороди, які отримує працівник за роботу, особливо на скільки вона є для нього справедливою;
- г) розмір винагороди.

13. Процес відстеження і вибір напрямів для здійснення необхідних коректив у діяльності організації з метою досягнення очікуваних безпечових результатів – це функція:

- а) контролювання;
- б) планування;
- в) мотивування;
- г) організування.

14. Який з наведених видів діяльності не належить до структури процесу управлінського контролю?

- а) попередній контроль;
- б) завершальний контроль;
- в) поточний контроль;
- г) господарський.

15. У таблиці подані підсистеми системи управління безпечною діяльністю організації. Кожній підсистемі властиві відповідні повноваження.

Таблиця

Підсистеми управління	Види повноважень системи управління
1. Керуюча	а) розпорядчі; в) виконавчі; б) організаційні; г) контрольні
2. Результативна	
3. Забезпечувальна	

У якому з поданих нижче варіантів правильно запропоновано для кожної підсистеми відповідні повноваження?

- а) 1. а, б, в; 2. а, в, г; 3. в, г;
- б) 1. а, б, г; 2. б, в, г; 3. б, в;
- в) 1. а, в; 2. б, г; 3. б, в, г;
- г) 1. а, б; 2. б, в, г; 3. в, г.

ПРАКТИКУМ З ДІАГНОСТИКИ БЕЗПЕКИ СОЦІАЛЬНИХ СИСТЕМ

Вступ

*Тільки практична діяльність
є тим вимогливим учителем,
який перевіряє доцільність та ефективність
отриманих під час набуття людиною знань
у тій чи іншій галузі та професійній діяльності*

Знання для фахівця варті тоді, коли вони сформовані на рівні умінь. Особливо, коли йдеться про уміння у сфері безпекової діяльності. Їх можна порівняти з уміннями лікаря, діяльність якого складається з двох частин: діагностики хвороби та її лікування. Від якості першої значною мірою залежить ефективність другої. Безпекознавець здійснює діяльність за аналогією лікаря. Відтак йому потрібен відповідний інструментарій, за допомогою якого можна закріпити теоретичні безпекові знання, трансформувавши їх в уміння діагностувати безпекову дійсність.

Запропонований у підручнику практикум спрямований на закріплення теоретичних знань з безпеки соціальних систем на рівні безпекових умінь, а саме на набуття вмінь використувати методики для оцінювання:

- 1) дестабілізуючого впливу загроз соціальній системі;
- 2) стану реалізації безпекових інтересів та корпоративних прав;
- 3) рівня сформованості безпекової культури у соціальній системі;
- 4) ефективності безпекової діяльності соціальної системи;
- 5) стану безпеки соціальної системи.

Ці методики розроблені на прикладі акціонерних товариств, мають відповідне комп'ютерно-програмне забезпечення та можуть успішно використовуватися викладачами вищих навчальних закладів для розробки практичних занять для студентів та підготовки ними кваліфікаційних випускових робіт. Науковцями – для проведення наукових досліджень, а практикаками-безпекознавцями – для підвищення ефективності безпекової діяльності.

Методика діагностики загроз соціальній системі

Суб'єктів господарської діяльності в Україні в процесі функціонування спіткають різні дестабілізуючі чинники. Вони можуть потенційно або реально загрожувати підприємницькій діяльності та загалом існуванню підприємницької структури, руйнуючи її зсередини чи ззовні. Зазначені фактори фахівцями з питань безпеки прийнято називати загрозами існуванню того чи іншого об'єкта.

Загроза – це дія дестабілізуючих природних і (або) суб'єктивних чинників, що спричиняють потенційні або реальні збитки.

Протидію загрозам необхідно розпочинати з їх ідентифікації, тобто необхідно відібрати серед значної кількості ті дестабілізуючі чинники, які можна кваліфікувати і сприймати як загрози. Для цього слід використовувати відповідні методики діагностики.

Під **діагностикою загроз** розуміється вивчення негативного впливу дестабілізуючих чинників в умовах неповної інформації на предмет можливого завдання збитків, погіршення стану процесів, об'єктів чи системи, порушення їх цілісності і на цій основі виявлення потенційних чи реальних загроз.

Для цього пропонується методика діагностики загроз соціальним системам. Вона технологічно інтегрована в управлінські процеси та механізми, що дає змогу вчасно для ухвалення управлінських рішень отримувати інформацію про можливі потенційні чи реальні загрози.

Структурно методика діагностики охоплює:

- 1) вимоги до оцінювання;
- 2) порядок оцінювання;
- 3) якісні і кількісні критерії оцінювання ймовірності загрози та величини можливого дестабілізуючого впливу (збитку);
- 4) якісні і кількісні критерії та формула визначення інтегрального очікуваного показника впливу загрози на об'єкт безпеки, основну сутність та зміст якої подано нижче.

Під час кваліфікації того чи іншого негативного чинника у форму загрози необхідно виходити з того, що загроза завдає організації збитків, погіршує його стан, порушує цілісність процесів, об'єктів.

Для діагностики загроз необхідно сформувати експертну групу на чолі з головним керівником підприємства чи керівником напряму діяльності. До складу експертної групи слід включити найпідготовленіших до аналітично-прогнозної діяльності керівників і фахівців. Доцільно, щоб така експертна група функціонувала як робоча група на постійній основі. Це дає можливість планомірно аналізувати ситуацію і оцінювати рівень її безпеки, а у разі необхідності оперативно оцінювати рівень загрозливості того чи іншого дестабілізуючого чинника. Крім того, систематична робота такої експертної групи сприяє підвищенню рівня знань експертів, формуванню відповідних вмінь та навиків, що, своєю чергою, значно покращує якість аналізу ситуації та її оцінки.

Кваліфікуючи той чи інший дестабілізуючий фактор у загрозу, потрібно здійснити низку технологічних дій:

1. Визначити об'єкт, на який спрямована дія чи вплив дестабілізуючого чинника.

2. Передбачити ймовірність реалізації дестабілізуючого фактора (P), використовуючи якісні та кількісні критерії оцінювання у відносному вираженні:

- малоймовірна загроза – 0,1–0,15;
- потенційна загроза – 0,16–0,99;
- реальна загроза – 1.

3. Визначити величину можливого дестабілізуючого впливу (збитку) (M), використовуючи якісні та кількісні критерії оцінювання у відносному вираженні:

- незначний дестабілізуючий вплив загрози, за якого стан процесів, об'єктів чи системи незначною мірою погіршується, (незначний збиток) – 1;

- помірний дестабілізуючий вплив загрози, за якого стан процесів, об'єктів чи системи погіршується в межах допустимого (помірний збиток) – 2;

– значний дестабілізуючий вплив загрози, за якого стан процесів, об’єктів чи системи значною мірою погіршується (значний збиток) – 3;

– руйнівний дестабілізуючий вплив загрози, за якого стан та чи цілісність процесів, об’єктів чи системи надмірно погіршується, (руйнівний збиток) – 4.

4. Визначити інтегральний очікуваний показник впливу загрози, використовуючи формулу (1):

$$I_{пз} = \frac{K_{e1}(P_1 \times M_1) + K_{e2}(P_2 \times M_2) + K_{en}(P_n \times M_n)}{n^*}, \quad (1)$$

де $I_{пз}$ – інтегральний очікуваний показник впливу загрози, який має таку градацію: 1) незначна загроза 0,01–0,2; 2) помірна загроза 0,21–0,50; 3) значна загроза 0,51–0,8; 4) руйнівна загроза 0,81–1.

K_e – ваговий коефіцієнт думки експерта. Він встановлюється від 0 до 1, причому в сумі має дорівнювати одиниці (2).

$$\sum_{i=1}^n K_{ei} = 1, \quad (2)$$

Розподіл вагових коефіцієнтів залежить від кількості учасників експертної групи, водночас головному експерту встановлюється максимальний ваговий коефіцієнт, решта рівномірно розподіляється між рядовими експертами. У разі наявності експерта, думка якого суттєво відрізняється від середньозваженої думки експертів, йому встановлюється мінімальний коефіцієнт; P – ймовірність загрози (малоймовірна загроза – 0,1–0,15; потенційна загроза – 0,16–0,99; реальна загроза – 1); M – можливий дестабілізуючий вплив (незначний збиток – 1; помірний збиток – 2; значний збиток – 3; руйнівний збиток – 4); n – кількість експертів; n^* – деякий адаптаційний параметр, пов’язаний з кількістю експертів. Під час використання чотирьох експертів $n^* = n$. В усіх інших випадках його числове значення визначається максимальним значенням параметра M , тобто $n^* = M_{max}$, якщо $n \neq 4$.

Отримавши в такий спосіб інформацію про інтегральний очікуваний показник впливу загрози, можна визначити найнебезпечніші загрози та рівень їх негативного впливу у відносному вираженні. Результати експертних оцінювань доцільно відображати у формі таблиці.

Таблиця

Оцінка загроз підприємству

№ з/п	Зміст загрози	Ймовірність загрози	Величина можливого збитку	Інтегральний показник впливу загрози
1.	Використання конкурентом комерційної таємниці, у зв'язку з неправомірним вилученням документів, що містять комерційну таємницю	0,79 0,83 0,56 0,64	3 3 4 3	Значна загроза (0,56)
2.	Розкрадання матеріальних цінностей особами, що працюють в організації	0,20 0,31 0,25 0,46	2 2 2 2	Незначна загроза (0,14)
3.	Низький рівень захисту комп'ютерних систем від несанкціонованого доступу	0,89 0,80 0,87 0,75	3 3 3 3	Значна загроза (0,63)

5. Сформувати перелік загроз, виділивши їх у групи:

- а) руйнівні загрози;
- б) значні загрози;
- в) помірні загрози;
- г) незначні загрози.

Загрози, які оцінені як руйнівні та значні, потребують термінової ліквідації, починаючи з руйнівних. Помірні загрози також повинні перебувати під наглядом керівництва і мають бути якомога скоріше усунені.

Ця методика має відповідне програмне забезпечення, відтак на практиці застосовується як комп'ютерна діагностика загроз соціальній системі.

Методика діагностики реалізації безпекових корпоративних інтересів

За *діагностикою реалізації безпекових корпоративних інтересів* можна визначити здатність АТ протидіяти внутрішнім і зовнішнім загрозам або навпаки. Пояснюється це тим, що АТ з усіх основних функцій розвитку (виробничої, фінансової, маркетингової, кадрової діяльності) планує конкретні цілі на підставі корпоративних інтересів відповідних учасників економічних відносин. Для досягнення цих цілей в АТ планується і проводиться великий за обсягом комплекс видів діяльності, робіт, операцій. На заваді їм стають внутрішні і зовнішні загрози. Це об'єктивний процес, саме так здійснюється процес життєдіяльності будь-якої організації, зокрема й АТ. Досягнути запланованих цілей можна не тільки через якісне виконання робіт, операцій тощо, а й ефективну протидію загрозам, тобто в комплексному поєднанні видів діяльності, спрямованих на досягнення обраних цілей і протидії загрозам. Якщо АТ досягає запланованих цілей, то це свідчить й про здатність системи безпеки протидіяти загрозам і в такий спосіб створювати умови для реалізації цілей і загалом функцій розвитку та може бути одним із критеріїв інвестиційної привабливості. У кожного з учасників корпоративних відносин є інтереси розвитку та інтереси безпеки. Реалізація в АТ інтересів безпеки створює певні умови для реалізації інтересів розвитку. Тому всі учасники економічних відносин зацікавлені в їх реалізації. Критерієм інвестиційної привабливості виступають не тільки показники розвитку (прибуток, дохідність акції тощо), а й показники безпеки (надзвичайні ситуації, конфлікти, стан розрахунків з державою, партнерами, постачальниками, кредиторами, безпечні умови праці тощо). Наявність в АТ позитивних показників за цими критеріями свідчить про те, що власники і топ-менеджери приділяють корпоративним інтересам з безпеки значну увагу. Це створює умови для формування привабливого для інвесторів АТ середовища. З часом

таке підприємство буде успішним і на ринку товарів, і на фондовому ринку.

Для діагностики рівня реалізації безпекових корпоративних інтересів експертам потрібно дати відповідь на низку питань, перелік яких може бути уточненим, зменшеним чи збільшеним. Це залежить від конкретного АТ. Оцінювання проходить шляхом заповнення експертом експертного листа, що поданий далі.

Експертний лист оцінки стану реалізації безпекових корпоративних інтересів

Прізвище, ім'я, по батькові _____

Посада _____

Науковий ступінь (якщо є) _____

Алгоритм оцінювання: уважно прочитайте питання і дайте відповідь, поставивши відмітку навпроти нього у правій колонці таблиці, обравши одну з трьох.

Таблиця

Перелік питань для діагностики реалізації безпекових корпоративних інтересів

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	Чи є ознаки переходу контролю над АТ від акціонерів-власників до групи осіб вищого менеджменту?			
2.	Чи є ознаки переходу власності АТ від акціонерів-власників до групи осіб вищого менеджменту?			
3.	Чи є сприятливі умови в АТ для вчинення правопорушень у процесі придбання товаро-матеріальних цінностей (ТМЦ) та інших ресурсів?			
4.	Чи є сприятливі умови в АТ для вчинення правопорушень у процесі збереження ТМЦ й інших ресурсів?			

5.	Чи є сприятливі умови в АТ для вчинення правопорушень у процесі руху ТМЦ та інших ресурсів у середині підприємства?			
6.	Чи є сприятливі умови в АТ для вчинення правопорушень у процесі відпуску ТМЦ та інших ресурсів у виробництво та їх використанні у виробничому процесі?			
7.	Чи є сприятливі умови в АТ для вчинення порушень у процесі відпуску ТМЦ й інших ресурсів у виробництво та їх використанні у виробничому процесі?			
8.	Чи є сприятливі умови в АТ для вчинення порушень у процесі готової продукції, робіт, послуг?			
9.	Чи є сприятливі умови в АТ для вчинення порушень у процесі реалізації готової продукції, робіт, послуг?			
10.	Чи є сприятливі умови в АТ для вчинення порушень у процесі розрахунків із контрагентами?			
11.	Чи є сприятливі умови в АТ для вчинення порушень у процесі розрахунків з оплати праці та її оптимізації?			
12.	Чи є сприятливі умови в АТ для вчинення порушень у процесі розрахунків і виплати дивідендів?			
13.	Чи є сприятливі умови в АТ для вчинення порушень у процесі розрахунків зі сплати податків?			
14.	Чи є сприятливі умови в АТ для вчинення порушень у процесі фінансових операцій?			
15.	Чи є сприятливі умови в АТ щодо порушень вимог охорони праці?			
16.	Чи є сприятливі умови в АТ щодо виникнення надзвичайних ситуацій?			
17.	Чи є сприятливі умови в АТ щодо порушень технологічних вимог якості та безпечності продукції?			
18.	Чи є перешкоди щодо виконання АТ договірних зобов'язань із кредиторами, постачальниками, партнерами?			
19.	Чи є ознаки функціонування супутньої (додаткової) структури, яка діє з метою нанесення збитку АТ на користь посадової особи			

Дата експертної оцінки _____ 20 __ р. _____

підпис

Кожне питання (параметр оцінки) оцінюється якісно та кількісно, користуючись критеріями та бальною шкалою: «так» – 0; «важко відповісти» – 0,5; «ні» – 1.

Визначення коефіцієнта захисту корпоративних інтересів з безпеки за результатами експертного оцінювання здійснюється за формулою:

$$K_{ib} = \left(\frac{\sum_{i=1}^{Ke} \sum_{j=1}^N E_{oij}}{Ke} \right) / N,$$

де K_{ib} – коефіцієнт реалізації інтересів безпеки; Ke – кількість експертів; N – кількість параметрів діагностики; E_{oij} – експертна оцінка i -тим експертом j -параметра діагностики; $\sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики i -тим експертом ($i=Ke$); $\sum_{i=1}^{Ke} \sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики експертною групою.

Діагностуючи рівень реалізації корпоративних інтересів безпеки в АТ за наведеним коефіцієнтом доцільно використовувати умовні величини – від 0 до 1 та характерні ознаки, а саме:

$K_{ib} = 0-0,20$ – корпоративні інтереси з безпеки практично нереалізовані;

$K_{ib} = 0,21-0,50$ – корпоративні інтереси з безпеки реалізовані недостатньо;

$K_{ib} = 0,51-0,80$ – корпоративні інтереси з безпеки реалізовані більшою мірою.

$K_{ib} = 0,81-1$ – корпоративні інтереси з безпеки реалізовані повною мірою.

За результатами оцінювання потрібно зробити аналіз, зауваживши на недоліки й причини, та підготувати висновок.

Методика діагностики стану справ в акціонерному товаристві із захистом корпоративних прав

За коефіцієнтом захисту корпоративних прав можна визначити потенційність чи реальність корпоративного конфлікту, який може спричинити небезпеку для АТ. Пояснюється це тим, що акціонери згідно з Законом України «Про акціонерні товариства» володіють правом власності на частину корпоративного капіталу, що засвідчується акцією. Щоб отримати належну ту чи іншу частку капіталу у вигляді дивідендів акціонер повинен бути активним і цікавитися не тільки результатами діяльності АТ, а й самим процесом, особливо процесом корпоративного управління. Така активність акціонерів, як правило, через різні причини і обставини не вигідна вищому менеджменту АТ, або сприймається ним як щось другорядне через низьку корпоративну і управлінську культуру. Відтак свідомо чи в результаті бездіяльності відповідних менеджерів АТ створюються різні перешкоди щодо активної участі акціонерів у корпоративному управлінні.

Власникам і акціонерам та загалом АТ як суб'єкта господарювання важливо, щоб на підприємстві не було перешкод для реалізації корпоративних прав. Для цього потрібна відповідна і водночас проста методика оцінки, яка б дозволяла отримувати інформацію про можливість виникнення корпоративного конфлікту з приводу штучних перешкод для реалізації корпоративних прав.

Оцінюючи умови, що мали би створюватися в АТ для реалізації корпоративних прав, необхідно послуговуватися Законом України «Про акціонерні товариства» та Статутами АТ, де вони виписані. Аналіз цих документів дасть змогу сформулювати перелік питань, відповіді на які дозволяють отримати інформацію про стан справ у тому чи іншому АТ з корпоративними правами. Перелік запитань може бути уточненим, зменшеним чи збільшеним, що залежить від конкретного АТ.

Для оцінки рівня реалізації корпоративних прав експертам потрібно відповісти на наведені у експертному листі питання. Кожне питання (параметр оцінки) оцінюється якісно та

кількісно, користуючись критеріями та бальною шкалою: «так» – 0; «важко відповісти» – 0,5; «ні» – 1.

Експертний лист оцінки стану реалізації корпоративних прав

Прізвище, ім'я, по батькові _____

Посада _____

Науковий ступінь (якщо є) _____

Алгоритм оцінювання: уважно прочитайте питання і дайте відповідь, поставивши відмітку навпроти нього у правій колонці таблиці, обравши одну з трьох.

Таблиця

Перелік питань для діагностики стану реалізації корпоративних прав

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	Чи затримують акціонерам виплату дивідендів, або не розподіляють і не виплачують їх?			
2.	Чи є перешкоди у АТ щодо розподілу між акціонерами, відповідно їх вкладу, частину його майна або вартості у разі його ліквідації?			
3.	Чи є перешкоди у АТ щодо отримання акціонером інформації про господарську діяльність та структуру капіталу?			
4.	Чи порушуються вимоги щодо вчасного повідомлення акціонера про скликання загальних зборів АТ, дату і місце їх проведення та порядок денний?			
5.	Чи є перешкоди у АТ, які б не дозволяли акціонерові (учаснику) своєчасно та у зручний спосіб ознайомлюватися з матеріалами, пов'язаними з порядком денним загальних зборів АТ?			
6.	Чи є перешкоди у АТ, які б не дозволяли акціонерові (учаснику) вносити пропозиції до порядку денного загальних зборів?			

7.	Чи є перешкоди у АТ, які б не дозволяли акціонерів (учаснику) брати участь в обговоренні та голосуванні з питань порядку денного особисто або заочно?			
8.	Чи є перешкодою регламент та процедура загальних зборів щодо забезпечення рівних умов для всіх акціонерів?			
9.	Чи існувало відсторонення акціонерів від голосування на загальних зборах?			
10.	Чи є перешкоди у АТ, які б не дозволяли акціонерів (учаснику) брати участь у виборах керівних органів АТ?			
11.	Чи є перешкоди у АТ, які б заважали акціонерів скористатися «переважним правом акціонера», тобто правом власника простих (чи привілейованих) акцій придбавати розміщені товариством прості (або відповідно – привілейовані) акції пропорційно частці належних йому акцій у загальній кількості акцій певного виду?			
12.	Чи було вимагання посадовими особами АТ від акціонера – працівника товариства надання відомостей про те, як він голосував чи який має намір голосувати на загальних зборах?			
13.	Чи було вимагання посадовими особами АТ від акціонера – працівника товариства надання відомостей про відчуження акціонером – працівником товариства своїх акцій чи намір їх відчуження?			
14.	Чи є вимагання посадовими особами АТ від акціонера – працівника товариства надання відомостей про передання довіреності на участь у загальних зборах?			
15.	Чи ухвалюються рішення щодо внесення змін до статуту без запрошення на загальні збори міноритарних акціонерів, у яких пакет акцій менший за блокуючий?			
16.	Чи приймаються рішення щодо додаткового випуску акцій без запрошення на загальні збори міноритарних акціонерів, у яких пакет акцій менший за блокуючий?			
17.	Чи проводяться загальні збори акціонерів без повідомлення частини міноритарних акціонерів із приводу збільшення статутного фонду товариства?			
18.	Чи проводяться загальні збори акціонерів без повідомлення частини міноритарних акціонерів			

	із приводу вибору реєстратора іменних цінних паперів?			
19.	Чи проводяться загальні збори акціонерів без повідомлення частини міноритарних акціонерів з приводу реорганізації товариства?			

Дата експертної оцінки _____ 20 __ р. _____
підпис

Визначити коефіцієнт захисту корпоративних прав за результатами експертного оцінювання можна використовуючи формулу:

$$K_{zp} = \left(\frac{\sum_{i=1}^{Ke} \sum_{j=1}^N E_{oij}}{Ke} \right) / N,$$

де K_{zp} – коефіцієнт захисту корпоративних прав; Ke – кількість експертів; N – кількість параметрів діагностики; E_{oij} – експертна оцінка і-тим експертом j-параметра діагностики; $\sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики і-тим експертом ($i=Ke$); $\sum_{i=1}^{Ke} \sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики експертною групою.

Для діагностики рівня реалізації корпоративних прав в АТ за наведеним коефіцієнтом доцільно використовувати умовні величини – від 0 до 1 та характерні ознаки, а саме:

$K_{zp} = 0-0,20$ – корпоративні права практично нереалізовані;

$K_{zp} = 0,2-0,50$ – корпоративні права реалізовані недостатньо;

$K_{zp} = 0,51-0,80$ – корпоративні права реалізовані більшою мірою;

$K_{zp} = 0,81-1$ – корпоративні права реалізовані повною мірою.

За результатами оцінювання потрібно зробити аналіз, взявши до уваги й причини, та підготувати висновок.

Методика діагностики безпекової корпоративної культури

Ефективність безпекової діяльності значною мірою залежить від **рівня сформованості безпекової корпоративної культури** в організації. Діагностуючи рівень вияву безпеки через корпоративну культуру, необхідно зважати, що її сформованість залежить від безпекових цінностей, поведінкових норм, знань з питань теорії та практики безпеки й управління засновниками і вищим менеджментом організації.

Експертна оцінка дає змогу з'ясувати, наскільки поведінка менеджерів і працівників, їх професійна діяльність спрямовані на забезпечення цілісності підприємства як системи. Для діагностики рівня реалізації безпекових корпоративних інтересів експертам потрібно відповісти на низку питань, перелік яких може бути уточненим, зменшеним чи збільшеним. Оцінювання відбувається шляхом заповнення експертного листа. Кожне питання (параметр оцінки) оцінюється якісно та кількісно, користуючись критеріями та бальною шкалою:

«так» – 0;

«важко відповісти» – 0,5;

«ні» – 1.

За результатами оцінювання формується певна сума балів.

Експертний лист оцінки безпекової корпоративної культури

Прізвище, ім'я, по батькові _____

Посада _____

Науковий ступінь (якщо є) _____

Алгоритм оцінювання: уважно прочитайте питання і дайте відповідь, проставивши відмітку на проти нього у правій колонці таблиці, обравши одну з трьох.

**Перелік питань для діагностики сформованості
безпекової корпоративної культури в організації**

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	Чи вважаєте Ви, що в АТ безпека становить одну з основних умов його розвитку?			
2.	Чи вважаєте Ви, що в АТ заходи і засоби безпеки є складовими виробничих, інформаційних і технологічних процесів?			
3.	Чи вважаєте Ви, що в АТ заходи безпеки є складовими корпоративних, соціальних і управлінських відносин?			
4.	Чи є, на Вашу думку, в АТ така робоча атмосфера і стосунки, завдяки яким працівники відмовилися б від надання допомоги іншим особам в отриманні конфіденційної інформації в обмін на винагороду?			
5.	Чи є, на Вашу думку, в АТ така робоча атмосфера і стосунки, за яких працівники поінформували б керівника підприємства чи служби безпеки про спробу третіх осіб отримати від них допомогу в отриманні комерційної таємниці чи здійсненні іншої протиправної діяльності?			
6.	Чи є у менеджерів і працівників нетерпимість до фактів крадіжок та інших порушень в АТ?			
7.	Чи є прерогативою безпека товарів, робіт, послуг у відносинах між АТ і споживачами та складовою технологічної політики підприємства й технологічних процесів?			
8.	Чи є у відносинах між вищим менеджментом АТ і працівниками не сприйняття такого явища як дискримінація?			
9.	Чи поділяється в колективі думка, про те, що дотримання екологічних стандартів – це соціальна відповідальність за безпечність навколишнього середовища?			
10.	Чи поділяється в колективі думка, про те, що дотримання АТ зобов'язань з економічними			

	контрагентами – це зменшення збитків для підприємства і формування іміджу відповідального партнера?			
11.	Чи поділяється у середовищі вищого менеджменту АТ позиція, згідно з якою, маніпуляції з інвестиціями неприпустимі?			
12.	Чи поділяється у середовищі вищого менеджменту АТ позиція, згідно з якою, таємні угоди (зговір) на ринку неприпустимі?			
13.	Чи поділяється у середовищі вищого менеджменту АТ позиція, згідно з якою, недобросовісна звітність та облік неприпустимі?			
14.	Чи вважаєте Ви, що питання забезпечення безпеки АТ – це обов’язок і право власника та кожного менеджера і працівника?			
15.	Чи вважається в АТ нормою обговорення і ухвалення рішень з питань безпеки?			

Дата експертної оцінки _____ 20 __ р. _____
підпис

Визначити коефіцієнт безпекової корпоративної культури за результатами експертного оцінювання можна використовуючи формулу:

$$K_{bk} = \left(\frac{\sum_{i=1}^{K_e} \sum_{j=1}^N E_{oij}}{K_e} \right) / N,$$

де K_{bk} – коефіцієнт безпекової корпоративної культури; K_e – кількість експертів; N – кількість параметрів діагностики; E_{oij} – експертна оцінка і-тим експертом j-параметра діагностики; $\sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики і-тим експертом ($i=K_e$); $\sum_{i=1}^{K_e} \sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики експертною групою.

Для оцінки рівня безпекової корпоративної культури в організації за наведеним коефіцієнтом доцільно використо-

увати умовні величини – від 0 до 1 та характерні ознаки, а саме:

$K_{bk} = 0-0,2$ – безпекова корпоративна культура в організації практично не сформована;

$K_{bk} = 0,21-0,5$ – безпекова корпоративна культура в організації сформована незначною мірою;

$K_{bk} = 0,51-0,8$ – безпекова корпоративна культура в організації сформована значною мірою;

$K_{bk} = 0,81-1$ – безпекова корпоративна культура в організації сформована достатньою мірою і сприяє формуванню умов, необхідних для розвитку підприємства.

За результатами оцінювання потрібно зробити аналіз, взявши до уваги прогалини й причини та підготувати висновок.

**Методика
діагностики та визначення рівня ефективності
безпекової діяльності**

Безпечний рівень організації залежить від ефективності її діяльності загалом, зокрема й безпекової, а саме її механізмів:

- 1) інформаційно-виявляючих;
- 2) попереджувально-профілактичних;
- 3) ліквідаційних
- 4) відновлювальних.

Під **ефективністю безпекової діяльності** розуміється вчасне документування правопорушень та отримання інформації про потенційні чи реальні загрози, їх попередження чи ліквідацію.

Для діагностики ефективності виконання наведених механізмів експертам потрібно оцінити низку тверджень, що подані у експертному листі. Кожне питання (параметр оцінки) оцінюється якісно та кількісно, користуючись критеріями та бальною шкалою:

«так» – 0;

«важко відповісти» – 0,5;

«ні» – 1.

За результатами оцінювання формується певна сума балів.

**Експертний лист оцінки ефективності
безпекової діяльності організації**

Прізвище, ім'я, по батькові _____

Посада _____

Науковий ступінь (якщо є) _____

Алгоритм оцінювання: уважно прочитайте питання і дайте відповідь, проставивши відмітку напроти нього у правій колонці, обравши одну з трьох.

Таблиця 1

**Перелік питань
для діагностики ефективності реалізації
інформаційно-виявляючих механізмів безпекової діяльності**

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	Використовуючи технології аналітично-пошукової діяльності, вищий менеджмент і власники АТ вчасно отримують інформацію про потенційні чи реальні загрози стратегічного характеру з боку зовнішнього середовища (основного конкурента, держави у вигляді зміни законодавства тощо).			
2.	Використовуючи технології аналітично-пошукової діяльності, вищий менеджмент і власники АТ вчасно отримують інформацію про потенційні чи реальні загрози стратегічного характеру з боку внутрішнього середовища (про рівень зносу виробничих фондів, про зниження кваліфікації персоналу тощо).			
3.	Використовуючи технології детективної діяльності, вищий менеджмент і власники АТ вчасно отримують інформацію про потенційні чи реальні загрози протиправного характеру з боку зовнішнього середовища і на ринку (підробку продукції, недобросовісну рекламу, рейдерське захоплення АТ тощо).			
4.	Використовуючи технології детективної діяльності, вищий менеджмент і власники АТ вчасно отримують інформацію про потенційні чи реальні загрози протиправного характеру в середині підприємства (наміри про виведення чи розмивання капіталу, наміри про підтримку групи осіб у рейдерському захопленні АТ тощо).			
5.	Використовуючи технології фізичної охорони, вищий менеджмент і власники АТ вчасно отримують інформацію про вчинення різних порушень всередині підприємства (крадіжки, спроби чи факти порушення встановленого режиму тощо).			

6	Використовуючи технології технічної охорони вищий менеджмент і власники АТ вчасно отримують інформацію про вчинення різних порушень у середині підприємства (крадіжки, спроби чи факти знищення чи ушкодження майна тощо).			
7.	Комунікаційні процеси в АТ організовані так, що унеможливають виникнення і розповсюдження неправдивої інформації, яка здатна порушити встановлений порядок управління, спровокувати конфлікти і в такий спосіб нанести підприємству збитки.			
8.	Комунікаційні процеси в АТ організовані так, що сприяють інформуванню відповідних керівників працівниками про можливі та реальні порушення на ринку і всередині підприємства.			
9.	Система контролю в АТ організована так, що дозволяє отримувати інформацію про невиконання чи неефективне виконання функціональних обов'язків, внаслідок чого підприємству завдаються збитки.			
10.	Система контролю в АТ організована так, що дозволяє отримувати інформацію про порушення внутрішнього розпорядку та встановлених режимів роботи підприємства та допусків до комерційної таємниці, в результаті чого підприємству наносяться збитки.			
11.	Проведення в АТ інвентаризації дає змогу виявляти проблеми чи порушення обліку і зберігання матеріальних цінностей.			
12.	Проведення в АТ аудиторської перевірки дозволяє виявляти неефективне використання капіталу, що опосередковано завдає збитків.			
13.	Проведення в АТ аудиту економічної безпеки дає можливість виявляти прогалини в системі економічної безпеки АТ.			
14.	Проведення в АТ перевірки фінансово-господарської діяльності дозволяє виявляти порушення, якими завдаються збитки.			
15.	Комунікаційні процеси в АТ організовані так, що є можливість інформувати працівників про необхідність протидії різним порушенням та проведення відповідного навчання.			
16.	Для отримання інформації про потенційні чи реальні загрози або її передання в АТ використовуються збори, наради.			

17.	Для здійснення оперативно-інформаційної функції в АТ створені відповідні організаційні умови і можливості: у положеннях про підрозділ чи у функціональних обов'язках відповідних фахівців передбачені конкретні види діяльності, що впливають з цієї функції тощо.			
18.	Використовуючи технології детективної діяльності, факти загрози протиправного характеру документуються вчасно і якісно.			

Таблиця 2

**Перелік питань
для діагностики ефективності
попереджувально-профілактичних механізмів
безпекової діяльності організації**

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	Встановлений в АТ пропускний режим є перешкодою для вчинення тих чи інших порушень (самовільний вивіз матеріальних цінностей, проникнення на територію з метою завдання збитків тощо).			
2.	Патрулювання охоронниками території АТ і вартова служба створюють умови, за яких учинення крадіжок, знищення майна тощо стає доволі складним процесом.			
3.	Протипожежні заходи, які проводяться в АТ, дають змогу створити умови, за яких ймовірність виникнення пожежі залишається незначною.			
4.	Фізична охорона відповідних посадових осіб АТ організується, з огляду на потенційні загрози для їх здоров'я чи життя.			
5.	Використовуючи методи детективної діяльності, вчасно виявляються наміри щодо вчинення правопорушень, спрямованих на завдання збитків АТ.			
6.	В АТ використовуються технічні засоби для попередження витоку інформації з відповідних			

	приміщень, що може зніматися спеціальними пристроями дистанційного відеоспостереження.			
7.	В АТ використовуються технічні засоби для попередження витоку інформації з обчислювальних систем.			
8.	В АТ використовуються технічні засоби для попередження витоку інформації з засобів зв'язку.			
9.	В АТ створена необхідна нормативно-правова база з питань економічної безпеки (норми з питань безпеки в Статуті, концепція економічної безпеки, положення про захист інформації тощо).			
10.	В АТ запроваджена внутрішня експертиза нормативних документів на предмет захисту корпоративних економічних інтересів та прав.			
11.	В АТ практикується консультування працівників з питань забезпечення їх безпеки під час здійснення професійної діяльності.			.
12.	У разі неправомірних дій чи бездіяльності менеджерів чи інших працівників АТ здійснюється відповідна правова їх оцінка.			
13.	В АТ створено необхідні умови для забезпечення безпеки технологічних процесів, виробничого устаткування, будівель, споруд.			
14.	В АТ створено необхідні, з погляду санітарно-гігієнічних вимог, умови праці.			
15.	Працівники АТ під час виконання небезпечних для здоров'я видів робіт забезпечені засобами колективного й індивідуального захисту.			
16.	У планах усіх видів діяльності АТ передбачено відповідні заходи з безпеки.			
17.	В АТ розроблені відповідні плани дій на випадок надзвичайних ситуацій.			
18.	Заробітна плата і преміювання менеджерів і працівників АТ є такими, що не спонукають їх до цілеспрямованого і свідомого завдання збитків, використовуючи для цього різні методи і форми.			
19.	Відносини між керівниками і підлеглими та в загалом у колективі АТ є такими, що не спонукають їх до цілеспрямованого і свідомого завдання збитків, використовуючи для цього різні методи і форми.			
20.	В АТ створена і діє система контролю за роботою менеджерів і працівників, про яку добре поінформований колектив.			

21.	В АТ створена і діє система контролю зберігання і використання товарно-матеріальних цінностей, про яку добре поінформований колектив.			
22.	В АТ створена і діє система контролю фінансово-господарської діяльності, про яку добре поінформований колектив.			
23.	Для забезпечення економічної безпеки в АТ створена і організаційно оформлена система безпеки.			
24.	Обов'язки щодо координації діяльності, пов'язаної з забезпеченням економічної безпеки АТ, покладено на відповідного керівника.			
25.	Для забезпечення економічної безпеки АТ створена власна служба безпеки або на умовах угоди залучаються зовнішні відповідні структури.			

Таблиця 3

**Перелік питань
для діагностики ефективності
реалізацією ліквідаційних механізмів
безпекової діяльності організації**

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	Використовуючи методи і засоби фізичної охорони, протиправні дії осіб в АТ припиняються вчасно.			
2.	Ліквідація загроз технічного характеру в АТ здійснюється вчасно завдяки використанню методів засобів технічної охорони.			
3.	Припинення витоку інформації з обчислювальних систем, засобів зв'язку та спеціальних приміщень АТ здійснюється вчасно внаслідок використання відповідних технічних засобів.			
4.	Припинення загроз протиправного характеру АТ здійснюється вчасно за допомогою методів і засобів юридичного захисту.			

5.	Загрози корпоративним економічним інтересам та правам АТ ліквідуються при використанні судової системи.			
6.	Загрози корпоративним економічним інтересам та правам АТ ліквідуються, використовуючи правоохоронні та контрольні органи держави.			
7.	Пом'якшення і мінімізації збитку АТ здійснюється завдяки вчасному і якісному документуванню фактів протиправного характеру, що їх спричинили.			
8.	В АТ розроблені й узгоджені плани дій структурних підрозділів і персоналу для ліквідації загроз надзвичайного характеру.			
9.	Система контролю АТ дає змогу вчасно припинити зловживання менеджерами і невиконання чи неналежне виконання роботи працівниками.			
10.	Система контролю АТ дозволяє вчасно припинити зловживання під час зберігання та використання товарно-матеріальних цінностей і грошових коштів, використовуючи методи інвентаризації, спеціальні методи економічного аналізу, методи дослідження документів та методи фактичного контролю за господарськими операціями.			
11.	Система контролю АТ дає змогу вчасно припинити зловживання у фінансово-господарській діяльності, використовуючи методи аудиту та ревізії.			
12.	В АТ створені всі необхідні механізми і організаційні структури або залучені зовнішні для ліквідації загроз.			
13.	Між АТ і ОВС розроблено ефективні механізми взаємодії для ліквідації тих чи інших правопорушень.			
14.	Між АТ і страховими компаніями укладено відповідні страхові угоди з метою мінімізації збитків у разі їх настання.			
15.	Відшкодування збитків, яких зазнало АТ, здійснюється в необхідному для розвитку обсязі, при використанні механізмів страхування.			
16.	Відшкодування збитків, яких зазнало АТ, здійснюється з резервного фонду, виходячи з його можливостей.			
17.	Відшкодування збитків, яких зазнало АТ, здійснюється в необхідному для розвитку обсязі, за допомогою використання механізмів довготермінового кредитування.			

Дата експертної оцінки _____ 20 __ р. _____

підпис

Таблиця 4

**Перелік питань
для діагностики ефективності
реалізацією відновлювальних механізмів
безпекової діяльності організації**

№	Параметри оцінювання	Критерії оцінки		
		Так	Важко відповісти	Ні
1.	В АТ розроблені й узгоджені механізми дій менеджменту для відновлення діяльності після довготривалого вимушеного простою через відсутність постачання відповідних ресурсів для виробництва.			
2.	В АТ розроблені й узгоджені механізми дій менеджменту для відновлення діяльності після завершення страйку працівників.			
3.	В АТ розроблені й узгоджені механізми дій структурних підрозділів і персоналу для відновлення діяльності після безпідставного рішення державних органів про вилучення документів, тимчасового припинення діяльності тощо.			
4.	В АТ розроблені й узгоджені механізми дій структурних підрозділів і персоналу для відновлення діяльності після спроби рейдерського захоплення			
5.	В АТ розроблені й узгоджені механізми дій структурних підрозділів і персоналу для відновлення діяльності після реалізації загроз (аварія, техногена аварія, пожежа)			
6.	Відшкодування збитків, яких зазнало АТ, здійснюється за допомогою використання механізмів добровільного відшкодування, визначених у відповідних договорах між АТ та іншим суб'єктом.			
7.	Відшкодування збитків, яких зазнало АТ, здійснюється за допомогою використання судових механізмів.			

8.	Відшкодування збитків, яких зазнало АТ, здійснюється за допомогою використання механізмів матеріального відшкодування.			
9.	Між АТ і страховими компаніями укладено відповідні страхові угоди з метою мінімізації збитків у разі їх настання.			
10.	Відшкодування збитків, яких зазнало АТ, здійснюється в необхідному для розвитку обсязі, при використанні механізмів страхування.			
11.	Відшкодування збитків, яких зазнало АТ, здійснюється з резервного фонду, виходячи з його можливостей.			
12.	Відшкодування збитків, яких зазнало АТ, здійснюється в необхідному для розвитку обсязі, за допомогою використання механізмів довготермінового кредитування.			

Дата експертної оцінки _____ 20 __ р. _____

Ефективність безпекової діяльності організації оцінюється через коефіцієнт ефективності реалізації кожного механізму за формулою, використовуючи умовні величини від 0 до 1.

$$K_{iv}(K_{pp}, K_l, K_v) = \left(\frac{\sum_{i=1}^{K_e} \sum_{j=1}^N E_{oij}}{K_e} \right) / N, \quad (1)$$

де K_{iv} – коефіцієнт ефективності реалізації інформаційно-виявляючих механізмів; K_{pp} – коефіцієнт ефективності реалізації попереджувально-профілактичних механізмів; K_l – коефіцієнт ефективності реалізації ліквідаційних механізмів; K_v – коефіцієнт ефективності реалізації відновлювальних механізмів; K_e – кількість експертів; N – кількість параметрів діагностики; E_{oij} – експертна оцінка і-тим експертом j-параметра діагностики; $\sum_{j=1}^N E_{oij}$ – сума балів, отриманих за результатами оцінювання усіх параметрів діагностики і-тим експертом ($i=K_e$); $\sum_{i=1}^{K_e} \sum_{j=1}^N E_{oij}$ –

сума балів, отриманих за результатами оцінювання усіх параметрів діагностики експертною групою.

Для оцінки ефективності реалізації кожного з наведених механізмів безпеки також потрібно використовувати характерні ознаки, а саме:

$K_{iv(pp, l, v)} = 0-0,20$ – механізми безпекової діяльності організації реалізуються на недостатньому рівні:

1) *інформаційно-виявляючі* (інформація про загрози не надається або надається не вчасно і недостатня за обсягом і за достовірністю; протиправні дії не документуються або документуються не якісно);

2) *попереджувально-профілактичні* (нормативно-правові документи з питань безпеки не розроблені і не запроваджені або розроблені та запроваджені на рівні, що дає змогу створити мінімальні умови для протидії тільки деяким загрозам);

3) *ліквідаційні* (загрози не ліквідуються або в незначній мірі мінімізується їх вплив).

4) *відновлювальні* (втрати дуже значні і поновити їх майже неможливо або складно).

$K_{iv(pp, l, v)} = 0,21-0,50$ – механізми безпекової діяльності організації реалізуються на критичному рівні:

1) *інформаційно-відновлювальні* (інформація про загрози в більшості випадках надається достовірна і в необхідному обсязі але часто невчасно; протиправні дії юридичних і фізичних осіб документуються в більшості випадків невчасно і неякісно);

2) *попереджувально-профілактичні* (більшість необхідних нормативно-правових документів з питань безпеки розроблені та запроваджені, або розроблено більшість, а запроваджено мінімум з необхідних, що дозволяє створити умови для протидії основним загрозам);

3) *ліквідаційні* (вплив загрози послаблюється);

4) *відновлювальні* (втрати від загрози є значними але ще є можливості їх поновлення).

$K_{iv}(pp, l, v) = 0,51-0,80$ – механізми без пекової діяльності організації реалізуються на достатньому рівні:

1) *інформаційно-виявляючі* (інформація про загрози надається достовірна і в необхідному обсязі чи в більшості достовірна і в необхідному обсязі але інколи не вчасно; протиправні дії юридичних і фізичних осіб документуються вчасно, але не завжди якісно);

2) *попереджувально-профілактичні* (основні нормативно-правові документи з питань безпеки розроблені і запроваджені, або розроблені всі необхідні, а запроваджені тільки основні з них, що дозволяє створити умови для протидії більшості загроз);

3) *ліквідаційні* (вплив загрози незначний);

4) *відновлювальні* (незначні втрати поновлюються).

$K_{iv}(pp, l, v) = 0,81-1$ – механізми безпекової діяльності організації реалізуються на оптимальному рівні:

1) *інформаційно-виявляючі* (інформація про загрози надається в повному обсязі достовірна та вчасно; протиправні дії юридичних і фізичних осіб документуються якісно і вчасно);

2) *попереджувально-профілактичні* (всі необхідні нормативно-правові документи з питань безпеки розроблені і запроваджені, що дає змогу протидіяти всім реальним та потенційним загрозам);

3) *ліквідаційні* (дія загрози припиняється повністю).

4) *відновлювальні* (втрат немає).

Оцінюючи ефективність безпекової діяльності організації, можна встановити сильні й слабкі її місця за конкретними напрямками діяльності та напрями удосконалення. Водночас потрібна і цілісна картина про рівень ефективності безпекової діяльності організації – кількісна і якісна. Кількісно коефіцієнт ефективності безпекової діяльності організації (K_{es}) визначається за середнім значенням показників наведених механізмів. Це пояснюється тим, що безпекові інформаційно-виявляючі, попереджувально-профілактичні, ліквідаційні та

відновлювальні механізми організації взаємопов'язані та становлять цілісний безпековий процес. Зміст цих зв'язків полягає у тому, що вузькі місця під час реалізації одних механізмів можна компенсувати кращим виконанням інших. Водночас слід брати до уваги те, що немає рівноцінної взаємної компенсації між цими механізмами. Так, інформаційно-виявляючі чи попереджувально-профілактичні механізми не можуть компенсувати неефективне виконання ліквідаційних чи відновлювальних механізмів, а радше навпаки. Тому розраховуючи коефіцієнт ефективності безпекової діяльності організації (K_{es}) необхідно брати до уваги цю обставину й надавати їй перевагу. Тобто, у випадку коли значення коефіцієнтів ефективності ліквідаційних (K_l) і відновлювальних (K_v) механізмів менше 0,21 K_{es} – коефіцієнт ефективності безпекової діяльності організації визначається саме за цими показниками, незважаючи на показники інших механізмів. Для цього використовується формула усереднення отриманих показників безпекової діяльності:

$$K_{es} = \sqrt[4]{\prod_{i=1}^4 K_i} = \sqrt[4]{K_{pp}} \times K_{iv} \times K_l \times K_v, \quad (2)$$

коефіцієнти K_l та K_v можна визначити таким чином:

$$K_l, K_v \begin{cases} 0, \text{ якщо } K_l \leq 0,2; K_v \leq 0,2 \\ K_l, K_v, \text{ якщо } K_l \geq 0,2; K_v \geq 0,2 \end{cases}$$

де K_{es} – коефіцієнт ефективності безпекової діяльності організації; K_{pp} – коефіцієнт ефективності профілактично-попереджувальних механізмів; K_{iv} – коефіцієнт ефективності інформаційно-виявляючих механізмів; K_l – коефіцієнт ефективності ліквідаційних механізмів; K_v – ефективності відновлювальних механізмів.

Зважаючи на зазначене ефективність безпекової діяльності організації можна розділити на чотири рівні:

- 1) недостатній рівень – 0–0,2;
- 2) критичний рівень – 0,21–0,5;

- 3) достатній рівень – 0,51–0,8;
- 4) оптимальний рівень – 0,81–1.

За результатами оцінювання потрібно зробити аналіз, зауважувати на недоліки. Особливо проаналізувати причини, коли ефективність безпекової діяльності буде оцінена як недостатня чи критична.

Методика діагностики та визначення рівня безпеки організації

Методику діагностики та визначення рівня безпеки організації запропоновано на прикладі акціонерних товариств (АТ).

Комплексними критеріями для діагностики стану безпеки АТ можуть бути:

- коефіцієнт збитку;
- коефіцієнт платоспроможності АТ;
- коефіцієнт встановлення протиправного контролю над АТ або його активами.

Показник коефіцієнта збитку комплексно характеризує стан безпеки. Його величина залежить від деструктивних граничних змін в АТ, які спричинені реалізацією тих чи інших загроз. Що більше їх реалізується, то більші загальні витрати АТ, які компенсуються доходами. Якщо доходи їх не покривають, то АТ за результатами діяльності матиме збиток. У цьому разі, з погляду безпеки, потрібно знати, до якої межі збиток ще залишає можливості для розвитку.

Граничним показником збитку може бути співвідношення власного капіталу до мінімального розміру статутного капіталу. Водночас згідно з ЗУ про «Акціонерні товариства» власний капітал не повинен бути меншим за мінімальний розмір статутного капіталу АТ. У разі, коли він менший, АТ зобов'язане упродовж десяти місяців усунути таку невідповідність або ухвалити рішення про самоліквідацію.

Отже, рівень безпеки соціальної системи АТ за критерієм завданих збитків визначається за формулою 1:

$$K_{zb} = \frac{B_k}{C_k}, \quad (1)$$

де B_k – власний капітал; C_k – статутний капітал; K_{zb} – коефіцієнт збитку.

Для оцінки стану безпеки за цим критерієм доцільно використовувати умовні величини – коефіцієнти від 0 до 1 та характерні ознаки, а саме:

$K_{zb} = 0-0,2$ – *збиток небезпечний* (в АТ практично немає можливості для його відшкодування шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців з моменту настання такої невідповідності);

$K_{zb} = 0,21-0,5$ – *збиток критичний* (якщо в АТ є можливість для його відшкодування шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців з моменту настання такої невідповідності);

$K_{zb} = 0,51-0,8$ – *збиток значний* (якщо в АТ є можливості для його відшкодування шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців із моменту настання такої невідповідності).

$K_{zb} = 0,81 - 1$ – *збиток незначний* (за умови, що АТ його відшкодує шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців із моменту настання такої невідповідності).

У разі, коли АТ не може відшкодувати збиток шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців із моменту настання такої невідповідності – оцінюється від 0 до 0,20, незважаючи на те, що K_{zb} може бути в межах від 0,21 до 0,99.

Коефіцієнти використовуються як нормативна величина, з якими порівнюються розрахунково фактичні.

Коефіцієнт платоспроможності для діагностики стану безпеки АТ є найінформативнішим і простим у застосуванні, що на практиці має велике значення. У процесі оцінювання загального стану безпеки підприємства визначальною є його фінансова сфера, оскільки інтегрує в собі результати діяльності всіх життєво важливих для підприємства сфер.

Тому індикатором, де відображаються результати діяльності АТ з усіх основних видових функцій і розвитку, і безпеки, є фінансовий критерій у вигляді показника обігових коштів, за яким можна визначити рівень платоспроможності та ознаки банкрутства.

Оцінюється стан безпеки за цим критерієм кількісно, використовуючи умовні величини, – коефіцієнти від 0 до 1 та характерні ознаки, а саме:

$K_{pl} = 0-0,2$ – АТ не вистачає власних коштів, у зв'язку з чим воно перебуває на стадії банкрутства;

$K_{pl} = 0,21-0,5$ – АТ нестачу власних обігових коштів компенсує короткостроковими кредитами;

$K_{pl} = 0,51-0,8$ – нестача обігових коштів компенсується АТ середньостроковими кредитами;

$K_{pl} = 0,81-1$ – нестача обігових коштів компенсується АТ довгостроковими кредитами;

K_{pl} – коефіцієнт платоспроможності.

Використання **коефіцієнта встановлення протиправного контролю над АТ або його активами** є обов'язковим під час оцінювання його стану безпеки. Він використовується комплексно з іншими. Виявити таку небезпеку можна шляхом проведення аналітично-пошукової та детективної діяльності. Виявлення перших ознак встановлення такого контролю необхідно кваліфікувати як початок реалізації реальних загроз, що обов'язково можуть спричинити небезпеку для АТ, наприклад, у формі рейдерського захоплення. Для цього потрібно володіти такою інформацією:

1) яка кількість дрібних власників акцій і чи розглядають вони акції як фінансові інвестиції, від яких регулярно отримують прибуток?

2) чи є можливість рейдерам оминати норми законодавства і які саме, що можуть бути використані для захоплення АТ?

3) чи є правопорушення в АТ, що можуть бути підтверджені документально, через які підприємство стає уразливим перед рейдерами?

4) чи є недооціненість акцій АТ, що може спровокувати масову їх купівлю, оскільки це є дуже вигідним у майбутньому, зокрема й для рейдерів?

5) чи є скупівля акцій, що перебувають у власності міноритарних акціонерів?

6) чи є спроби або факт скликання загальних зборів акціонерів з метою ухвалення рішень, спрямованих на зміну власників АТ?

7) чи є спроби або факти тиску з боку органів державної влади на керівництво АТ з метою сприяння рейдерським атакам?

8) чи є спроби або факт суперечливих судових рішень на користь агресорів?

9) чи є спроби або факт залучення силових структур і використання силових методів під час вирішення конфліктних ситуацій?

Оцінити рівень безпеки АТ за критерієм протиправного контролю над ним можна кількісно, використовуючи наведений перелік питань, коефіцієнти від 0 до 1 та відповідні ознаки, а саме:

$K_{pk} = 0-0,2$ – є реальний над АТ чи його активами контроль всупереч його волі та протиправними методами;

$K_{pk} = 0,21-0,5$ – існують реальні спроби встановлення над АТ чи його активами контроль всупереч його волі та протиправними методами;

$K_{pk} = 0,51-0,8$ – відсутність будь-яких реальних спроб встановити над АТ чи його активами контроль всупереч його волі та протиправними методами;

$K_{pk} = 0,81-1$ – відсутність реальних чи потенційних намірів встановити над АТ чи його активами контроль всупереч його волі та протиправними методами;

Оцінюючи стан безпеки АТ, потрібно зауважити на принципове положення: безпека є тоді, коли загальний показник (коефіцієнт) стану безпеки та окремі його індикатори (*збиток та коефіцієнт встановлення протиправного контролю над АТ або його активами*) будуть не нижче граничного, тобто самодостатність та стійкість соціальної системи є такими, за яких зберігаються умови і можливості для розвитку.

Зважаючи на це положення, загальний стан (рівень) безпеки акціонерного підприємства необхідно визначати через коефіцієнт (K_{sb}) за такою формулою 2:

$$K_{sb} = \alpha_1 K_{ib} + \alpha_2 K_{zp} + \alpha_3 K_{zb} + \alpha_4 K_{pl} + \alpha_5 K_{pk}, \quad (2)$$

де K_{sb} – стан безпеки АТ; K_{zb} – коефіцієнт збитку; K_{pl} – коефіцієнт платоспроможності; K_{pk} – коефіцієнт встановлення протиправного контролю над АТ.

Вагові множники вибираються на підставі вагомості впливу кожної складової безпеки на загальний її стан. Перевага надається таким її складовим, як збиток (K_{zb}) та встановлення протиправного контролю над АТ або його активами (K_{pk})

Якщо $K_{zb} \leq 0,2$ і $K_{pk} \leq K_{pk}$, то вектор вагових множників $\alpha(\alpha_1; \alpha_2; \alpha_3; \alpha_4; \alpha_5)$ набуває виду, відповідно (0; 0; 1; 0; 0), тобто рівень коефіцієнта K_{zb} визначає рівень K_{sb} .

Якщо $K_{pk} \leq 0,2$ і $K_{pk} \leq K_{zb}$, то маємо ситуацію аналогічну до попередньої з таким вектором вагових множників (0; 0; 0; 0; 1), тобто рівень коефіцієнта K_{pk} визначає рівень K_{sb} .

У разі, коли $K_{zb} > 0,2$ і $K_{pk} > 0,2$, пропонується такий алгоритм вибору вагових множників:

1) ваговим множникам надаються такі значення у порядку їх зростання 0,10; 0,15; 0,20; 0,25; 0,30.

2) у разі конкретного набору коефіцієнтів K_i вагові множники вибираються так: для $K_{\min}$ вибирається $\alpha_{\max}$, для наступного (більшого за величиною) значення K наступне (менше за величиною) α тощо, і насамкінець для $K_{\max}$ вибирається множник $\alpha_{\min}$.

Наприклад: для набору $K_{ib} = 0,2$; $K_{zp} = 0,4$; $K_{zb} = 0,6$; $K_{pl} = 0,5$; $K_{pk} = 0,3$ вагові множники будуть такими: $\alpha_1 = 0,30$; $\alpha_2 = 0,20$; $\alpha_3 = 0,10$; $\alpha_4 = 0,15$; $\alpha_5 = 0,25$.

Стан економічної безпеки АТ можна розділити на чотири рівні:

1. Недостатній рівень – 0–0,2;
2. Критичний рівень – 0,21–0,5;
3. Достатній рівень – 0,51–0,8;
4. Оптимальний рівень – 0,81–1.

На практиці ймовірність того, що показники безпеки будуть або дуже низькими або достатньо високими, є незначною.

В основному вони мають середні значення. Тому для оцінки важливо, щоб відрізки у вигляді граничних показників небезпеки (недостатній рівень) та оптимального рівня безпеки були найменшими, а показники безпеки критичного та достатнього рівня мали пріоритет. Крім того, необхідно врахувати чутливість розподілу та його математичну зручність. Для цього використано квазісиметричний (наближено-симетричний) розподіл балів та формулу 3.

$$X_n = 0,25n + 0,05k, \quad (3)$$

де, n – граничні межі рівнів безпеки,

$$k = \begin{cases} 0; \text{ якщо } n = 0, 2, 4 \\ -1; \text{ якщо } n = 1 \\ 1; \text{ якщо } n = 3 \end{cases}$$

Зона небезпеки починається за умови, якщо рівень безпеки перебуває в межах 0–0,2 (недостатній рівень). Пояснюється це тим, що небезпека для організації виникає за умови, коли його безпековий потенціал наближається до 0. *Небезпека може виявлятися у таких комбінаціях:*

1) існує реальний над АТ чи його активами контроль всупереч його волі та протиправними методами; АТ не вистачає власних коштів, у зв'язку з чим воно перебуває на стадії банкрутства; АТ має надмірні збитки, які практично немає можливості відшкодувати шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців з моменту настання такої невідповідності;

2) існує реальний над АТ чи його активами контроль всупереч його волі та протиправними методами; АТ не вистачає власних коштів, у зв'язку з чим воно перебуває на стадії банкрутства;

3) існує реальний над АТ чи його активами контроль всупереч його волі та протиправними методами;

4) АТ має надмірні збитки, які практично немає можливості відшкодувати шляхом збільшення власного капіталу до

рівня не нижче статутного впродовж десяти місяців з моменту настання такої невідповідності.

Зона безпеки, навпаки, є тоді, коли показники безпекового потенціалу АТ близькі до 1. Вона розпочинається з 0,21 до 1 з розподілом на рівні безпеки: 0,21–0,5 (критичний рівень); 0,51–0,8 (достатній рівень); 0,81–1 (оптимальний рівень).

Для зони безпеки АТ характерними ознаками є:

1) відсутність реальних чи потенційних намірів та реальних спроб встановити над АТ чи його активами контроль всупереч його волі та протиправними методами, а якщо й існують то ліквідуються;

2) нестачу власних обігових коштів АТ компенсує короткостроковими середньостроковими та довгостроковими кредитами;

3) АТ має збитки аж до критичного стану, але ще має можливості відшкодовувати їх шляхом збільшення власного капіталу до рівня не нижче статутного впродовж десяти місяців із моменту настання такої невідповідності.

Інформація про стан безпеки організації, з одного боку, в практичній управлінській діяльності спонукає власників і топ-менеджерів оперативніше ухвалювати більш виважені й ефективніші рішення, а з іншого, – виконує роль своєрідного інвестиційного індикатора.

СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ БЕЗПЕКОЗНАВСТВА

Адміністративно-організаційні методи – група методів, які використовуються для впорядкування безпекової діяльності у логічно структуровану та створення відповідного організаційного механізму забезпечення безпеки соціальної системи.

Безпека соціальної системи – це стан системи в межах граничних значень і здатність протидіяти загрозам чи небезпеці з метою захисту інтересів, збереження цілісності системи та сприяння її розвитку.

Безпекова діяльність – форма активного ставлення суб'єктів безпеки до безпекової дійсності, зміст якого полягає у проведенні в ній відповідних змін і перетворень на основі засвоєння та розвитку безпекової культури. Тобто це діяльність, спрямована на протидію загрозам з метою захисту корпоративних інтересів, збереження цілісності процесів чи системи та сприяння її розвитку на основі засвоєння та розвитку безпекової культури.

Безпекова корпоративна культура – це складова корпоративної культури, яка виявляється у формі безпекового мислення як цінності та безпекової поведінки як норми у відносинах для збереження цілісності організації.

Безпекова поведінка як норма у відносинах – це відносини, що сформувалися та підтримуються у середині організації та відносини організації до зовнішнього середовища у яких немає ознак діяльності, спрямованої на збурення, нанесення її матеріальних чи моральних збитків, порушення цілісності.

Безпекова філософія управління організацією – це спосіб мислення та безпекова поведінка у відносинах, які необхідні для збереження цілісності організації.

Безпекове мислення як корпоративна цінність – це спосіб мислення працівників, менеджерів та власника (засновника) організації, який сприймається у колективі та не спонукає до збурення, нанесення її матеріальних чи моральних збитків, а навпаки до створення сприятливих умов для розвитку.

Безпекові парадигми – усталені підходи до розуміння та вирішення теоретичних і практичних питань, пов'язаних із забезпеченням економічної безпеки підприємства.

Видові функції (види) безпекової діяльності – це будь-які види діяльності, які містять інформаційні, попереджувальні, ліквідаційні та відновлювальні механізми, завдяки яким здійснюється безпекова діяльність (функція безпеки соціальної системи).

Виклик – це нова ситуація у зовнішньому середовищі, яка висуває нові вимоги до ухвалення рішень власниками і менеджментом організації, спрямованих на подальший розвиток.

Відновлювальні механізми безпекової діяльності – це сукупність видів безпекової діяльності та відповідних методів й засобів з відновлення якісних чи кількісних показників, зв'язків, цілісності об'єкта, діяльності соціальної системи, а також компенсації, відшкодування за отриманні збитки.

Відносини координації – це відносини, що виникають між органами, структурними підрозділами, керівниками і підлеглими одного рівня при спільній участі у вирішенні завдання з питань безпеки.

Відносини субординації – це службове підпорядкування молодшого за посадою старшому, виконання правил службової дисципліни.

Групові інтереси – це узгодженні приватні інтереси, реалізація яких необхідна для створення умов і механізмів для функціонування групи чи загалом колективу (організації).

Діагностика загроз – це вивчення негативного впливу дестабілізуючих чинників в умовах неповної інформації на предмет можливого завдання збитків, погіршення стану процесів, об'єктів чи системи, порушення їх цілісності і на цій основі виявлення потенційних чи реальних загроз.

Діагностика стану безпеки організації – це вивчення наслідків впливу загроз на діяльність організації та об'єкти безпеки в умовах неповної інформації на предмет встановлення рівня її безпеки.

Діяльність – форма активного ставлення до довкілля, а її зміст становить доцільність зміни і перетворення цього світу на основі засвоєння та розвитку культури.

Домінуючий безпековий світогляд – це сукупність уявлень про життєдіяльність людей в умовах дії різних загроз та небезпек.

Він впливає на формування типу домінуючого безпекового та наукового мислення.

Економічний злочин – це умисна суспільно небезпечна діяльність або бездіяльність, яка призводить до істотних втрат суб'єкта господарювання і фізичних осіб, і стає на перешкоді реалізації економічних інтересів, зумовлюючи цим погіршення їх соціально-економічного стану.

Економічні засоби – економічні відносини з державними структурами, юридичними і фізичними особами з метою забезпечення конкурентоспроможності, а також фінансово-матеріальні ресурси – гроші, цінні подарунки та ін., які використовуються здебільшого при отриманні інформації через агентурні джерела та зв'язки в органах влади, контрольних органах у цілях детективної діяльності та забезпечення безпеки.

Економічні методи – це методи, які дають змогу оцінювати економічний стан соціальної системи з погляду безпеки, ідентифікувати загрози економічно характеру, а також припиняти дію загроз чи небезпек, та ліквідовувати їх наслідки й відновлювати втрати.

Емпіричне пізнання – це пізнання, яке досягається здебільшого за допомогою органів чуття.

Завдання – це види робіт, які необхідно виконати певним способом та в обумовлений термін.

Загроза – це дія дестабілізуючих природних і (або) суб'єктивних чинників, що спричиняють потенційні або реальні збитки.

Засоби забезпечення безпеки – це можливості, інструменти матеріального і нематеріального характеру, за допомогою яких здійснюється безпекова діяльність.

Індикатор безпеки – це показник з граничним значенням, котрий показує на якому полі безпеки чи небезпеки перебуває соціальна система.

Інформаційні засоби – це інформаційні й аналітичні матеріали, наукові розробки, публікації, комп'ютерні технології, журнали тощо з питань безпеки, а також комунікаційний зв'язок підприємства з громадськістю, владою, засобами масової інформації, працівниками і акціонерами.

Інформаційно-аналітичні методи – це група методів, що передбачають механізми збору, обробки й аналізу інформації та

дають змогу кваліфікувати дестабілізуючі фактори у загрози чи небезпеки, а також визначати рівень безпеки організації.

Інформаційно-виявляючі механізми безпекової діяльності – це сукупність відповідних видів діяльності, методів та засобів, пов'язаних зі збором і аналізом інформації про загрози та документуванням протиправних дій у відповідному часі та просторі.

Керована підсистема – елементи підсистеми, які забезпечують безпосередній процес виробничої (виробництво товарів, надання послуг тощо), господарської, фінансової, комерційної, безпекової та інших видів діяльності.

Керуюча підсистема – складові підсистеми, що забезпечують процес управління.

Контроль – це процес відстеження і вибір напрямів для здійснення необхідних коректив у діяльності організації з метою досягнення очікуваних безпечових результатів.

Корінні функції – це взаємопов'язані функції процесу життєдіяльності соціальної системи, які безпосередньо визначають у цьому процесі якісні і кількісні перетворення, його стабільність та довговічність.

Корпоративна культура – це система цінностей, які сформовані та підтримуються членами колективу, виявляються у формі певного способу мислення та правил і норм поведінки, що дозволяє зберігати цілісність організації.

Корпоративні інтереси – це сукупність об'єктивних потреб соціальної системи, які виявляються як узгоджені інтереси відповідних суб'єктів учасників корпоративних відносин, реалізація яких необхідна для її життєдіяльності.

Корпоративні інтереси з безпеки – це узгоджені інтереси внутрішніх і зовнішніх суб'єктів соціально-економічних та безпечових відносин, реалізація яких необхідна для створення відповідних умов і механізмів для протидії внутрішнім й зовнішнім загрозам і сприяння в такий спосіб реалізації інтересів розвитку та збереження цілісності організації.

Корпоративні інтереси з розвитку – це узгоджені інтереси внутрішніх і зовнішніх суб'єктів соціально-економічних відносин, реалізація яких необхідна для створення відповідних умов і механізмів, спрямованих на здійснення цілеспрямованих якісних і кількісних перетворень в організації.

Критерій оцінювання безпеки – це ознака, за якою визначається стан безпеки соціальної системи.

Ліквідаційні механізми безпекової діяльності – це сукупність видів безпекової діяльності та відповідних методів й засобів, пов'язаних з ліквідацією (припиненням) загроз на будь-якій стадії реалізації конфіденційними методами та методами роботи у надзвичайних ситуаціях.

Логічна організація діяльності – це цілеспрямована активність людини з метою упорядкування її в цілісну систему з чітко визначеними характеристиками (логічно структуровану).

Методи – (від грецьк. *methodos* – шлях дослідження, теорія, вчення), впорядковані способи пізнання й формування знання про безпекову реальність та забезпечення безпеки суб'єкта господарювання.

Методи безпекової діяльності – це способи, за допомогою яких реалізуються засоби безпеки у межах виконання відповідних видових функцій безпеки.

Методика забезпечення безпеки – сукупність конкретизованих, формалізованих, адаптованих до предмета і завдань забезпечення безпеки підприємства процедур, засобів, техніки і прийомів збирання, обробки й узагальнення інформації та протидії загрозам.

Методологічний підхід – об'єднані домінуючим методом взаємозалежні методи, теорії та інші наукові знання про безпекову дійсність та її забезпечення.

Методологія безпеки організації – це вчення (сукупність теоретичних положень) про логічну структуру та організацію безпекової діяльності у вигляді системи.

Моделювання – це відображення будь-яким способом процесів, які відбуваються в реальному об'єкті або зразок, макет конструкції чого-небудь, відтворений у зменшеному або збільшеному вигляді.

Мотивування – вид управлінської діяльності, що забезпечує процес спонукування до діяльності для досягнення особистих цілей і цілей організації.

Небезпека – це деструктивні граничні зміни, спричинені реалізацією загрози в соціальній системі, що викликають її кризовий стан.

Недобросовісна конкуренція: а) будь-який акт конкуренції, що є не сумісним із чесними звичками в промислових і торгових домах (*Паризька конвенція з охорони промислової власності, 1988 р.*); б) будь-які дії у конкуренції, які не відповідають правилам, торговим або іншим чесним звичкам у підприємницькій діяльності (*Закон України «Про захист від недобросовісної конкуренції», 1997 р.*).

Об'єкт безпеки – це все те, на що спрямована діяльність суб'єктів і сил безпеки з метою захисту їх від загроз.

Організаційно-управлінські засоби – це структури, процедури, режими, що обмежують або виключають можливість завдання економічних збитків акціонерному товариству.

Організація діяльності – це впорядковувати її у цілісну систему з чітко визначеними характеристиками, логічною структурою та процесом її здійснення.

Організування – це процес формування структури управління, встановлення зв'язків та відносин, що дає змогу ефективно працювати для досягнення цілей.

Пізнання – це процес активного, цілеспрямованого, категоріального відображення дійсності свідомістю людини, що виявляється у вигляді емпіричного й теоретичного пізнання, які взаємопов'язані.

Планування – це відособлений вид управлінської діяльності, який визначає перспективу розвитку і майбутнього стану системи безпеки організації, а також створює умови для спрямування зусиль всіх її суб'єктів та сил безпеки на досягнення місії та загальних цілей.

Пов'язані інтереси – це інтереси суб'єктів, що мають з організацією відповідні соціально-економічні відносини, необхідні для забезпечення її життєдіяльності та офіційного функціонування.

Повноваження – це обмежене право розпоряджатися людьми і ресурсами організації або структурного підрозділу для вирішення завдань.

Попереджувально-профілактичні механізми безпекової діяльності – це сукупність відповідних видів діяльності, методів та засобів, пов'язаних з розробкою та дотриманням законів, підзаконних актів з питань безпеки, а також нормативів безпеки та

інших управлінських рішень, від режиму і до регламентації і мотивації поведінки працівників підприємства.

Правові засоби – це засоби, які містять правові механізми безпекової діяльності у вигляді законів та нормативно-правових документів.

Правові методи – це способи юридичного й судового захисту корпоративних інтересів соціальної системи та формування нормативно-правових документів, які регламентують її внутрішню діяльність, зокрема з питань безпеки.

Приватні (особисті) інтереси – це усвідомлені потреби людини, задоволення яких необхідне для її життєдіяльності.

Принципи забезпечення безпеки – це основні орієнтири, яких повинні дотримуватися суб'єкти безпеки організації у безпечовій діяльності.

Продуктивна діяльність – це діяльність, що спрямована на отримання нового результату чи нових знань і потребує відповідного впорядкування, логічної її організації тощо, тобто виникає необхідність у застосуванні методології.

Репродуктивна діяльність – це діяльність, що заснована на попередньому досвіді на рівні раз і назавжди засвоєних технологій.

Самодостатність соціальної системи – це наявність у розпорядженні суб'єктів управління відповідних ресурсів та уникнення залежності від джерел їх походження, що може становити загрозу, а також їх використання на рівні, необхідному для збереження параметрів життєдіяльності системи.

Сили безпеки – це фізичні особи, які безпосередньо виконують заходи безпеки.

Система безпеки організації – це сукупність взаємопов'язаних елементів, що має властивості, відмінні від властивостей структурного елемента, необхідних для протидії загрозам з метою захисту корпоративних інтересів і загалом створення безпечних умов для розвитку та забезпечення цілісності процесів, об'єктів та підприємства.

Соціальна система – це сукупність взаємодіючих елементів, що становлять цілісне утворення, яке має властивості, відмінні від властивостей елементів та забезпечує її життєдіяльність.

Соціально-психологічні методи – способи психологічного впливу на потенційні чи конкретні особи (джерела) з метою отри-

мання інформації про можливі загрози, їх попередження чи припинення.

Стійкість соціальної системи – це наявність необхідних умов, елементів та системних зв'язків між ними на рівні, достатньому для стримування дії дестабілізуючих чинників.

Структура – це взаємовідносини рівнів управління і видів робіт (функціональних обов'язків), які виконують підрозділи організації або окремі працівники.

Суб'єкт безпекової діяльності – це фізична (посадова) або юридична особа, яка бере участь в управлінні, або лише в організації безпекової діяльності соціальної системи.

Теоретичне пізнання – це вище відображення дійсності за допомогою абстрактного мислення й дослідження, у процесі якого виділяються істотні властивості або сторони об'єкта, виявляються об'єктивні закономірності, зв'язки та тенденції його розвитку, недоступні для чуттєвого пізнання.

Технічні засоби – це засоби які мають технічні можливості чи властивості для протидії загрозам.

Технічні методи – це способи технічного захисту засобів обчислення інформації, телекомунікаційних мереж та технологій виробництва. Наприклад, відеоспостереження, підслуховування за допомогою так званих «жучків», криптологічний захист інформації тощо.

Технологічні засоби – це засоби, що забезпечують унікальність продукту або послуги, унеможливають його копіювання чи підробку.

Технологія – це поєднання відповідних знань, кваліфікаційних навиків, обладнання, інструменту та інфраструктури, необхідних для здійснення бажаних перетворень у матеріалах, інформації, людях.

Тип безпекового мислення – сукупність взаємозалежних і взаємообумовлених ідей, принципів, норм, форм пізнання й відображення безпекової дійсності.

Тіньова економіка – це протиправна економічна діяльність, а також та, що не враховується офіційною статистикою і не потрапляє до ВВП.

Управління організацією – це цілеспрямований вплив на об'єкт управління та створення у ньому внутрішніх і зовнішніх

умов, необхідних для збереження цілісності соціальної системи, її безпеки, розвитку та реалізації корпоративних інтересів.

Управлінська технологія – поєднання менеджерських знань, вмінь, використання інформаційної техніки та процесу управління, що необхідні для здійснення бажаних перетворень в інформації і людях.

Управлінські відносини – це зв'язок людей за їх правами, обов'язками та підпорядкуванням один одному в спільній трудовій діяльності. Розрізняють: відносини субординації та відносини координації.

Фізичні засоби – це використання фізичної охорони об'єктів, а також застосування фізичної сили під час затримання правопорушників.

Функція безпеки – це конкретні дії, які необхідно виконати, щоб захистити функцію розвитку соціальної системи від потенційних чи реальних внутрішніх і зовнішніх загроз, створити в такий спосіб необхідні умови для її реалізації.

Функція розвитку – це конкретні дії, пов'язані з реалізацією інтересів і спрямовані на незворотні та закономірні зміни конкретних матеріальних об'єктів, що ведуть до виникнення їх якісно нових станів або принципово нових об'єктів як цілісних систем, або ж до забезпечення їх стабільного достатньо кількісного чи якісного станів.

Функція управління – це конкретні дії, які необхідно виконати, щоб інтегрувати в єдиний процес функції розвитку, безпеки і забезпечуючи на цій основі життєдіяльність організації.

Цілі – це конкретний очікуваний результат або кінцевий стан організації.

Ціль (мета) системи безпеки – це виключення або зведення до мінімуму можливих втрат (збитків) та сприяння у реалізації корпоративних інтересів і загалом функції розвитку, а також забезпечення цілісності соціальної системи шляхом протидії загрозам.

СПИСОК ЛІТЕРАТУРИ

1. Алексеев Н. Г. Личностно ориентированное обучение: вопросы теории и практики / Н. Г. Алексеев. – Тюмень: ТГУ, 1997. – С. 171.
2. Баринов В. А. Корпоративная культура организации в России / В. А. Баринов, Л. В. Макаров // Менеджмент в России и за рубежом. – 2000. – № 2. – С. 110–121.
3. Большой энциклопедический словарь: в 2 т. / гл. ред. А. М. Прохоров. – М.: Сов. энциклопедия, 1991. – Т. 1. – 863 с.
4. Борисов Н. И. Конкурентная разведка как инструмент конкурентной борьбы / Н. И. Борисов [Электронный ресурс]. – Режим доступа: http://www.marketing.spb.ru/lib-research/competition_spy.htm.
5. Будович Л. С. Управление предприятием на основе совершенствования системы экономической безопасности: дисс. ... канд. эконом. наук: спец. 08.00.05 / Лидия Сергеевна Будович. – М., 2007. – 212 с.
6. Вареник Н. П. Охорона: між безробіттям і злочинністю. Гральні заклади – найбільший сегмент, втрачений охоронним бізнесом / Н. П. Вареник // Дзеркало тижня. – 27 червня – 3 липня 2009 р. – № 24 (752).
7. Ведомственная охрана предприятий тормозит развитие рынка частных охранных услуг, считают специалисты [Электронный ресурс]. – Режим доступа: <http://president.org.ua/news/news-128881>.
8. Вінник О. М. Проблеми правового забезпечення приватних і публічних інтересів в акціонерних товариствах / О. М. Вінник // Проблеми вдосконалення господарського законодавства України: тези виступів учасників круглого столу (м. Київ, 17–18 квітня 2001 р.). – К., 2001. – С. 45–48.
9. Власюк О. С. Теорія і практика економічної безпеки в системі науки про економіки / О. С. Власюк; Нац. Ін-т проблеми міжнар. безпеки при Раді нац. безпеки і оборони України. – К., 2008. – 48 с.
10. Гладченко Т. М. Науково-методичні основи створення механізму державного управління і регулювання системи безпеки підприємницької діяльності: регіональний аспект: автореф. дис. на здобуття наук. ступ. канд. наук з держ. упр.: спец. 25.00.02. «Механізми державного управління» / Т. М. Гладченко. – Донецьк, 2004. – С. 9.
11. Государственное регулирование экономики: конспект лекций для студентов специальностей 6.050.100 «Учет и аудит» и

«Экономика предприятия» факультета последипломного образования и заочного обучения / сост. Т. А. Пушкарь. – Х.: ХНАГХ, 2006. – 62 с.

12. Даль В. И. Толковый словарь живого великорусского языка / В. И. Даль. – М.: ТЕРРА, 2000. – Т. 1. – С. 167.

13. Денис О. Б. Соціально-економічні механізми управління акціонерним капіталом: дис. ... канд. екон. наук: спец. 08.06.01 / О. Б. Денис; НАН України; Інститут регіональних досліджень. – Львів, 2004. – 245 с.

14. Державна служба охорони [Електронний ресурс]. – Режим доступу: http://www.dso.com.ua/index.php?lang_id=1&menu_id=2.

15. Доронин А. И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия / А. И. Доронин. – Тула: Гриф и К°, 2000. – 116 с.

16. Економічна безпека: навч. посібник / за ред. З. С. Варналія. – К.: Знання, 2009. – 647 с.

17. Задихайло Д. В. Корпоративне управління: навчальний посібник / Д. В. Задихайло, О. Р. Кібенко, Г. В. Назарова. – Х.: Еспада, 2003. – 688 с.

18. Защита становится навязчивой. Столичный рынок охранных услуг пожинает плоды перенасыщения [Электронный ресурс]. – Режим доступа: <http://www.dsnews.ua/companies-markets/29762.html>.

19. Каган М. С. Человеческая деятельность / М. С. Каган. – М.: Политиздат, 1974. – С. 189.

20. Каленяк В. Приватна охоронна структура як соціальна необхідність держави / В. Каленяк // Персонал. – 2007. – № 1 [Електронний ресурс]. – Режим доступу: <http://www.personal.in.ua/article.php?ida=431>.

21. Кельман М. С. Юридична наука: проблеми методології / М. С. Кельман. – Тернопіль: Тернограф, 2011. – 492 с.

22. Кибенко Е. Р. Корпоративное право Украины: учеб. пособие / Е. Р. Кибенко. – Х.: Эспада, 2001. – 288 с.

23. Кобелев Н. Б. Практика применения экономико-математических методов и моделей / Н. Б. Кобелев. – М.: Финстатинформ, 2000. – 211 с.

24. Копейкин Г. К. Экономическая безопасность предприятия: обучение персонала / Г. К. Копейкин, Н. А. Лапина // Защита информации. Конфиден. – 2004. – № 3. – С. 44–49.

25. Копнин П. В. Наука как прикладная логика / П. В. Копнин // Логика научного исследования. – М.: Наука, 1965. – 450 с.

26. Крутов В. В. Становлення та розвиток недержавної системи безпеки підприємництва / В. В. Крутов. – К.: Фенікс, 2008. – 406 с.

27. Кузьмін О. Є. Теоретичні та прикладні засади менеджменту: навч. посібник / О. Є. Кузьмін, О. Г. Мельник. – Львів: Національний університет «Львівська політехніка»; «Інтелект-Захід», 2003. – 352 с.

28. Кустовська О. В. Методологія системного підходу та наукових досліджень / О. В. Кустовська. – Тернопіль: Економічна думка, 2005. – 123 с.

29. Логинов Е. А. Актуальные проблемы экономико-правового обеспечения экономической безопасности / Е. А. Логинов, В. К. Лукин, Ю. С. Чечулина. – Краснодар: Краснодарский юридический институт МВД России, 2000. – 129 с.

30. Методика розрахунку рівня економічної безпеки України, затв. наказом Мінекономіки України від 02.03.2007 р. – № 60. – 23 с.

31. Методология: вчера, сегодня, завтра: в 3-х т. / ред.-сост. Г. Г. Хромченко, М. С. Крылов. – М.: Изд-во Школы Культурной Политики, 2005. – С. 323.

32. Минаев Г. А. Безопасность – менеджмент организации / Г. А. Минаев // Best of security. – 2008. – №4 (26). – С. 25.

33. Минаев Г. А. Безопасность организации: учебник / Г. А. Минаев. – К.: КНТ, 2009. – 440 с.

34. Молчановский В. Ф. Безопасность – атрибут социальной системы / В. Ф. Молчановский // Социально-политические аспекты обеспечения государственной безопасности в современных условиях: сб. статей. – М.: Граница, 1994. – С. 104.

35. Низенко Э. И. Обеспечение безопасности предпринимательской деятельности / Э. И. Низенко. – К.: МАУП, 2003. – 123 с.

36. Новиков А. М. О предмете и структуре методологии / А. М. Новиков, Д. А. Новиков // Мир образования – образование в Мире. – 2008. – № 1. – С. 32–40.

37. Ожегов С. И. Словарь русского языка / С. И. Ожегов. – М., 1989. – С. 253.

38. Основы философии науки: учеб. пособие для аспирантов / В. П. Кохановский и др. – Изд. 2-е. – Ростов н/Д: Феникс, 2005. – С. 185.

39. Позднишев Є. В. Інформаційно-аналітичне забезпечення безпеки підприємництва (методи та їх застосування): навч. посібник / Є. В. Позднишев. – Кн. 1. – К.: Видавець Позднишев, 2007. – 76 с.

40. Реверчук Н. Й. Економічна безпека в Україні: держави, фірми, особи: навч. посібник / Н. Й. Реверчук, Я. Й. Малик, І. І. Кульчицький, С. К. Реверчук; за ред. С. К. Реверчука. – Львів: ЛФМАУП, 2000. – 192 с.

41. Рыбалкин Н. Н. Философия безопасности: учеб. пособие / Н. Н. Рыбалкин. – М.: Московский психолого-социальный институт, 2006. – 296 с.

42. Сенчагов В. К. Экономическая безопасность России. Общий курс / под ред. В. К. Сенчагова. – М.: Дело, 2005. – 896 с.
43. Серебрянников В. В. Гражданское общество и проблемы безопасности России (материалы «круглого стола») / В. В. Серебрянников, Ю. И. Дерюгин, Н. Н. Ефимов, В. И. Ковалев // Вопросы философии. – 1995. – № 2. – С. 26.
44. Система економічної безпеки: держава, регіон, підприємство: монографія: у 3 т. / О. М. Ляшенко, Ю. С. Погорелов, В. Л. Безбожний та ін.; за заг. ред. Г. В. Козаченко. – Луганськ: Елтон, 2010. – Т. 1 – 282 с.
45. Словник термінів та визначень недержавної системи безпеки України / В. В. Крутов, П. Я. Пригунов, М. О. Будаков та ін. – К.: УСПП, 2008. – С. 37–38.
46. Соснин А. С. Менеджмент безопасности предпринимательства: учеб. пособие / А. С. Соснин, П. Я. Пригунов. – К.: Изд-во Европейского университета, 2004. – 555 с.
47. Спивак В. А. Корпоративная культура / В. А. Спивак. – СПб.: Питер, 2001. – 352 с.
48. Сучасний тлумачний словник української мови: 100 000 слів / за заг. ред. проф. В. В. Дубічинського. – Х.: ВД ШКОЛА, 2008. – С. 254.
49. Философский энциклопедический словарь. – М.: Сов. Энциклопедия, 1983. – С. 250.
50. Франчук В. І. Основи менеджменту: навч. посібник / В. І. Франчук. – Львів: Каменяр, 1997. – 95 с.
51. Франчук В. І. Особливості організації системи економічної безпеки акціонерних товариств в умовах трансформаційної економіки: монографія / В. І. Франчук. – Львів: Львівський державний університет внутрішніх справ, 2010. – 440 с.
52. Хміль Ф. Формування культур вітчизняних організацій в умовах стабілізації ринкових відносин / Ф. Хміль // Вісник Тернопільської академії народного господарства. – Вип. 7/1. – 2002. – С. 11–12.
53. Шлемко В. Т. Економічна безпека України, сутність і напрямки забезпечення / В. Т. Шлемко, І. Ф. Бінько. – К.: НІСД, 1997. – 144 с.
54. Щедровицкий Г. П. К анализу утопии организационно-деятельностных игр / Г. П. Щедровицкий. – Препринт. – Пушкино: ЦНБИ ИНГ АН, 1987. – С. 42.
55. Экономическая и национальная безопасность: учебник / под. ред. Л. П. Гончаренко. – М.: Экономика, 2007. – 543 с.
56. Ярочкин В. И. Корпоративная разведка / В. И. Ярочкин, Я. В. Бузанова. – 2-е изд., перераб. и доп. – М.: Ось-89, 2005. – 304 с.

НАВЧАЛЬНЕ ВИДАННЯ

Франчук Василь Іванович
доктор економічних наук

ТЕОРІЯ БЕЗПЕКИ СОЦІАЛЬНИХ СИСТЕМ

Підручник

Підписано до друку 08.10.2020.
Формат 60x84/16. Ум-друк. арк. 13,02.
Наклад 500 прим. Зам. № 2010-06.

Видано і віддруковано в ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
Тел. +38 050 7775901 +38 048 7959160
e-mail: fenix-izd@ukr.net
www.feniksbooks.com