ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

ФАКУЛЬТЕТ ПРАВА, ПУБЛІЧНОГО УПРАВЛІННЯ І МЕНЕДЖМЕНТУ
КАФЕДРА ФУНДАМЕНТАЛЬНИХ І ПРИВАТНО-ПРАВОВИХ ДИСЦИПЛІН

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ФОРМУВАННЯ ТА УПРАВЛІННЯ СТРАТЕГІЄЮ БЕЗПЕКИ ОРГАНІЗАЦІЇ»

Студента 2 курсу ММЮД групи
Освітньої програми Менеджмент в юридичній діяльності
Спеціальності 073 Менеджмент
Галузі знань 07 Управління та адміністрування
Ступеня вищої освіти магістр
Швеця Федора Васильовича

Науковий керівник: к.ю.н., доц. Кронівець Т.М.

Національна шкала _____

Кількість балів: _____ Оцінка: ECTS _____

Голова комісії _____ _____

(підпис) (ініціали та прізвище)

Члени комісії _____ _____

(підпис) (ініціали та прізвище)

_____ _____

(підпис) (ініціали та прізвище)

_____ _____

(підпис) (ініціали та прізвище)

Вінниця 2024

АНОТАЦІЯ

Швець Ф.В. «Формування та управління стратегією безпеки організації», спеціальність 073 Менеджмент, Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, 2024 р.,

У кваліфікаційній роботі розкрито особливості формування і управління в системі створення стратегії безпеки підприємств, установ, організацій на прикладі товариства з обмеженою відповідальністю. Мета полягає в аналізі особливостей формування стратегії безпеки організації в сучасних умовах та напрацювання рекомендацій щодо управління нею.

Проаналізований вплив воєнного стану на роботу організації і розробку її стратегії безпеки, а також сформовані пропозиції щодо перегляду стратегій безпеки таким чином, щоб у оновлених варіантах передбачити: можливість забезпечення резервного джерела електропостачання; обов'язкову розробку плану дій на випадок відключення електроенергії, що включатиме порядок реагування на планові та позапланові відключення, алгоритм забезпечення безпеки працівників та процедуру відновлення роботи виробництва; організацію навчання працівників з питань безпеки в умовах відключення електроенергії задля мінімізації ризиків для себе та підприємства.

Впроваджено рекомендації щодо створення та управління стратегією безпеки на ТОВ «ВІНГАЛАГРО» з урахуванням сучасного інструментарію менеджменту.

КЛЮЧОВІ СЛОВА:. менеджмент, стратегія безпеки, організація, воєнний стан, управління ризиками.

ABSTRACT

Shvets F.V. “Formation and management of the organization’s security strategy”, specialty 073 Management, Vinnytsia State Pedagogical University named after Mykhailo Kotsiubynsky, Vinnytsia, 2024

The qualification work reveals the features of the formation and management in the system of creating a security strategy for enterprises, institutions, organizations using the example of a limited liability company. The goal is to analyze the features of forming an organization’s security strategy in modern conditions and develop recommendations for its management.

The impact of martial law on the organization’s work and the development of its security strategy was analyzed, and proposals were made to revise security strategies in such a way that the updated versions provide for: the possibility of providing a backup source of power supply; mandatory development of an action plan in the event of a power outage, which will include the procedure for responding to planned and unplanned outages, an algorithm for ensuring employee safety and the procedure for restoring production; organization of training of employees on safety issues in conditions of power outages in order to minimize risks for themselves and the enterprise.

Recommendations for the creation and management of a safety strategy at LLC "VINGALAGRO" were implemented, taking into account modern management tools.

KEYWORDS:. management, safety strategy, organization, martial law, risk management**.**

ЗМІСТ

ВСТУП

Актуальність теми наукового дослідження. З огляду на стрімкий розвиток технологій, глобальну конкуренцію та нестабільність у світовій економіці сучасне корпоративне управління потребує комплексного підходу до забезпечення безпеки, який охоплює не лише технічні та інформаційні аспекти, але й вимагає виважених управлінських та стратегічних рішень. Відтак формування та впровадження ефективної стратегії безпеки має бути пріоритетом для організацій усіх типів, які прагнуть залишатися конкурентоспроможними та впевнено крокувати у світі економічних викликів.

Відтак наукове дослідження з питань формування стратегії безпеки в організації, на підприємстві в сучасних умовах є надзвичайно актуальним та має практичне значення, оскільки спрямоване на розробку ефективних інструментів та методів для адаптації бізнесу до нових реалій господарювання.

Література. При підготовці до написання роботи нами було розглянуто та проаналізовано різні джерела. Так, науково-теоретичним підґрунтям цього дослідження стали праці з теорії менеджменту, економіки, підприємництва та права. Зокрема, окремо слід відзначити наукові праці таких вчених, як: Т. Сабецька, яка ретельно дослідила особливості формування організаційно-економічного механізму забезпечення економічної безпеки сучасного підприємства; Л. Ковальська, О. Голій та В. Голій, що присвятили свою увагу вивченню сутності, структури та механізмів забезпечення економічної безпеки підприємства; С. Міщенко, який здійснив ґрунтовний аналіз концептуальних аспектів економічної безпеки підприємств у ринковій економіці; О. Борисюк та Д. Маленицький, основою дослідження яких стала сутність стратегії та її значення для безпеки підприємства. Водночас нормативно-правову базу роботи складають законодавчі акти, що регулюють питання забезпечення безпеки в організаціях, а саме: Кодекс цивільного захисту України, Господарський та Цивільний кодекси України, постанова Кабінету Міністрів України «Деякі питання ідентифікації об’єктів підвищеної небезпеки», укази Президента

України «Про Положення про технічний захист інформації в Україні», «Про введення воєнного стану в Україні» та інші.

Мета дослідження полягає в аналізі особливостей формування стратегії безпеки організації в сучасних умовах та напрацювання рекомендацій щодо управління нею.

Для досягнення мети були поставлені такі **завдання:**

– визначити стан дослідження особливостей формування стратегії безпеки організації в сучасних умовах;

– дослідити теоретичні основи формування стратегії безпеки організації;

– охарактеризувати основні елементи формування стратегії економічної безпеки організації;

– окреслити особливості формування та реалізація стратегії безпеки організації в кризових ситуаціях;

– визначити основні елементи зарубіжного досвіду щодо стратегічного управління безпекою організацій.

Об’єктом дослідження є управління організацією.

Предметом дослідження є формування та управління стратегією безпеки організацією в сучасних умовах.

Методи дослідження. Робота виконана із використанням загальнонаукових та спеціальних методів.

Серед загальнонаукових методів, зокрема, використано методи індукції та дедукції – для визначення стану дослідження особливостей формування стратегії безпеки підприємства в сучасних умовах, методи формальної логіки та узагальнення – для простеження закономірностей розвитку дефініцій та процесів формування понять «стратегія безпеки підприємства» та «стратегія економічної безпеки підприємства», а також метод комплексного аналізу основних елементів формування стратегії економічної безпеки організації. Крім цього вагому роль у дослідженні відіграли і методи абстрагування та прогнозування, які застосовувалися насамперед при виявленні та конкретизації

найкращих механізмів забезпечення безпеки організацій всіх типів в умовах воєнного стану.

Водночас спеціальними методами, які використовувались у роботі, є, наприклад, методи аналізу прогалин, системний аналіз, вибірковий метод тощо.

Наукова новизна: полягає у впровадженні в діяльність ТОВ «Вінгалагро» таких заходів: призначення особи/ створення штатної структури, відповідальної за вирішення питань безпеки; проведення навчання (тренінгів) для майбутніх працівників для їх ознайомлення з основними правилами забезпечення безпеки організації; здійснення поділу конфіденційної інформації підприємств на блоки і допуск до них (в разі необхідності) лише через коди доступу; організація контролю роботи працівників за сумісництвом (для недопущення конфлікту інтересів і витоку даних).

Практичне значення одержаних результатів полягає у тому, що організації усіх типів які функціонують в Україні набули унікальний досвід реагування на особливі стани, зокрема воєнний. Відтак вивчення цього досвіду, порівняння його з іншими успішними практиками дозволяють запропонувати дієві заходи щодо організації системи безпеки підприємств та організацій. Зокрема в дослідженні визначено вплив воєнного стану на роботу організації і розробку його стратегії безпеки, а також сформовано пропозиції щодо перегляду стратегій безпеки таким чином, щоб у оновлених варіантах передбачити: можливість забезпечення резервного джерела електропостачання; обов’язкову розробку плану дій на випадок відключення електроенергії, що включатиме порядок реагування на планові та позапланові відключення, алгоритм забезпечення безпеки працівників та процедуру відновлення роботи виробництва; організацію навчання працівників з питань безпеки в умовах відключення електроенергії задля мінімізації ризиків для себе та підприємства тощо.

Апробація. Опубліковані тези:

1.Швець Ф.В. Розробка стратегії економічної безпеки організації та забезпечення її кадрового потенціалу. Збірник матеріалів Науково-практичного

симпозіуму «Ринок праці, людський капітал та професійна орієнтація молоді в умовах війни» (Вінниця, 10.05.2024 р.). Вінниця, 2024. С.45-49

2. Швець Ф.В. Сутність стратегії безпеки організації. Збірник матеріалів круглого столу «Філософія публічного управління, менеджменту та функціонування медіа» (Вінниця, 18.11.2024 р.) Вінниця, 2024 С. 37-43.

Структура роботи: вступ, 3 розділів, 9 підрозділів, висновки, список використаних джерел та додатки. Повний обсяг роботи складає __ сторінок. Список використаних джерел містить 81 позицію.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ СТРАТЕГІЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

1.1. Стан дослідження особливостей формування стратегії безпеки організації в сучасних умовах

Сучасний бізнес, опинившись під впливом глибоких змін у економічному, технологічному та соціальному середовищі, постійно постає перед унікальними викликами та загрозами, які потребують інноваційного підходу до стратегічного управління безпекою. Зокрема, сьогоденні реалії вимагають від підприємств не лише адаптації до непередбачуваних викликів, але й активного управління ризиками та забезпечення ефективного захисту від потенційних небезпек. У таких умовах формування ефективної стратегії безпеки підприємства стало визначальним фактором збереження його конкурентоспроможності та стійкості у контексті високого рівня нестабільності у світовій економіці. З огляду на це, вивчення питання формування стратегії безпеки підприємства в сучасних умовах є одним з провідних напрямків наукових досліджень вітчизняних та зарубіжних науковців.

Так, передусім слід згадати українську вчену Т. Сабецьку, яка присвятила аналізу заданої теми не одну наукову працю. Наприклад, у своїй статті «Особливості формування організаційно-економічного механізму забезпечення економічної безпеки сучасного підприємства» вона дослідила проблематику формування механізму забезпечення економічної безпеки підприємства в умовах розвитку вітчизняної економіки [1, с. 118]. Разом з тим ґрунтовними є також праці «Теоретичні засади стратегічного планування економічної безпеки підприємства» та «Поняття та класифікація інноваційних стратегій економічної безпеки підприємства», написані дослідницею у співавторстві з В. Сабецьким та А. Вакарчуком відповідно [2; 3, с. 130]. Таким чином, із вищезазначеного стає цілком очевидно, що Т. Сабецька спільно з іншими науковцями в своїх

дослідженнях висвітлює не лише окремі теоретичні питання формування стратегії безпеки підприємства, а й розкриває актуальні проблеми, які чатують на підприємства в умовах економічної та соціальної нестабільності, а також надає практичні рекомендації для формування стратегій безпеки та управління персоналом. Її внесок у розвиток наукової бази є важливим для розуміння сучасних викликів та можливостей у сфері економічної безпеки підприємств.

Не менш важливою є також робота «Концептуальні аспекти економічної безпеки підприємств у ринковій економіці» С. Міщенка, у якій вчений розкриває ключові питання формування та забезпечення економічної безпеки підприємств в умовах сучасної ринкової економіки [4, с. 190]. У своїй праці він, зокрема, ретельно вивчає основні елементи системи безпеки підприємства та акцентує особливу увагу на важливості стратегічного планування та формування стратегії безпеки підприємства.

Окрім С. Міщенка, всебічний аналіз сутності економічної безпеки підприємства, її компонентів та механізму забезпечення досліджує також О. Орлик. Так, у одній зі своїх статей він насамперед комплексно досліджує особливості та основи формування стратегії забезпечення фінансово-економічної безпеки підприємства [5, с. 67]. Враховуючи творчий підхід та глибокий аналіз О. Орлика, можна зазначити, що його наукові дослідження інтегрують теоретичний підхід та практичний досвід, сприяючи розвитку наукових основ стратегічного управління економічною безпекою підприємств в сучасних умовах.

Схожою тематика досліджень щодо вивчення механізму формування стратегії забезпечення економічної безпеки підприємства прослідковується і в роботах Л. Васільєвої. Велике теоретичне значення має, приміром, її праця «Теоретичні засади механізму формування стратегії забезпечення економічної безпеки підприємства» у якій вчена аналізує методологічні підходи до визначення основних етапів розробки стратегії забезпечення економічної безпеки та її впровадження в практику підприємств. Так, її дослідження спрямовані на визначення сутності стратегічного управління безпекою

підприємств, а також вивчення конкретних механізмів, які дозволяють ефективно реалізовувати стратегії для забезпечення стійкості та успішності бізнесу [6].

Поміж інших визначних дослідників, які присвятили свою увагу вивченню питання особливостей формування стратегії безпеки підприємств, необхідно згадати і Л. Ковальську, О. Голія та В. Голія. Вказані науковці здійснили значний внесок у розуміння сутності, структури та механізмів забезпечення економічної безпеки підприємств, зокрема, вони системно дослідили ключові аспекти цього питання та розробили власну класифікацію стратегій економічної безпеки підприємств [7, с. 126].

На нашу думку, показовою з практичного погляду є і робота старшого директора з інформаційної безпеки платформи Smartsheet П. Олерта щодо визначення критичних принципів безпеки підприємства [8]. Зокрема, вона відображає саме ті принципи, яких дійсно дотримується зазначена організація при розробці своєї стратегії безпеки. Проте не меш вагоме прикладне значення має і стаття менеджера із забезпечення безпеки Infopulse Д. Сіроша, який глибинно дослідив питання реорганізації та централізації системи кібербезпеки підприємств шляхом проведення різних статистичних досліджень та створення матриці ризиків для ІТ-безпеки підприємств [9]. На нашу думку, згадані роботи можуть бути основою для вивчення та імплементації позитивного практичного вітчизняного та світового досвіду щодо розробки і реалізації стратегії безпеки підприємства будь-якої сфери діяльності.

Крім того, з огляду на те, що метою цієї роботи є системне дослідження та аналіз особливостей формування стратегії безпеки підприємства в сучасних умовах, то слід наголосити і на стані дослідження питання стратегічного управління підприємством в деяких актуальних кризових ситуаціях, а саме в умовах воєнного стану та при екстрених відключеннях електроенергії. Отож загалом варто насамперед зауважити, що наразі кількість наукових праць, присвячених даній темі, обмежена. Проте деякі вчені все ж активно

спрямовують свої зусилля на виявлення оптимальних стратегій управління в умовах надзвичайних обставин.

Наприклад, Р. Майстро і О. Більовська зосередилися на вивченні конкурентоспроможності бізнесу в умовах війни в Україні [10, с. 21], О. Мінц та Г. Дорошкевич, зі свого боку, проаналізували різні сценарії подолання енергетичного колапсу підприємствами малого бізнесу України [11, с. 61], а основний зміст одного з досліджень Л. Кримчак становить розкриття проблеми трансформації ризиків та загроз економічної безпеки вітчизняних суб'єктів господарювання [12, с. 56]. Вичерпною є також праця «Особливості підбору персоналу на українському ринку праці в умовах воєнного стану», написана І. Панченком у співавторстві з О. Вітковською [13, с. 200]. Ця робота є цінною, оскільки авторам вдалося докладно охарактеризувати сучасну ситуацію на ринку праці, зокрема, в контексті воєнного стану. І хоча зазначені доробки не розривають всі аспекти формування стратегії безпеки підприємства в кризових ситуаціях, однак вони в сукупності з іншими дослідженнями, зокрема журналістськими, таки роблять значний внесок у розвиток наукового розуміння цієї теми і дозволяють отримати комплексне уявлення про можливі шляхи вирішення проблем, які стосуються безпеки підприємств.

Насамкінець вважаємо за доцільне зазначити, що теоретичні та практичні аспекти формування стратегії безпеки підприємства в сучасних умовах, досліджували й інші вчені: Ю. Богач, О. Борисюк, С. Бортнік, В. Варга, О. Васьків, О. Вівчар, О. Гетьман, Ю. Глушач, Р. Горин, О. Гуменюк, О. Данченко, І. Доценко, С. Дуда, К. Жирій, В. Занора, О. Захаров, М. Зяйлик, Н. Кривокульська, Ж. Крисько, Н. Кубіній, Л. Лаврентьєва, Д. Маленицький, О. Марценюк, Г. Матвіїшина, О. Мельничук, В. Мойсєєва, В. Москальчук, В. Носалюк, О. Орлик, В. Панченко, Ю. Поскрипко, В. Приймак, Я. Прищепа, П. Пуцентейло, О. Роженко, Н. Стеклова, О. Фальченко, О. Хитра, С. Царюк, А. Шкальова, Л. Шостак, О. Штоляр, Н. Якимова. Вказані науковці також зробили не менш вагомий внесок у формування наукового підґрунтя щодо здійснення стратегічного управління безпекою підприємств.

Отже, вивчення науковцями питання формування стратегії безпеки підприємства має важливе значення для розвитку теоретичних засад та практичних аспектів управління безпекою в сучасних умовах оскільки роботи вчених сприяють розширенню розуміння сутності та складових стратегії безпеки, а також надають цінні рекомендації для підприємств у їхніх зусиллях з забезпечення ефективного захисту від загроз. Але навіть незважаючи на наявність різних наукових праць, питання особливостей формування стратегії безпеки підприємства в сучасних умовах є все ще недостатньо вивченим. У контексті дослідження заданої теми, на нашу думку, доволі актуальною мала б бути і проблема визначення конкретних етапів розробки стратегії безпеки підприємства. Проте, проаналізувавши різні вітчизняні джерела та зарубіжні ресурси, ми дійшли висновку, що попри свою важливість, зазначене питання детально вивчають тільки декілька вчених, зокрема: Л. Лаврентьєва, О. Гавриш та Г. Черняк.

Таким чином, вивчення особливостей формування стратегії безпеки підприємства в сучасних умовах залишається актуальним та критично важливим для сучасного бізнесу, особливо з огляду на появу таких нових ризиків для підприємств, як: постійні кібератаки, масовані обстріли об’єктів інфраструктури, різкі зміни на ринку праці, екстрені відключення електроенергії тощо.

1.2. Поняття та сутність стратегії безпеки організації, принципи її формування

У контексті сучасного динамічного бізнес-середовища, у якому технологічні виклики, економічні коливання та різноманітні ризики стають частиною підприємницької реальності, невід'ємним елементом ефективного управління діяльністю підприємства є формування його стратегії безпеки, яка передбачає комплексний аналіз зовнішнього та внутрішнього середовища, ідентифікацію потенційних загроз і ризиків, а також розробку ефективних заходів для їх запобігання.

На думку С. Міщенка, основними елементами безпеки підприємства є: захист комерційної таємниці і конфіденційної інформації, комп'ютерна безпека, внутрішня безпека, безпека будівель і споруд, фізична безпека, технічна безпека, безпека зв'язку, безпека перевезень вантажів і осіб, екологічна безпека, конкурентна розвідка тощо [4, с. 193]. І хоча, як видно з дослідження вказаного вченого, безпека підприємства охоплює багато різноманітних факторів, однак при цьому варто зауважити, що говорячи про формування стратегії безпеки підприємства, переважна більшість вітчизняних науковців мають на увазі розробку саме стратегії економічної безпеки, оскільки економічні інтереси є основою існування та розвитку підприємства. Відтак від стану економічної безпеки підприємства залежить його здатність ефективно функціонувати та розвиватися. Недотримання вимог економічної безпеки може призвести до таких негативних наслідків, як, наприклад, фінансові втрати, втрата конкурентоспроможності, зниження ефективності діяльності тощо.

Вітчизняні та зарубіжні вчені трактують визначення поняття «стратегія економічної безпеки» неоднозначно, у зв'язку з чим наразі не існує єдиного визначення вказаного терміну. Це, на нашу думку, насамперед пов'язано з тим, що стратегія безпеки визначає комплексні підходи та дії, спрямовані на забезпечення надійності, стійкості та захищеності підприємства. Так, зазначений термін об'єднує велику кількість питань, а безпосереднє

формування конкретної стратегії залежить і від особливостей галузі, у якій діє підприємство.

Зокрема, досліджуючи це питання, О. Фальченко та Ю. Глушач визначають стратегію економічної безпеки як «економічну систему забезпечення економічної безпеки підприємства в довгостроковому періоді, що являє собою сукупність приватних взаємоузгоджених складових, які об'єднує єдина глобальна мета – досягнення рівня економічного прибутку» [14, с. 157]. Л. Васільєва зауважує на такій дефініції вищезазначеного терміну: «Стратегія політики економічної безпеки в управлінні підприємством – це комплекс і взаємодія важливих заходів, а також система заходів і методів, які визначають безпеку підприємства як зараз, так і в майбутньому» [6, с. 16]. О. Захаров, зі свого боку, стверджує, що «це довготривалі, найбільш принципові і важливі установки, плани, наміри керівників (власників) підприємства, спрямовані на створення та постійний розвиток системи економічної безпеки, здатної адекватно протидіяти всім внутрішнім та зовнішнім небезпекам і загрозам його стабільної роботи та розвитку в даний час, а також у найближчій та віддаленій перспективах» [15, с. 275]. Л. Лаврентьєва вважає, що досліджуване поняття насамперед слід розуміти як «функціональну стратегію забезпечення економічної безпеки у довгостроковому періоді, яка представляє собою сукупність засобів, заходів, рішень та інструментів, спрямованих на подолання негативного впливу загроз та ризиків задля досягнення рівня економічного прибутку фінансової стійкості та економічного зростання в умовах динамічності зовнішнього середовища» [16, с. 51]. Водночас, на думку Т. Сабецької і В. Сабецького, стратегія економічної безпеки підприємства – це «комплексна, орієнтована на тривалу перспективу цілісна концепція сталого й безпечного розвитку підприємства на основі побудови адекватної й ефективної системи економічної безпеки, яка здатна вчасно реагувати на будь-які загрози й небезпеки, максимально нівелюючи їх негативний вплив на підприємство» [2].

І хоча усі згадані дефініції відображають складність і багатогранність підходів до тлумачення поняття «стратегії економічної безпеки підприємств» та

акцентують увагу насамперед на необхідності довгострокового планування, цілісності концепції та реагування на різноманітні виклики та загрози, однак ми вважаємо, що найбільш повне та вдале визначення надала саме Л. Лаврентьєва. На нашу думку, визначення саме цієї вченої акцентує увагу на системному та цілеспрямованому характері стратегії, підкреслюючи, що вона повинна бути не лише довгостроковою, але й спрямованою на створення сприятливих та безпечних умов для реалізації завдань підприємства.

Не менш важливо також зауважити, що з усіх вищезазначених визначень, попри їх чималу кількість, можна визначити і ключові завдання, які має вирішувати стратегія економічної безпеки. Відтак загальною метою розробки такої стратегії є насамперед створення умов для стійкого і безпечного функціонування підприємства в умовах існування економічної нестабільності та постійного виникнення різноманітних ризиків. Що стосується інших завдань, то вони можуть варіюватися в залежності від конкретних обставин та особливостей підприємства, однак основними, на думку багатьох вітчизняних вчених, є саме такі:

– мінімізація витрат, пов'язаних з коливаннями на фінансових ринках, змінами валютних курсів та іншими факторами, що можуть впливати на економічну стабільність підприємства;

– створення потенціалу формування фінансових ресурсів підприємства, адекватного потребам його стратегічного розвитку, а саме: забезпечення реалізації корпоративної стратегії підприємства, зростання потенціалу формування фінансових ресурсів підприємства з внутрішніх джерел та забезпечення необхідної «фінансової гнучкості» підприємства (достатнього доступу до зовнішніх джерел фінансування) [5, с. 69];

– оптимізація розподілу фінансових ресурсів підприємства по напрямкам та формам інвестування за критерієм їх ефективності, тобто, по-перше, забезпечення необхідної пропорційності розподілу фінансових ресурсів за напрямками інвестування; по-друге, забезпечення необхідної пропорційності розподілу фінансових ресурсів за стратегічними зонами господарювання; по-

третє, забезпечення необхідної пропорційності розподілу фінансових ресурсів за стратегічними господарськими одиницями підприємства [5, с. 69];

– забезпечення стійкості ланцюга постачання, тобто диверсифікація постачальників, визначення стратегічних резервів та управління ризиками у виробничому процесі;

– збереження репутації та відносин зі зацікавленими сторонами, що сприяє стабільності та довірі до підприємства;

– формування системи умов підвищення якості управління діяльністю підприємства у стратегічній перспективі, що охоплює як забезпечення високого рівня кваліфікації та організаційної культури менеджерів, так і формування достатньої інформаційної бази для розробки альтернативних рішень щодо розвитку підприємства і ефективної організаційної структури управління його діяльністю [5, с. 69];

– адаптація до змін в зовнішньому середовищі, тобто вчасна реакція на зміни в законодавстві, технологічних та ринкових тенденціях;

– створення резервів і запасів, які дозволятимуть підприємству ефективно продовжувати свою роботу в непередбачуваних та навіть кризових ситуаціях.

Таким чином, усі зазначені завдання яскраво демонструють, що стратегія економічної безпеки, безперечно, є невід'ємною складовою загальної стратегії безпеки підприємства і ключовим інструментом, який забезпечує як швидку адаптацію до змін в економічному середовищі, так і допомагає досягнути довгострокового успіху [17, с.43].

Стратегія безпеки підприємства, як і будь-яка інша стратегія, повинна ґрунтуватися на певних основоположних правилах – принципах, які здатні забезпечити її ефективність та результативність, а також відповідність потребам підприємства. Так, принципи формування стратегії безпеки насамперед виступають методологічним підґрунтям для розробки заходів забезпечення економічної безпеки підприємства.

На сьогодні існує чимала кількість підходів щодо того, які саме принципи варто враховувати при розробці стратегії безпеки підприємств. Так, наприклад, колектив авторів, до якого входять Л. Ковальська, О. Голій і В. Голій, визначає, що до основних принципів забезпечення безпеки підприємства, належить: системність, безперервність, гнучкість і адаптивність, інноваційна спрямованість, ефективність, раціональність та стратегічна орієнтація [7, с. 134-135].

Зі свого боку, О. Данченко, Ю. Поскрипко, В. Занора вважають, що стратегія безпеки підприємства повинна бути законною, ефективною, доцільною, системною, скоординованою, спланованою та динамічною [18, с. 113-114]. Схожої думки додержується і С. Міщенко, який з-поміж інших виділяє такі принципи формування стратегії безпеки підприємства, як: системність, своєчасність, безперервність та плановість [4, с. 192-193].

Водночас Н. Стеклова зазначає, що формування стратегічного управління безпекою підприємства, зокрема і економічною, має ґрунтуватися на принципах інтегрованості із загальною системою менеджменту, орієнтації на поставлені цілі діяльності підприємства, адаптивності механізму до мінливих умов зовнішнього та внутрішнього середовища, комплексного формування інформаційного простору для оцінки рівня економічної безпеки підприємства, діагностики рівня безпеки підприємства в умовах дії загроз внутрішнього та зовнішнього середовища, розробки та реалізації управлінських рішень з підвищення рівня економічної безпеки підприємства та контролю і регулювання рівня економічної безпеки підприємства [19, с. 226].

І. Доценко та О. Мельничук стверджують, що концептуальне управління економічною безпекою підприємства має здійснюватися з урахуванням принципів законності (відповідність нормам і законам, встановленим у державі на сучасному етапі суспільного розвитку); дотримання балансу інтересів особистості, підприємства, його найближчого економічного середовища, регіону, держави, суспільства загалом; взаємної відповідальності усіх структурних підрозділів, персоналу, стейкхолдерів, менеджменту підприємства

за забезпечення фінансово-економічної безпеки; взаємозв'язку усіх рівнів фінансово-економічної безпеки, а саме внутрішнього середовища підприємства та його зовнішнього середовища (на рівні взаємодії з іншими юридичними та фізичними особами, в межах регіону, держави, світогосподарської системи) [20, с. 83].

На особливу увагу заслуговує також думка В. Панченко, який, на основі власних досліджень та праць Г. Козаченко, Л. Шемаєвої, І. Белоусової, І. Мігус (Шульги), В. Франчука, В. Алькемої, Л. Гнилицької, О. Ляшенка, З. Живко, С. Кавуна, В. Андрієнка та М. Копитко, визначив такі основні принципи, як: законність та додержання прав і свобод людини і громадянина, пріоритетність превентивних заходів, пріоритетність захисту прав осіб в процесі забезпечення безпеки, конфіденційність, співробітництво, комплексне застосування сил та коштів, компетентність, економічна доцільність, планова основа діяльності, системність, інтегрованість у загальні завдання суб'єкта господарювання, принцип потенційної з'єднуваності, активного впливу, суб'єктності, принцип синергізму, рефлексії та компромісу [21].

Говорячи про зарубіжний досвід, не менш актуальний для всебічного аналізу досліджуваного питання, варто відзначити позицію міжнародної охоронної агенції DeltaGuard, відповідно до якої формування системи безпеки підприємства має будуватися на основі пріоритетності профілактичних заходів, законності, комплексного використання енергії та ресурсів, координації і взаємодія всередині та поза підприємством, поєднання прозорості з секретністю, компетентності, економічної доцільності, плановості і системності [22].

Також доцільно відзначити і доробок П. Олерта – старшого директора з інформаційної безпеки платформи Smartsheet, у якому він насамперед звертає увагу на основні чотири принципи безпеки підприємства, які важливо враховувати при розробці стратегії безпеки, а саме:

– принцип «найменших привілеїв» – фундаментальний принцип, що лежить в основі багатьох видів корпоративної безпеки різних компаній і

передбачає використання практики найменших привілеї, тобто надання кожному користувачеві лише стільки доступу, скільки їм потрібно для використання, виконання трудових обов'язків, і не більше;

– принцип «масштабного керування безпекою», який визначає нагальну потребу управління безпекою підприємства у зв'язку з плинністю кадрів та постійним обміном інформацією між працівниками;

– принцип захисту даних;

– принцип проведення аудиту і моніторингу безпеки [8, с. 2-6].

Таким чином, можна зробити висновок, що існує широкий спектр думок щодо визначення принципів формування стратегії безпеки підприємства. Проте, незважаючи на відмінності в підходах та на наявність більш ніж 20 принципів, про які згадували різні вітчизняні та зарубіжні вчені, ми виділили ряд ключових, що, на нашу думку, виступають базисом для розробки ефективної стратегії безпеки підприємства *(Додаток 1)*:

1. Законність – стратегія безпеки підприємства повинна відповідати чинному законодавству країни, у якій воно функціонує;

2. Системність – стратегія безпеки має розглядати підприємство як цілісну систему, яка складається з взаємопов'язаних елементів, оскільки це дозволяє забезпечити комплексний захист економічних інтересів підприємства від зовнішніх і внутрішніх загроз;

3. Адаптивність – при формуванні вказаної стратегії робочій групі та керівнику підприємства варто зосереджувати увагу на тому, аби вона була гнучкою та адаптивною до будь-яких можливих змін;

4. Раціональність та доцільність – заходи щодо забезпечення безпеки мають бути економічно обґрунтованими та не призводити до надмірних витрат;

5. Стратегічна орієнтація, тобто розробка стратегії безпеки з урахуванням стратегічних цілей підприємства;

6. Скоординованість – заходи щодо забезпечення безпеки повинні бути узгоджені між собою та з іншими аспектами діяльності підприємства;

7. Плановість, яка виражається в тому, що стратегія безпеки має розроблятися та впроваджуватися за певним планом з чітко визначеними етапами;

8. Конфіденційність та захист даних – у разі використання інформації, яка є конфіденційною для підприємства, вона обов'язково повинна бути захищена від несанкціонованого доступу, використання, модифікації або знищення;

9. Принцип проведення контролю (аудиту, моніторингу), який передбачає необхідність проведення керівництвом підприємства регулярних перевірок ефективності заходів щодо забезпечення безпеки.

Відтак усі згадані нами принципи взаємопов'язані та доповнюють один одного, а їх дотримання дозволяє забезпечити формування ефективної стратегії безпеки підприємства, яка в подальшому забезпечить стійкість, конкурентоспроможність та успішний розвиток організації.

2.3. Класифікація стратегій безпеки організації

Як вже можна було переконатися, в умовах сучасного бізнес-середовища, насиченого різноманітними ризиками, розробка та реалізація ефективної стратегії безпеки стають необхідністю для збереження стабільності та успішності підприємств у всіх галузях. Водночас велике значення надається не лише розумінню загального концепту безпеки, але і класифікаціям стратегій, які дозволяють підприємствам правильно реагувати на конкретні виклики.

Отож систематизація різноманітних стратегій безпеки відкриває можливості для кращого аналізу, планування та впровадження заходів, спрямованих на забезпечення стійкості та конкурентоспроможності підприємства. З огляду на важливість стратегії безпеки не лише як інструмента захисту від загроз, але і як ключового елемента стратегічного управління, спрямованого на досягнення позитивних результатів у довгостроковій перспективі, досліджуване питання привертає увагу як вчених і практиків, так і керівників підприємств. Зважаючи на це, наразі стратегії безпеки підприємства можна класифікувати за різними критеріями та підходами.

Так, ґрунтовний аналіз типології стратегій безпеки підприємств висвітлено, зокрема, у праці «Сутність стратегії та її значення для безпеки підприємства» О. Борисюк та Д. Маленицького. На основі праць українських та зарубіжних науковців автори вказаного дослідження зазначили, що загальні стратегії безпеки поділяються на чотири основні групи, а саме: конкурентні стратегії, стратегії відносин із суспільством, комерційні стратегії та портфельні стратегії. За цією класифікацією конкурентні стратегії являють собою стратегії товарної та ринкової диференціації; стратегії відносин із суспільством – це стратегії соціальної відповідальності та переговорів; комерційні стратегії, зі свого боку, охоплюють маркетингові, інноваційні та виробничі стратегії; а портфельні – це стратегії вдосконалення діяльності, товарної експансії, розвитку ринку та диверсифікації [23, с. 162].

Вказана типологія, на нашу думку, дозволяє глибше зрозуміти різноманітні аспекти управління безпекою підприємства і свідчить про те, що будь-який бізнес, незалежно від сфери діяльності, має бути готовим впроваджувати як конкурентоспроможні, комерційні та портфельні стратегії, так і активно взаємодіяти з суспільством через стратегії соціальної відповідальності та переговорів.

Одночасно із класифікацію стратегій безпеки за чотирма раніше охарактеризованими критеріями О. Борисюк та Д. Маленицький аналізують також й іншу класифікацію, яка передбачає поділ на такі стратегії, як: стратегії зростання (розвитку), стабілізації, виживання (скорочення) та ліквідації [23, с. 162-163].

Отож стратегія зростання (розвитку), як видно із самої її назви, використовується у сприятливих для підприємства умовах і розрахована на розширення його діяльності шляхом «виходу на нові ринки, підвищення якості продукції, поліпшення іміджу підприємства на ринку, здійснення технологічного розвитку підприємства, розроблення інноваційної продукції, підвищення ефективності використання персоналу» [23, с. 162-163].

Що стосується стратегії стабілізації, то її основним завдання є недопущення втрати вже зайнятих позицій на етапі досягнення найбільшого успіху, тобто на фазі так званого «піку» діяльності. Підтипами цієї стратегії, що також відображають і основні завдання, які мають здійснюватися в процесі впровадження та реалізації заходів стабілізації, прийнято називати: стратегію зниження витрат, стратегію реструктуризації та стратегія утримання позицій [23, с. 162-163].

Наступні взаємопов’язані стратегії – це стратегії виживання (скорочення) та ліквідації, які застосовуються керівниками на підприємстві, коли його діяльність вже не забезпечує такий прибуток, як раніше, або є зовсім не рентабельною. Однак суттєвою їх різницею є те, що при реалізації стратегії виживання все ж розглядається варіант виходу з кризи і відновлення прибутковості, а стратегія ліквідації передбачає повну або часткову ліквідацію

підприємства без можливості відновити його роботу у попередньому вигляді [23, с. 162].

Отже, ця класифікація описує базові стратегії безпеки, надає цільові орієнтири та відзначає конкретні завдання, які адміністрації слід вирішити в межах стратегічного управління на кожному етапі діяльності підприємства. Важливо підкреслити, що такий підхід дозволяє ефективно реагувати на виклики та забезпечує сталість розвитку бізнесу, зважаючи на конкретні обставини, в яких здійснюється робота.

Окремо, на нашу думку, варто виокремити і класифікацію стратегій економічної безпеки підприємства, які, як зазначалося раніше, доволі часто ототожнюються із загальними стратегіями безпеки з огляду на те, що саме економічні інтереси є основою існування та розвитку підприємства.

Відтак першим вважаємо за доцільне згадати концептуальний підхід, запропонований О. Роженко, який охоплює дві концепції: нижнього та вищого рівнів. Зокрема, концепція нижчого рівня розглядає економічну безпеку як протистояння загрозам, а за концепцією вищого рівня економічна безпека виступає формою розвитку і уподібнюється до певного результату, визначається як досягнення цілей функціонування і не передбачає подолання загроз та викликів [24, с. 54].

З концепції нижнього рівня випливають так звані інтереси протистояння загрозам (забезпечення стабільності та безперервності виробничої діяльності при здатності до протистояння) та інтереси стабільності (гарантування фінансово-економічної стійкості, при здатності бізнесу до адаптації), що формують відповідно два типи стратегій безпеки підприємства – виживання і існування [24, с. 54].

Тим часом з концепції вищого рівня прийнято виділяти лише один інтерес – розвиток, тобто ефективне використання ресурсів, при здатності підприємства до постійного розвитку. І саме з інтересу розвитку виділяються дві інші важливі стратегії – обмеженого зростання та зростання [24, с. 54].

Схожа класифікація наводиться також у роботі «Формування стратегій забезпечення економічної безпеки підприємства» Г. Коптєвої. Відповідно до дослідження вченої стратегії забезпечення економічної безпеки бізнес-процесів підприємств залежно від зон безпеки, які поділяються на шість основних видів:

– «стратегія виживання – зона найвищого рівня безпеки;

– стратегія стабілізації – зона низького рівня безпеки;

– стратегія підтримки – зона граничного рівня безпеки;

– стратегія обмеженого зростання – зона достатнього рівня безпеки;

– стратегія зростання – зона високого рівня безпеки;

– стратегія сталого розвитку – зона найвищого рівня безпеки» [25, с. 218].

Як бачимо, вказані класифікації О. Роженко і Г. Коптєвої не надто відрізняється від вже згаданої раніше класифікації О. Борисюк та Д. Маленицького. Так, стратегії виживання, існування, обмеженого зростання, зростання, стабілізації, підтримки та сталого розвитку, які виокремлюють О. Роженко і Г. Коптєва, перегукуються із стратегіями зростання (розвитку), стабілізації, виживання (скорочення) та ліквідації О. Борисюк та Д. Маленицького.

Це зайвий раз доводить, що науковці та експерти розглядають питання економічної безпеки як невід'ємну частину загальної стратегії підприємства. При цьому відсутність чіткого розмежування між стратегіями безпеки та економічної безпеки є викликом для розвитку більш конкретних та адаптованих підходів до побудови стратегій економічної безпеки, які враховували б усі особливості сучасного бізнес-середовища.

Варто зауважити, що хоча ототожнення зазначених стратегій все ж відбувається, проте Л. Ковальська, О. Голій та В. Голій запропонували таку класифікацію, яка є більш властивою саме для стратегій економічної безпеки. Зокрема, згадані автори за критерієм стану економічної безпеки підприємства виділяють чотири типи стратегій безпеки, а саме:

– стратегія формування передумов забезпечення економічної безпеки, застосування якої доцільне, коли підприємство знаходиться у стані небезпеки. Така стратегія передбачає створення керівництвом підприємства необхідних умов для гарантування безпеки, наприклад, може здійснюватися створення інформаційної бази, формування кадрового та фінансового потенціалу, а також матеріально-технічної бази підприємства;

– стратегія фокусування забезпечення економічної безпеки, яка є раціональною, коли підприємство знаходиться у стані ризику. При розробці, впровадженні та реалізації цієї стратегії адміністрації необхідно здійснити концентрацію ресурсів, зокрема і фінансових, на вирішенні найбільш актуальних проблем, що дозволить у найкоротший термін вийти зі стану ризику та перейти до стану безпеки;

– стратегія активізації процесів забезпечення економічної безпеки, яка впроваджується при виникненні на підприємстві стану загрози з метою зосередження діяльності на тих напрямах роботи, які є найбільш важливими для стійкого функціонування та забезпечення економічної безпеки;

– стратегія підтримки стану економічної безпеки, що, виходячи з назви, є актуальною, коли підприємство функціонує у стані безпеки і основним завданням його діяльності є підтримка вже наявних позитивних тенденцій розвитку [7, с. 133-134].

На наше глибоке переконання, враховуючи актуальність та наукову обґрунтованість усіх згаданих Л. Ковальською, О. Голієм та В. Голієм стратегій, їх застосування може виявитися ефективним інструментом для забезпечення економічної безпеки підприємств в різних умовах, тобто у всіх можливих станах: небезпеки, ризику, загрози та безпеки. Окрім цього, така класифікація здатна слугувати і підґрунтям для розробки та реалізації нових стратегій, спрямованих на досягнення оптимального рівня економічної безпеки та гарантування стабільності підприємства в різних сценаріях його функціонування.

Разом з тим актуальною, зважаючи на стрімке поширення сучасних технологій, є також класифікація стратегій економічної безпеки, розроблена А. Вакарчуком та Т. Сабецькою. Як основний критерій поділу стратегій на типи науковці використали напрям стратегічного розвитку, який визначається з урахуванням того, які методи господарювання використовуються підприємством для подолання загроз. Так, згідно з наведеною класифікацією підприємство може обрати один із двох шляхів забезпечення економічної безпеки: або стратегію традиційного розвитку, тобто використання традиційних засобів ведення господарської діяльності, або стратегію інноваційного розвитку, яка передбачає постійний пошук нових способів підвищення ефективності діяльності підприємства і охоплює як розвиток нових ринків і покращення якості продукції, так і зміну внутрішньої структури підприємства [3, с. 131-132].

На особливу увагу заслуговує також і класифікація О. Гавриша та Г. Черняк, які, проаналізувавши різні наукові підходи, виокремили два види стратегій забезпечення економічної безпеки: «стратегію підтримання економічної безпеки (нівелювання існуючих загроз, превенції загрозам, компенсації збитку) та стратегію відновлення економічної безпеки (збільшення прибутків, зниження витрат, продажу активів, комплексна стратегія відновлення)» [26]. Такий підхід відображає складність завдань, які стоять перед керівництвом підприємств у сучасних умовах та визначає необхідність індивідуального підходу до розробки та впровадження стратегій безпеки.

Отже, аналіз різних класифікацій дозволяє розкрити різноманітні аспекти формування стратегій безпеки та зробити обґрунтований вибір стратегії, враховуючи унікальні умови конкретного підприємства. Ми вважаємо, що кожна з досліджених класифікацій має право на існування, оскільки усі вони, по-перше, розглядають загальну стратегію безпеки та стратегію економічної безпеки як багатогранні та складні поняття, що охоплюють усі сфери діяльності бізнесу, та, по-друге, вказують на те, що вибір стратегії безпеки має залежати від особливостей, притаманних тому чи іншому підприємству, зокрема від

характеру і масштабу його роботи, конкретних загроз, можливих ризиків та фінансових можливостей.

РОЗДІЛ 2
ОСНОВНІ ЕЛЕМЕНТИ ФОРМУВАННЯ СТРАТЕГІЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ (НА ПРИКЛАДІ ТОВ «ВІНГАЛАГРО»)

3.1. Етапи розробки стратегії економічної безпеки організації

Розробка стратегії економічної безпеки та формування загальної стратегії безпеки підприємства, є складним та відповідальним процесом, який вимагає ретельного вивчення внутрішніх і зовнішніх факторів, що впливають на його діяльність.

Аналіз наукової літератури щодо цього питання вказує на те, що єдиного визначеного порядку розробки стратегії економічної безпеки підприємства також не існує, як і визначення зазначеного поняття. Однак, враховуючи найбільш загальний підхід, вважаємо за доцільне згадати насамперед концепцію, яку пропонує Л. Лаврентьєва. Так, у своєму дослідженні вчена виокремлює шість основних етапів, які підприємство має пройти при розробці стратегії економічної безпеки, аби вона була ефективною та результативною, а саме:

1. Визначення глобальної цілі діяльності підприємства.

2. Виявлення резервів підвищення ефективності можливостей операційної діяльності і врахування зовнішніх небезпек.

3. Вибір елементів, які включатиме сама стратегія.

4. Визначення локальних цілей діяльності підприємства.

5. Тактичне планування і розроблення альтернативних варіантів тактичних дій.

6. Контроль за виконанням та результатами реалізації стратегії [16, с. 52].

Досліджуючи концепцію Л. Лаврентьєвої, ми звернули увагу на те, що, хоча вона є доволі універсальною, однак потребує певних уточнень.

Зокрема, вважаємо, що першочерговим завданням при розробці стратегії економічної безпеки, який не включила у своє дослідження згадана вчена, має бути формування робочої групи. Відтак перед тим, як визначати цілі діяльності

підприємства, вибирати елементи, які включатиме стратегія економічної безпеки, необхідно спершу визначити осіб, які відповідатимуть за її розробку.

Аналізуючи наукову працю О. Гавриша та Г. Черняк, ми дійшли висновку, що формування зазначеної робочої групи може здійснюватися двома шляхами:

1. «Зверху-вниз», коли керівництво підприємства ініціює процес формування стратегії економічної безпеки і уповноважує відділ економічної безпеки на її розроблення з подальшим погодженням;

2. «Знизу-вверх», коли процес розробки стратегії забезпечення економічної безпеки ініціює структурний підрозділ, що відповідає за забезпечення економічної безпеки [26].

Однак, незважаючи на те, який саме спосіб буде обрано при формуванні робочої групи, до її складу, на нашу думку, повинні входити представники різних рівнів управління підприємством, а також зовнішні експерти, оскільки саме така різноманітність та компетентність думок може якнайкраще вплинути на ефективність процесу розробки стратегії економічної безпеки. Так, представники різних рівнів управління підприємством можуть надати групі необхідну інформацію про діяльність підприємства, його сильні та слабкі сторони та потенційні загрози і ризики, а зовнішні експерти – експертні знання та досвід у сфері забезпечення економічної безпеки.

Доповнюючи концепцію Л. Лаврентьєвої щодо першого етапу, який полягає у визначенні глобальної цілі діяльності підприємства, важливо додати, що при його реалізації керівникам підприємств варто чітко сформулювати стратегічну мету, яка відображатиме основні завдання та методи досягнення успіху. Так, глобальна ціль має бути цілісною і конкретною, а також обов’язково визначати бажаний результат.

Після визначення глобальної цілі доцільно також здійснювати виявлення резервів підвищення ефективності операційної діяльності та врахування зовнішніх небезпек. Цей етап є критичним для забезпечення стійкості і успішності, а тому вимагає від відповідальних за розробку стратегії ретельного

вивчення внутрішнього та зовнішнього середовища підприємства. Наприклад, внутрішній аналіз ресурсів підприємства може охоплювати оцінку ефективності внутрішніх процесів, виявлення можливих технологічних і організаційних проблем, дослідження сильних та слабких сторін компанії та визначення можливих перспектив розвитку, а зовнішній – вивчення актуальних ринкових тенденцій, конкурентних ситуацій, технологічних інновацій, змін у законодавстві та інших факторів, що можуть впливати на діяльність підприємства. Таким чином, саме процес виявлення резервів підвищення ефективності операційної діяльності та зовнішніх небезпек дозволяє підприємству ідентифікувати та вдосконалити різноманітні ресурси підприємства, що, зі свого боку, впливає на економічну безпеку.

Надалі, згідно із концепцією Л. Лаврентьєвої, здійснюється вибір елементів, які включатиме сама стратегія. Зокрема, на цьому етапі, на нашу думку, варто ретельно дослідити та обрати найефективніші організаційно-структурні, кадрові, інформаційні та фінансові заходи, що здатні будуть створити систему управління економічною безпекою, а також забезпечити підприємство необхідними фінансовими ресурсами, кваліфікованими кадрами та дієвими механізмами збереження інформації, яка є важливою для забезпечення економічних інтересів підприємства.

На наступному, однак не менш важливому, четвертому етапі найчастіше прийнято визначати локальні цілі діяльності підприємства, які будуть реалізовані в межах стратегії економічної безпеки. Так, локальні цілі повинні бути конкретними, вимірюваними, досяжними, релевантними та обґрунтованими. Отож вони мають визначати конкретні напрямки діяльності підприємства, які будуть спрямовані на забезпечення його економічної безпеки.

Наприклад, розглянемо ситуацію, коли метою стратегії економічної безпеки підприємства є забезпечення його фінансової стійкості. У такому разі локальними цілями можуть бути: формування резервного фонду у розмірі не менше, наприклад, трьох місяців поточних витрат, диверсифікація джерел фінансування та розвиток систем управління ризиками та персоналом.

Уточнюючим до четвертого етапу є також п’ятий – тактичне планування і розроблення альтернативних варіантів тактичних дій. Він може охоплювати такі елементи, як: визначення конкретних заходів, які будуть реалізовані для досягнення локальних цілей, розробка альтернативних варіантів тактичних дій для кожного з заходів оцінки ефективності альтернативних варіантів тактичних дій та вибір оптимального варіанту дій для кожного із заходів.

Завершальним етапом, який покликаний об’єднати всі попередні, Л. Лаврентьєва визначає контроль за виконанням та результатами реалізації стратегії. Відтак саме забезпечення можливості контролю дозволяє своєчасно виявити відхилення від запланованої стратегії економічного безпеки і вжити заходів для їх усунення.

Однак, ми також вважаємо за доцільне додати, що одночасно із контролем за виконанням та результатами реалізації стратегії має здійснюватися і оцінка її ефективності. Зокрема, цей етап здатен логічно завершити процедуру розробки стратегії економічної безпеки підприємства і визначити, наскільки вдалося досягти поставлених цілей. В подальшому ця інформація може бути використана для корегування стратегії економічної безпеки, розробки нових стратегічних цілей і завдань, оцінки ефективності діяльності підприємства в цілому.

Враховуючи запропоновані нами зміни, перелік етапів розробки стратегії економічної безпеки можна представити у такому вигляді:

1. Формування робочої групи.

2. Визначення глобальної цілі діяльності підприємства.

3. Виявлення резервів підвищення ефективності можливостей операційної діяльності і врахування зовнішніх небезпек.

4. Вибір елементів, які включатиме сама стратегія.

5. Визначення локальних цілей діяльності підприємства.

6. Тактичне планування і розроблення альтернативних варіантів тактичних дій.

7. Контроль за виконанням та результатами реалізації стратегії.

8. Оцінка ефективності стратегії економічної безпеки.

Таким чином, кожен з цих етапів є важливим і необхідним для розробки ефективної стратегії економічної безпеки підприємства, оскільки створює цілісний і добре продуманий план, який охоплює всі аспекти забезпечення безпеки підприємства.

2.2. Управління кадровим потенціалом в контексті стратегії безпеки організації

Розробка стратегії економічної безпеки підприємства є складним завданням, оскільки передбачає оптимальне використання всіх ресурсів підприємства, включаючи матеріальні, нематеріальні, трудові та фінансові [27, с. 39]. Цей аспект надзвичайно актуальний, особливо враховуючи сучасні реалії, коли стрімкий технологічний прогрес і зростання конкуренції визначають нові вимоги до підприємств.

Як справедливо відзначає С. Бортнік: «Нині саме кадри, а не технологія, обладнання чи фінансові ресурси є визначальним чинником успішності підприємства, вагомою детермінантою його стабільності та розвитку» [28, с. 333].

Аналогічна думка висвітлена також і у дослідженнях О. Гетьман та С. Царюка, які переконані, що «якщо в минулому конкурентна перевага однієї компанії перед іншою розглядалася переважно з технічного погляду, тобто з позиції наявності та ступеня використання новітніх технологій виробництва, обладнання, то зараз найважливішою конкурентною перевагою стає персонал компанії, який вирізняється високим рівнем професійних компетенцій» [29, с. 536].

Відтак кадровий потенціал – це один з ключових елементів формування стратегії економічної безпеки. Зокрема, як вже було досліджено раніше, забезпечення підприємства кадрами являє собою обов’язковий четвертий етап розробки стратегії. Зважаючи на це, надзвичайно важливими питаннями є, по-перше, підбір кваліфікованого персоналу та, по-друге, забезпечення можливості постійного підвищення фахового рівня працівників.

Отже, як зазначають О. Гетьман та С. Царюк, підбір персоналу являє собою важливий етап у системі управління персоналом, який охоплює методи, використовувані організаціями для забезпечення якнайкращого складу потенційної кваліфікованої робочої сили, кандидатів з якої вони зможуть за

необхідності найняти [29, с. 537]. З цього визначення випливає, що основною метою підбору кадрів є створення команди фахівців, здатних ефективно виконувати завдання підприємства та відповідати його стратегічним цілям.

Варто зауважити, що важливим аспектом вищезазначеного процесу є адаптованість методів підбору до конкретних вимог та специфіки організації. Так, підприємство може використовувати два види методів, а саме: традиційні та інноваційні.

Аналізуючи праці українських дослідників В. Приймака, В. Москальчук, Н. Кубіній та В. Варги, а також статтю, підготовлену редакційним колективом всесвітньої системи з пошуку зайнятості Indeed, ми визначили, що традиційними є, зокрема, такі методи, як: аналіз анкетних даних та резюме, центри оцінювання (тренінг-гри, у якій претендент знаходиться в ситуації, максимально наближеній до робочої обстановки), тестування, особиста чи групова співбесіда, аналіз рекомендацій та стажування [30, с. 110; 31, с. 171; 32].

Що стосується інноваційних, то найбільш відомими є, наприклад:

– хедхантінг – «виявлення та залучення в організацію сильних кандидатів, які самостійно не шукають перспективну роботу» [30, с. 110], тобто так зване «переманювання» конкретного спеціаліста;

– скринінг – «швидкий відбір претендентів виключно за формальними ознаками (освіта, вік, стать, приблизний досвід роботи, навички і уміння), що здійснюється самим підприємством» [30, с. 110; 31, с. 172];

– рекрутмент – «процес пошуку і відбору фахівців відповідно до потреб підприємства, тобто з урахуванням реальних особливостей робочого місця та ділових, особистісних якостей кандидата» [31, с. 172; 30, с. 110];

– цифровий рекрутинг – використання соціальних мереж для пошуку нових працівників [31, с. 172];

– краудсорсинг – «передача роботи не професіоналам, а низькооплачуваним або неоплачуваним любителям-професіоналам, які

отримують завдання зазвичай через мережу Інтернет та витрачають на її виконання свій вільний час» [30, с. 110].

Як справедливо зазнають Н. Кубіній та В. Варга, не всі роботодавці готові застосовувати інноваційні методи підбору персоналу, адже деякі з них потребують великих капіталовкладень [30, с. 110]. У таких випадках популярним залишається використання традиційних методів, які, хоча є менш ефективними та адаптованими до сучасних вимог ринку праці, однак все ж більш фінансово доступні.

Таким чином, кожне підприємство має самостійно визначати, як саме здійснювати підбір персоналу, враховуючи наявні ресурси та стратегічні цілі. У контексті розробки стратегії економічної безпеки це стає особливо важливим аспектом, оскільки саме підбір персоналу може бути ключовим фактором для створення стійкого кадрового потенціалу, необхідного для реалізації стратегії безпеки підприємства.

Що стосується забезпечення можливості постійного підвищення фахового рівня працівників, то цей процес передбачає організацію та проведення різноманітних заходів, зорієнтованих на повноцінне розкриття кадрового потенціалу підприємства, стимулювання особистісного зростання та розвитку кожного співробітника для того, щоб в подальшому вони зробили власний внесок у діяльність підприємства [33].

Питання професійного навчання працівників регулюється, зокрема, ст. 7 Закону України «Про професійний розвиток працівників», згідно з частиною першою якої «професійне навчання працівників здійснюється за денною, вечірньою (змінною), очно-заочною, дистанційною, екстернатною формою, з відривом і без відриву від виробництва та за індивідуальними навчальними планами» [34]. Разом з тим частиною другою вказаного Закону передбачено і те, що «професійне навчання працівників за робітничими професіями забезпечується шляхом: курсового навчання, що передбачає формування навчальних груп і здійснюється в навчальних класах (лабораторіях); індивідуального навчання, що передбачає навчання на робочому місці під

керівництвом кваліфікованих робітників – інструкторів виробничого навчання» [34]. З огляду на ці законодавчі норми можна зробити висновок, що до заходів підвищення фахового рівня співробітників можна віднести, приміром, підвищення кваліфікації працівників за рахунок підприємства, самостійне навчання працівників, міжвідомчу співпрацю, організацію стажувань, проведення конкурсів та олімпіад, нагородження та заохочення працівників для підтримання мотивації.

Оскільки головна мета розвитку персоналу полягає в забезпеченні підприємства висококваліфікованими кадрами, то при формуванні загальної та економічної стратегій безпеки підприємств варто також обов'язково розробити і стратегію розвитку персоналу. Залежно від глобальних та локальних цілей підприємства зазначена стратегія може передбачати здійснення:

– концентрованого розвитку, тобто спеціалізованого навчання та підтримки професійного розвитку конкретних груп співробітників на підприємстві;

– розвитку потенційних та нових працівників задля забезпечення їх адаптації до роботи підприємства;

– диверсифікованого розвитку персоналу – навчання та здобуття додаткової кваліфікації, переміщення персоналу, реалізація програми розвитку, яка спрямована на удосконалення комунікацій та формування ефективної команди;

– інтегрованого розвитку персоналу, а саме реалізація комплексного підходу до розвитку кадрів, використання спеціалізованих навчальних програм, створення умов для формування необхідної поведінки працівників підприємства;

– аналізу кадрових резервів, потреб підприємства та можливостей працівників [33].

Управління персоналом є важливою складовою забезпечення безпеки бізнесу та ефективного функціонування підприємства. Одним із ключових аспектів є впровадження посадових інструкцій, які допомагають чітко

визначити обов'язки співробітників, мінімізувати ризики та забезпечити дотримання встановлених стандартів. На прикладі підприємства ТОВ "Вінгалагро" розглянемо основні етапи та практичні аспекти впровадження цього процесу.

Посадові інструкції дозволяють:

- встановити чіткі обов'язки працівників, це сприяє уникненню дублювання функцій та зниженню конфліктів між підрозділами;

- забезпечити безпеку праці, інструкції містять інформацію про запобіжні заходи, що допомагають уникнути нещасних випадків на робочому місці;

- дотримуватися законодавства, документація відповідає вимогам нормативних актів, що регулюють трудові відносини.

- підвищити ефективність роботи, чітко визначені завдання допомагають працівникам зосереджуватися на пріоритетних аспектах своєї діяльності.

Практичний приклад: ТОВ "Вінгалагро", для розробки посадових інструкцій використовуються такі джерела: Інструкція з охорони праці для персоналу охорони; Пам'ятка охороннику для організації безпечної охорони об'єкта; Інструкція для водіїв та відвідувачів для контролю доступу на територію підприємства.

Етапи впровадження. Аналіз існуючих процесів. На першому етапі аналізуються функції кожного працівника, визначаються ризики та проблемні зони. Для цього створюється робоча група, до якої входять представники HR-відділу, керівництво і служба безпеки.

Розробка інструкцій. З урахуванням специфіки підприємства розробляються:

Інструкції для охоронників, які враховують безпеку об'єктів, організацію пропускного режиму та дії в екстрених ситуаціях.

Інструкції для водіїв та відвідувачів щодо правил в'їзду на територію та безпеки.

Затвердження документів. Посадові інструкції підписуються керівником підприємства, після чого стають обов'язковими до виконання.

Навчання персоналу. Усі співробітники проходять первинний інструктаж. Особливу увагу приділяють роз'ясненню пунктів, які безпосередньо впливають на безпеку.

Наприклад, охоронники повинні знати алгоритм дій під час виявлення пожежі, правила користування засобами сигналізації.

Впровадження в роботу. Інструкції передаються працівникам, їх зміст обговорюється на зборах або тренінгах.

Контроль виконання. Регулярно проводяться перевірки дотримання інструкцій, результати яких фіксуються у відповідних журналах.

Особливості використання інструкцій. Організація пропускного режиму. Інструкції регламентують порядок входу сторонніх осіб і в'їзду транспорту. Наприклад, водії повинні розташовувати транспорт у визначених місцях, дотримуватися обмеження швидкості.

Безпека праці охоронників.

Працівники зобов'язані: Контролювати територію за затвердженим маршрутом. Використовувати спеціальні засоби за встановленим регламентом

Дії в аварійних ситуаціях. Працівники ознайомлюються з алгоритмами дій під час пожежі, проникнення сторонніх осіб або інших інцидентів

Впровадження посадових інструкцій на ТОВ "Вінгалагро" сприяє підвищенню організованості та безпеки на підприємстві. Вони дозволяють зменшити ризики, пов'язані з людським фактором, забезпечити виконання законодавчих вимог і підвищити ефективність роботи персоналу. Регулярне оновлення цих документів відповідно до змін у законодавстві та внутрішніх потреб підприємства є запорукою їхньої актуальності та ефективності.

Значення посадових інструкцій для безпеки підприємства неможливо переоцінити. Вони є основою для забезпечення ефективного функціонування підприємства, мінімізації ризиків і захисту матеріальних, фінансових та

людських ресурсів. На основі аналізу вказаних інструкцій їх роль у забезпеченні безпеки можна охарактеризувати наступним чином:

1. Підвищення безпеки праці персоналу

Інструкції містять чіткі вимоги та правила, які спрямовані на захист здоров'я та життя працівників. Наприклад: інструкція з охорони праці регламентує дії працівників перед початком, під час та після роботи. Вона визначає, як уникати небезпечних зон, поводитися з електрообладнанням і забезпечувати безпеку пересування на території підприємства. Чітке дотримання цих правил допомагає мінімізувати нещасні випадки, спричинені людським фактором або недоліками організації.

2. Захист території та майна. Інструкція для охоронників детально описує організацію постів охорони, правила прийому та здачі змін, алгоритми патрулювання, що сприяє зменшенню ризиків проникнення сторонніх осіб, крадіжок та пошкодження майна. Завдяки впровадженню перепускного режиму забезпечується контроль за пересуванням працівників, відвідувачів і транспортних засобів, що дозволяє швидко реагувати на потенційні загрози.

3. Контроль доступу. Інструкція для водіїв і відвідувачів спрямована на забезпечення порядку під час в’їзду та перебування на території підприємства. Правила визначають: обмеження руху транспорту; контроль документів і вантажів. Це дозволяє уникнути перевищення допустимого навантаження на територію підприємства, запобігти аварійним ситуаціям через недотримання правил пожежної чи дорожньої безпеки.

4. Оперативне реагування на надзвичайні ситуації. В усіх інструкціях є пункти, присвячені діям у випадках пожеж, аварій, проникнення сторонніх осіб чи інших загроз. Чіткі алгоритми включають: виклик екстрених служб, організацію евакуації, застосування первинних засобів гасіння пожежі. Це забезпечує злагодженість дій персоналу, що критично важливо для мінімізації втрат у кризових ситуаціях.

5. Юридичний захист підприємства. Документальне оформлення посадових інструкцій є юридичною підставою для врегулювання спірних

ситуацій між роботодавцем та працівником. Наприклад:при порушенні працівником правил він може бути притягнутий до дисциплінарної або матеріальної відповідальності . Інструкції забезпечують дотримання норм законодавства у сфері охорони праці, що знижує ризики санкцій з боку контролюючих органів.

6. Профілактика та планування. Завдяки детальним описам можливих небезпек, таких як шкідливі виробничі фактори, несправності обладнання чи порушення правил поведінки, інструкції дозволяють проводити профілактичні заходи: технічне обслуговування обладнання та регулярний інструктаж персоналу.

7. Забезпечення психологічної безпеки. Чітко прописані правила створюють середовище, де працівники знають свої обов'язки та відповідальність, що знижує рівень стресу та покращує взаємодію між колегами. Наприклад, охоронник, який розуміє порядок дій у разі нападу чи крадіжки, може діяти впевненіше, не завдаючи шкоди собі та іншим.

Впровадження інструкцій на підприємстві є необхідною умовою для створення безпечного та контрольованого середовища. Інструкції, розроблені для ТОВ "Вінгалагро", забезпечують не лише фізичну, але й організаційну та правову безпеку підприємства. Вони служать дорожньою картою для працівників і допомагають зменшити вплив людського фактора на ризики. Регулярне оновлення цих документів та

Отже, підсумовуючи сказане, ми можемо зробити висновок, що керівництву важливо розглядати кожного працівника як цінний актив, який може зробити значний внесок у досягнення стратегічних цілей будь-якої організації. Відтак, враховуючи роль, яку відіграє кадровий потенціал у формуванні стратегії економічної безпеки, підприємства повинні приділяти особливу увагу управлінню персоналом та виробленню довгострокових планів розвитку кадрів, що враховуватимуть динаміку сучасного бізнес-середовища [35, с.49].

2.3. Роль логістичної стратегії у системі забезпечення економічної безпеки організації

Логістика є одним із найважливіших елементів економічної безпеки підприємства. Вона забезпечує ефективне управління матеріальними, інформаційними та фінансовими потоками, що дозволяє підприємству знижувати витрати на виробництво та реалізацію продукції, підвищувати якість продукції та послуг, збільшувати конкурентоспроможність на ринку та зменшувати ризики. Основою для ефективного управління логістичними процесами на підприємстві є розробка логістичної стратегії.

Як стверджують О. Вівчар, М. Зяйлик та Р. Горина, логістична стратегія у системі забезпечення економічної безпеки підприємства є «довгостроковим, якісно визначеним напрямком розвитку логістики, що стосується форм і засобів її реалізації у фірмі, міжфункціональній і міжорганізаційній координації й інтеграції, сформульоване вищим менеджментом компанії відповідно до корпоративних цілей та з метою підвищення рівня економічної безпеки підприємства» [36, с. 34].

Водночас Л. Шостак та В. Носалюк визначають логістичну стратегію як «одну з функціональних стратегій підприємства, що вирішує проблему завантаження виробничого асортименту на основі сформованого логістичними службами запасу замовлень, забезпечення високого рівня логістичного обслуговування, забезпечення мінімального акцептованого рівня загальних витрат у логістичному каналі, де визначаються центри втрат та розробляються вимоги до якості продукції» [37, с. 156].

Систематизувавши вищевикладені дефініції, кожна з яких є раціональною та обґрунтованою, ми дійшли висновку, що найбільш повно поняття логістичної стратегії можна визначити так:

Логістична стратегія – одна з основних стратегій підприємства, яка являє собою комплексний план розвитку логістики, що визначає цілі, завдання та принципи логістичної діяльності підприємства, а також шляхи їх досягнення.

Варто зауважити, що згадані у запропонованому нами визначенні цілі та завдання логістичної діяльності повинні бути обов'язково узгоджені з іншими локальними актами, а також при їх формуванні мають бути враховані й такі фактори, як: особливості логістичних процесів на конкретному підприємстві, його зовнішнє середовище, технічний рівень та можливості.

Відтак для того, щоб логістична стратегія була ефективною, її формування має здійснюватися одночасно або ж з урахуванням вже існуючої стратегії безпеки. Лише в комплексі вони здатні забезпечити економічну безпеку та суттєве зменшення загроз. Наприклад, якщо стратегія безпеки підприємства передбачає мінімізацію ризиків, пов'язаних з логістичними операціями, то логістична стратегія повинна бути спрямована на розробку та реалізацію заходів, які забезпечать зниження цих ризиків.

Отже, цілком раціональним є формування логістичної стратегії за певним чітко визначеним планом. Зокрема, С. Дуда та Л. Шостак, досліджуючи це питання, запропонували певний алгоритм, якого варто дотримуватися при розробці згаданої стратегії. Так, він складається із семи основних етапів, а саме:

– «виявлення узгодженості між корпоративною та логістичною стратегіями підприємства;

– проведення стратегічного аналізу логістичної діяльності підприємства;

– формування моделі логістичної стратегії;

– діагностика можливих альтернатив логістичної стратегії та сценарій їх можливої реалізації із передбаченням можливих наслідків;

– вибір оптимальної логістичної стратегії та її реалізація;

– контроль за реалізацією стратегії;

– оцінка результатів реалізації логістичної стратегії (за необхідності – внесення корективів та правок)» [38, с. 66-67].

Аналізуючи цей алгоритм, вважаємо, що доречно звернути увагу на його схожість із дослідженими раніше етапами розробки стратегії економічної безпеки підприємства. Обидва підходи визнають важливість систематичного та довгострокового планування, аналізу поточного стану, формулювання цілей та

визначення стратегічних кроків для досягнення успіху. Така аналогія може свідчити про те, що успішна логістична стратегія та стратегія економічної безпеки взаємодіють, створюючи цілісний план забезпечення стабільної роботи підприємства.

Проте, незважаючи на такий тісний зв'язок між досліджуваними стратегіями, С. Дуда та Л. Шостак цілком аргументовано, на нашу думку, зазначають, що тип логістичної стратегії, яку варто використовувати на підприємстві, не можна визначати лише в контексті стратегії безпеки. Ми переконані, що це пов'язано насамперед з тим, що вибір логістичної стратегії повинен враховувати специфічні потреби підприємства.

Отож науковці виокремлюють такі види логістичних стратегій:

– «тоща» стратегія, яка базується на принципах управління витратами, тобто виконання кожної операції з використання найменшої кількості ресурсів;

– динамічна стратегія, спрямована на забезпечення високої якості обслуговування споживачів шляхом швидкого реагування на зміни у зовнішніх умовах та корегування логістичних характеристик;

– стратегія, заснована на стратегічних союзах між постачальниками та замовниками, мета якої полягає у підвищенні ефективності ланцюга постачань за рахунок спільної роботи та отримання прибутку від довгострокової кооперації [38, с. 67].

Усе вищевикладене дозволяє нам сформулювати певні рекомендації, які доцільно взяти до уваги керівникам підприємств. Так, вважаємо, що при здійсненні вибору типу логістичної стратегії та при її розробці варто враховувати такі фактори, як: специфічні потреби підприємства (сфера діяльності, розмір підприємства, його географічне розташування, обсяги виробництва та реалізації продукції, вимоги споживачів), конкурентну ситуацію на ринку, стратегії конкурентів та інші зовнішні умови (економічну ситуацію в країні, політичні події та технологічні зміни). Впевнені, що дотримання цих рекомендацій дозволить гармонійно інтегрувати логістику у

загальну стратегічну концепцію підприємства, забезпечуючи його стійкість та конкурентоспроможність.

РОЗДІЛ 3 УПРАВЛІННЯ СТРАТЕГІЄЮ БЕЗПЕКИ У МОВАХ ОСОБЛИВИХ СТАНІВ: ВІТЧИЗНЯНИЙ І ЗАРУБІЖНИЙ ДОСВІД

3.1.Управління організацією та формування стратегії безпеки в умовах воєнного стану

Рівень безпеки діяльності суб'єктів господарювання є складною та багатогранною характеристикою, яка, за визначенням Р. Крамара, залежить від:

– рівня виконання співробітниками своїх обов'язків;

– рівня дотримання норм чинного законодавства;

– рівня правопорядку у державі та регіоні, де функціонує суб'єкт господарювання;

– своєчасного реагування на загрози, що виникають на шляху розвитку (загрози щодо кадрового, матеріального, фінансового та інформаційного забезпечення) [39, с. 5].

Усі ці фактори взаємодіють між собою, створюючи інтегровану стратегію безпеки. Відтак, якщо рівень виконання співробітниками своїх обов'язків залежить від кадрової політики, рівень правопорядку в регіоні – від конкретних зовнішніх обставин, непідвладних суб'єктам господарювання, своєчасне реагування на загрози – від якості логістичної стратегії та стратегії безпеки, то високий рівень дотримання норм чинного законодавства залежить насамперед від обізнаності керівництва та працівників про наявність тих чи інших нормативно-правових актів, які регулюють діяльність підприємств.

В цілому правові основи діяльності суб'єктів господарювання передбачені Господарським кодексом України (ГК України), Цивільним кодексом України (ЦК України), Кодексом законів про працю України (КЗпП України), Кодексом України про адміністративні правопорушення (КУпАП) та Кримінальним кодексом України (КК України). Хоча ці нормативно-правові акти і встановлюють загальні засади господарювання, визначають правовий статус учасників відповідних відносин, а також відповідальність за порушення чинних норм законодавства, однак не менш важливу роль відіграє і спеціальне

законодавство, яке безпосередньо регулює безпеку підприємств в Україні. Отож така нормативно-правова база складається з різних законів та підзаконних нормативно-правових актів, зокрема щодо: процедур легалізації (реєстрація суб'єкта господарювання, надання ліцензій, патентів, стандартизація і сертифікація діяльності) [39, с. 6], захисту прав суб'єктів господарювання (у ситуаціях регулювання цін та тарифів, порядку квотування, застосування лімітів та нормативів, регулювання антимонопольного становища) [39, с. 6-7], здійснення контролю діяльності підприємств (здійснення наглядів, перевірок, ревізій) органами державної влади [39, с. 7], охорони праці та запобігання аваріям та надзвичайним ситуаціям, захисту інформації, захисту навколишнього природного середовища.

Загалом перші три зазначені категорії, тобто процедури легалізації, контролю за діяльністю та захист прав суб'єктів господарювання, можна назвати основою безпеки підприємства у сфері законності здійснення діяльності. Відповідні питання регулюється такими законодавчими актами, як: Закони України «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань», «Про ліцензування видів господарської діяльності», «Про захист економічної конкуренції», «Про стандартизацію», «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», «Про засади державної регуляторної політики у сфері господарської діяльності», «Про дозвільну систему у сфері господарської діяльності» [39, с. 7].

Водночас серед основних законодавчих актів, що регулюють питання охорони праці та безпеки на робочому місці в Україні, ключове значення має Кодекс цивільного захисту України (КЦЗ України), який визначає загальні принципи та стратегії цивільного захисту населення, об'єктів господарювання та територій в умовах надзвичайних ситуацій [40]. Як справедливо зазначає О. Хитра, досліджуючи особливості діяльності ДСНС щодо реалізації державної політики у сфері цивільного захисту населення, саме у КЦЗ України

започатковано Єдину державну систему цивільного захисту та її складові [41, с. 215].

Не менш важливу роль відіграє і Закон України «Про охорону праці», спрямований на запобігання та зменшення травматизму і професійних захворювань працівників. Так, цей нормативний акт «визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних органів державної влади відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні» [42].

Разом з тим підзаконними нормативно-правовими актами у сфері охорони праці та безпеки на робочому місці є: Постанова Кабінету Міністрів України «Деякі питання ідентифікації об'єктів підвищеної небезпеки» [43] і накази Міністерства внутрішніх справ України «Про затвердження Правил пожежної безпеки в Україні» [44], Державного комітету України з нагляду за охороною праці «Про затвердження Типового положення про службу охорони праці» [45] та багато інших.

Що стосується екологічного законодавства, то його основною метою в цьому випадку є недопущення нанесення шкоди навколишньому природному середовищу в процесі здійснення підприємницької діяльності. Для цього в Україні діють норми, які встановлюють стандарти допустимого впливу на довкілля, визначають порядок отримання дозволів на здійснення спеціального природокористування, а також передбачають відповідальність за порушення встановлених правил. Усі ці та інші питання регулюються насамперед Законами України «Про охорону навколишнього природного середовища», «Про оцінку впливу на довкілля» та «Про управління відходами».

Відтак Закон України «Про охорону навколишнього природного середовища» визначає основні принципи державної політики у сфері охорони довкілля, встановлює права та обов'язки громадян, юридичних осіб у сфері

охорони довкілля та визначає порядок здійснення державного контролю за додержанням природоохоронного законодавства [46]. Водночас основним завдання Закону України «Про оцінку впливу на довкілля» є визначення порядку проведення оцінки впливу на довкілля планованої діяльності й встановлення вимог до ведення відповідної документації [47]. У останньому ж згаданому Законі «Про управління відходами» передусім закріплено правові та організаційні основи поводження з відходами та вимоги до збирання, транспортування, зберігання, переробки, утилізації і захоронення відходів [48].

Наявність усіх вищезазначених актів доводить, що дотримання екологічного законодавства є не лише «сучасним трендом управління комерційною діяльністю», як стверджують Н. Кривокульська, Ю. Богач і Ж. Крисько [49], а й обов'язком для всіх підприємств, що здійснюють свою діяльність на території України.

На відміну від вже згаданих сфер відносно новою можна вважати саме сферу правового регулювання захисту інформації. У зв'язку зі стрімким та безупинним розвитком технологій виникають нові унікальні виклики та загрози для безпеки даних підприємств, а тому проблема забезпечення кібербезпеки постала як перед юридичними та фізичними особами, так і перед законодавцями. Отже, ключовими актами, які регулюють відповідне коло питань є:

– Закон України «Про захист інформації в інформаційно-комунікаційних системах», який відповідно до ч. 1 ст. 1 «регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних» [50];

– Закон України «Про основні засади забезпечення кібербезпеки України», що «визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних

органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» [51];

– Закон України «Про захист персональних даних», дія якого «поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів» [52];

– Закон України «Про інформацію», який покликаний визначати загальні принципи та основи регулювання обігу інформації в Україні, а також встановлювати права та обов'язки учасників цього процесу, а саме фізичних осіб, юридичних осіб, об'єднань громадян та суб'єктів владних повноважень [53];

– Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року № 1229/99, – встановлює законодавчі вимоги та стандарти, яких повинні дотримуватися всі підприємства, що здійснюють обробку і зберігання важливої інформації [54].

Цей перелік не є повним, адже сфера захисту інформації наразі регулюється й іншими законами та підзаконними актами, однак саме вищезазначені вважаються базовими законодавчими актами, що визначають правила та стандарти збереження конфіденційності та безпеки даних.

Таким чином, підприємства зобов'язані дотримуватися усіх зазначених вимог з питань процедур легалізації, охорони праці, забезпечення недоторканості персональних даних та недопущення нанесення шкоди довкіллю. У разі порушення встановлених законодавством правил існує встановлений державою механізм юридичної відповідальності за відповідні дії.

Згідно зі ст. 44 Закону України «Про охорону праці», ст. 28 Закону України «Про захист персональних даних» та ст.ст. 68, 70 Закону України «Про охорону навколишнього природного середовища» за порушення законів та інших нормативно-правових актів про охорону праці, захист персональних даних і охорону навколишнього природного середовища винні особи

притягаються до дисциплінарної, адміністративної, матеріальної, кримінальної відповідальності згідно із законом [42; 46; 52]. Так, наприклад, адміністративна відповідальність за згадані правопорушення передбачена ст.ст. 41, 52-91^{6} і 188^{39} КУпАП [55], а кримінальна – ст. 182, 236-254, 271 КК України [56].

Аналізуючи дане питання, варто наголосити, що деякі з цих статей самі по собі не встановлюють конкретного переліку дій, за які особа понесе покарання. Зокрема, ст. 271 КК України є відсильною, тобто направляє до специфічних нормативно-правових актів, як то законодавчих чи локальних, що встановлені на конкретному підприємстві. Разом з тим кримінальній відповідальності за даною статтею підлягають виключно фізичні особи, а до юридичних осіб застосування заходів кримінально-правового характеру за заподіяння шкоди здоров'ю чи заподіяння смерті працівникам на підприємстві не передбачено [57, с. 155-156]. Тобто в даному випадку можна говорити про те, що відповідальність за вчинення правопорушення, передбаченого ст. 271 КК України, понесе не безпосередньо підприємство як юридична особа, а фізична особа, відповідальна за додержання правил безпеки. Підтвердженням цього є вироки Слов'янського міськрайонного суду Донецької області від 27.05.2019 року у справі № 243/4624/19 [58], Лозівського міськрайонного суду Харківської області від 28.01.2020 року у справі № 629/5515/19 [59] та Луцького міськрайонного суду Волинської області від 15.06.2020 року у справі № 161/6422/20 [60].

При цьому доречно також зауважити, що до адміністративної та кримінальної відповідальності підприємства можуть бути притягненні не лише за вищевказані правопорушення.

У цьому контексті вивчення та дотримання чинного законодавства є невід'ємною частиною стратегії безпеки підприємства, оскільки ретельний аналіз правових норм може допомогти підприємству, по-перше, уникнути вчинення тих чи інших протиправних діянь при здійсненні господарської діяльності, а, по-друге, захистити свої права в разі їх порушення іншими

суб’єктами: фізичними чи юридичними особами, органами державної влади та місцевого самоврядування.

24 лютого 2022 року Указом Президента України № 64/2022 введено воєнний стан в Україні. Це рішення було прийнято на підставі пропозиції Ради національної безпеки і оборони України, відповідно до п. 20 ч. 1 ст. 106 Конституції України, Закону України «Про правовий режим воєнного стану» у зв’язку з військовою агресією Російської Федерації проти України [61].

Такий крок дав можливість владі вжити додаткових заходів для забезпечення безпеки країни та її громадян. Зокрема, було запроваджено комендантську годину, обмежено пересування громадян, а також посилено контроль за діяльністю підприємств. Відтак воєнний стан вплинув на роботу підприємств усіх галузей економіки. Зокрема, у багатьох сферах спостерігалося зменшення попиту на продукцію та послуги, зростання витрат, порушення логістичних ланцюгів та збільшення ризиків.

Відповідно до дослідження Р. Майстро і О. Більовської від початку повномасштабного вторгнення країни-агресора в Україну було пошкоджено або зруйновано щонайменше більше 120 підприємств та заводів, 30 % підприємств взагалі припинили свою діяльність, а 45% частково призупинили робочий процес [10, с. 22].

Отож реалії сьогодення диктують нові умови, у яких має працювати сучасний бізнес, а тому доречно зазначити, що зараз особливо актуально для керівників підприємств формувати та змінювати вже наявні стратегії безпеки. Залежно від сфери діяльності, кожне підприємство має виокреми, які саме зміни зовнішнього середовища найбільш гостро впливають на його роботу. Наприклад, організації, які працюють в галузі постачання товарів та послуг, наразі найбільше потерпають від порушення логістичних ланцюгів у зв’язку з воєнними діями і для них найактуальнішим питанням є розробка стратегії безпеки, яка б передбачала заходи щодо забезпечення стабільної логістики. Водночас ІТ-компанії, що страждають через постійні кібератаки, мають

ретельно зосередитися на розробці стратегії безпеки, яка б передбачала заходи захисту від такого неправомірного втручання у свою роботу.

Проте, незважаючи на те, що підприємствам різних галузей необхідно розробляти стратегії безпеки, які відповідають їхнім конкретним потребам, існують деякі загальні елементи, що обов'язково потребують уваги з огляду на зміни, які відбулися через повномасштабне вторгнення. До таких складових, зокрема, належать: врахування змін на ринку праці, забезпечення безпеки працівників (при надзвичайних ситуаціях, оголошеннях повітряної тривоги тощо) та захист інформації від ворожих атак.

Говорячи про зміни на ринку праці, важливо зауважити, що війна в Україні спричинила високий рівень плинності кадрів, пов'язаний з евакуацією працівників, мобілізацією до лав Збройних Сил України та зміною пріоритетів у житті людей.

Вітчизняні науковці О. Вітковська та І. Панченко зазначають, що напруженість на ринку праці, яка відчувалася й раніше, зараз зросла мало не вдвічі, адже виник дисбаланс між попитом та пропозицією робочої сили. Так, нездатність підприємств працювати в зонах бойових дій призвела до серйозних труднощів у логістиці та обмежила можливість довгострокового планування, а збільшення випадків тимчасового працевлаштування без офіційного оформлення спричинило різке зростання тіньового сектору. І незважаючи на, здавалось би, позитивну тенденцію повернення бізнесу до роботи після 24 лютого 2024 року, у країні все одно залишається високий відсоток безробітних [13, с. 200].

Наукова праця згаданих авторів яскраво продемонструє, що динаміка вакансій та резюме пройшла три фази, у які спостерігалися значні зміни. У першу фазу, тобто період до 23 лютого 2022 року, пропозиція вакансій на ринку відповідала зворотному відклику у вигляді поданих резюме, тобто кількість пропозицій працевлаштування майже дорівнювала кількість охочих отримати роботу [13, с. 201].

Друга фаза, початок якої вчені пов’язують із першим днем повномасштабного вторгнення, є фазою невизначеності та стрімкої кризи. У цей період, відповідно до статистичних даних, відбулося завмирання бізнесу, стрімке падіння кількості поданих резюме та активних вакансій. Також із 24 лютого до 5 квітня 2022 року спостерігалася ситуація, коли кількість вакансій перевищувала кількість резюме щонайменше у 3,5 рази [13, с. 201].

Що стосується третьої фази, то вона вважається найдовшою: почалася з квітня 2022 року і триває досі. Цей період можна охарактеризувати як умовну адаптацію до нових реалій, що охоплює як і поступове відновлення роботи підприємств у безпечних регіонах, так і поступове повернення працездатного населення та актуалізацію програми підтримки. З огляду на дані дослідження О. Вітковської та І. Панченка, у третій фазі різко змінюється динаміка вакансій та резюме: на відміну від попередньої фази на цьому етапі кількість поданих резюме значно перевищує кількість активних вакансій [13, с. 201]. На нашу думку, це пов’язано з тим, що в період з 24 лютого до квітня 2022 року більшість підприємств зосередила усі можливі ресурси на адаптацію до нових умов, а в деяких випадках і на релокацію підприємств у регіони, де не ведуться активні бойові дії. Так, цілком очевидно, що організації були змушені зменшити витрати на пошук нових кадрів або ж і взагалі скоротити вже наявний персонал.

Отже, бачимо, що воєнний стан суттєво вплинув на сучасний ринок праці. Цей фактор має обов’язково враховуватися при формуванні стратегій безпеки, оскільки він вносить суттєві зміни у динаміку працевлаштування та вимагає переосмислення підходів до управління персоналом. Зокрема, підприємствам варто розробити стратегію безпеки таким чином, щоб при різкому зменшенні кількості резюме, як відбувалося на другій фазі у лютому-квітні 2022 року, не виникло дефіциту кадрів та відповідно простою.

Наприклад, в стратегії безпеки підприємства може бути розглянута, по-перше, здатність оптимізації робочих процесів шляхом переходу до дистанційного формату у разі нагальної потреби, по-друге, можливість

розширення географії пошуку працівників. Такі заходи можуть допомогти організаціям впоратися з дефіцитом кадрів у короткий термін та довгостроковій перспективі, адже передбачають можливість працевлаштування осіб з різних регіонів України, а також з інших країн. Оптимальним рішенням є також формування адаптивної стратегії безпеки, регулярний перегляд та оновлення якої не вимагатиме від підприємства залучення значних фінансових та інших ресурсів.

Як зазначалося раніше, наступним не менш важливим питанням, яке варто врахувати при формуванні стратегії безпеки підприємства, є забезпечення безпеки працівників при надзвичайних ситуаціях, оголошеннях повітряної тривоги тощо.

У зв'язку зі зростанням різноманітних ризиків, пов'язаних з природними катастрофами, техногенними аваріями та іншими небезпеками, підприємства повинні розробляти та впроваджувати ефективні заходи безпеки працівників. Це охоплює створення планів евакуації та проведення тренувань і навчань з персоналом щодо дій у надзвичайних ситуаціях. Зокрема, наявність спеціальних приміщень для укриття, систем оповіщення та координації в разі надзвичайних ситуацій може значно зменшити ризики для працівників та підвищити загальний рівень безпеки на підприємстві.

Так, план подолання надзвичайних ситуацій є важливим елементом програми з безпеки праці на підприємстві, оскільки його наявність говорить про небайдужість організації до питань безпеки працівників. Загальною метою такого документа є визначення процедури для усунення раптових або несподіваних ситуацій, а також запобігання летальним наслідкам і травмам співробітників, зменшення пошкодження будівель, інвентарю та обладнання, захисту навколишнього середовища і території громад та прискорення відновлення нормального функціонування [62].

Варто зазначити, що розробка плану дій при надзвичайних ситуаціях – це не просто важливий елемент стратегії безпеки, а й прямий обов'язок. Відповідно до ст. 130 КЦЗ України: «Для організації діяльності єдиної

державної системи цивільного захисту Кабінетом Міністрів України, Радою міністрів Автономної Республіки Крим, центральними органами виконавчої влади, місцевими державними адміністраціями, органами місцевого самоврядування, суб'єктами господарювання розробляються та затверджуються плани реагування на надзвичайні ситуації, локалізації і ліквідації аварій та їх наслідків на об'єктах підвищеної небезпеки, цивільного захисту на особливий період, основних заходів цивільного захисту України на рік, план проведення заходів з евакуації населення (працівників), матеріальних і культурних цінностей у разі загрози або виникнення надзвичайних ситуацій» [40].

Згідно із згаданою правовою нормою плани реагування на різні небезпеки розробляються на державному, місцевому рівнях та суб'єктами господарювання. Наразі на державному рівні чинним є План реагування на надзвичайні ситуації державного рівня, затверджений постановою Кабінету Міністрів України № 223 від 14 березня 2018 року [63]. Натомість план реагування на надзвичайні ситуації суб'єктами господарювання розробляється, якщо кількість персоналу є більшою за 50 осіб, та затверджується керівником відповідного підприємства [64].

При цьому кожне підприємство має враховувати і конкретні характеристики своєї діяльності та потенційні ризики, що можуть виникнути в надзвичайних обставинах. Важливо, щоб плани реагування були не лише ретельно розробленими, але й регулярно оновлювалися для врахування змін у ситуації. Оперативне та систематичне вдосконалення цих планів дозволить забезпечити швидку та ефективну реакцію на різноманітні загрози.

Наразі можна виокремити три основні види небезпек, які здатні загрожувати стабільній роботі підприємств: техногенні, природні та соціальні.

О. Штоляр зауважує, що прикладами техногенних небезпек є пожежі, вибухи, обвалення будівель, структурні несправності, розливи хімічно небезпечних речовин, ненавмисне вивільнення небезпечних речовин, навмисне вивільнення небезпечних речовин, вплив іонізувального випромінювання, втрата електричної потужності, втрата водопостачання та втрата зв'язку.

Водночас природними небезпеками вважаються повені, землетруси, штормовий вітер, снігові бурі, сильні перепади температури та пандемічні захворювання [62].

Усі техногенні та природні небезпеки, безумовно, загрожують фізичному стану об’єктів інфраструктури підприємств, безпеці працівників та можуть викликати значні економічні та соціальні втрати, однак у світлі сучасних геополітичних подій та ризиків, пов’язаних із збройною агресією Російської Федерації проти України, також важливо розглядати питання забезпечення безпеки працівників під час можливих надзвичайних ситуацій, пов’язаних із загальним безпековим станом в країні чи регіоні. Для цього підприємства повинні співпрацювати з відповідними органами та службами для розробки та впровадження ефективних заходів забезпечення безпеки працівників в умовах можливих обстрілів.

Зокрема, основною локальних планів дій під час сигналу «Повітряна тривога» може стати алгоритм поведінки в умовах надзвичайної ситуації воєнного характеру, розроблений Державною службою України з надзвичайних ситуацій [65]. Так, локальний план дій може включати в себе такі елементи, як: евакуаційні заходи, заходи безпеки (визначення можливих безпечних місць та організація контролю за доступом до укриття під час повітряної тривоги), заходи з інформування та комунікації і плани щодо швидкого відновлення роботи підприємства після закінчення надзвичайної ситуації.

У цьому аспекті не менш актуально згадати, що загрози для життя та здоров’я працівників, знищення чи пошкодження об’єктів інфраструктури підприємств, пов’язані з обстрілами України – це не єдині небезпеки, які чатують на вітчизняний бізнес. Не менш часто відбувають і кібератаки на інформаційні ресурси підприємств. Найбільш відомими є, наприклад, хакерська атака мережі Київстар 12 грудня 2023 року [66], DDoS-атаки на Monobank 12 грудня 2023 року і 21 січня 2024 року [67; 68], DDoS-атаки на ТОВ «ЦСК «Україна» 4 і 14 жовтня 2023 року [69; 70] та постійні атаки на сервери «Нової пошти» [71].

Такі кібератаки можуть викликати серйозні наслідки для підприємств, зокрема, порушення безпеки даних, переривання нормальної роботи і нанесення фінансових втрат. Тому, розробка стратегії безпеки повинна включати заходи захисту від інформаційних загроз та відновлення бізнес-процесів у разі їхнього порушення.

Таким чином, забезпечення безпеки підприємства в умовах наявності різних небезпек вимагає комплексного підходу та розробки стратегії безпеки, у якій було б передбачено не лише загальні принципи, але й конкретні алгоритми захисту кадрового потенціалу, матеріальних та інформаційних ресурсів від можливих загроз. Водночас необхідно враховувати специфіку кожного виду небезпеки та розробляти адаптивні заходи для їх протидії, спрямовані на мінімізацію можливих наслідків та забезпечення стійкості підприємства в умовах несприятливих обставин.

3.2. Ризики в управлінні організацією на прикладі ТОВ «Вінгалагро»

На підприємстві яке функціонує в сучасних умовах існує багато ризиків, що потребують аналізу, вироблення механізмів їх прогнозування, реагування тощо. Тому на ТОВ «Вінгалагро» автор зібрав аналітику щодо тих ризиків, що найбільш системно негативно впливають на діяльність і дійшов до висновку, що це відключення електроенергії.

У сучасних умовах електроенергія стала невід'ємною частиною функціонування підприємств, а тому її відсутність є серйозною загрозою для їхньої економічної безпеки. Це можна пояснити тим, що саме завдяки електричній енергії забезпечується нормальна робота виробничих ліній, технологічного устаткування та інфраструктури.

Причини її відключення можуть бути різноманітні: від технічних збоїв та природних катастроф до кібератак та терористичних актів. У кожній з вказаних ситуацій існують унікальні ризики та негативні наслідки для підприємств. Разом з тим найбільш гостро питання відсутності стабільного постачання електроенергії постало саме восени 2022 та взимку 2022-2023 років, коли через масовані обстріли безліч об'єктів критичної інфраструктури по всій Україні були пошкоджені або ж цілком знищені. Так, терористичні атаки на енергосистеми спричинили великі перебої у постачанні електроенергії, що суттєво підірвало економічну стабільність підприємств та національної економіки в цілому.

З матеріалів дослідження Л. Кримчак, зокрема, яскраво видно, що якщо до 2022 року вчені вважали ключовою загрозою безпеці промислових підприємств високу вартість енергоресурсів, то з початком повномасштабного вторгнення великим викликом для усіх суб'єктів господарювання, а особливо для промислових гігантів, саме відключення електроенергії стало прямою загрозою не лише економічній безпеці, а й взагалі їх функціонуванню [12, с. 59]. Це, на нашу думку, пов'язано передусім з тим, що зараз діяльність бізнесу все більше автоматизується, а тому відключення електроенергії

призводить до зупинки виробництва, а відтак до втрати прибутку і порушення ділових зобов'язань перед клієнтами, втрати даних, пошкодження обладнання тощо.

У період планових відключень електроенергії у листопаді 2022 року – лютому 2023 року більшість підприємств не були готові до подібних труднощів, проте намагаючись побороти їх, знайшли можливі вирішення ситуації шляхом використання потужних промислових генераторів, переходу на нічний режим роботи, а подекуди і скорочення виробництва [12, с. 59]. Так, компанія IDS Ukraine («Моршинська», «Миргородська») в умовах віялових відключень електроенергії перейшла від подобового планування роботи підприємств на планування з огляду наявності ресурсів, а супермаркети «Сільпо» працювали з автономним живленням [72]. Згадані заходи хоча і дозволили підтримувати нормальну роботу підприємств, виробничих ліній, зберігати функціональність технологічного устаткування, однак не були доступні всім, приміром, через дорогу вартість придбання та обслуговування (якщо говорити про генератори великої потужності). З огляду на це, середній та малий бізнес намагалися подолати тимчасові труднощі менш витратними методами, які однак не були надто дієвими, про що свідчать результати опитування «Дія.Бізнес» щодо стану та потреб бізнесу в умовах війни в листопаді 2022 року, згідно з яких «31,7% підприємств повністю або майже повністю припинили роботу, а 48% – заявили, що через перебої з електроживленням обороти знизилися на 20% і більше» [73].

Отож незалежно від того, як підприємства пристосовувалися до нових умов роботи, як справедливо стверджує керівниця департаменту комунікацій Європейської бізнес-асоціації О. Миронько: «Немає індустрії, про яку можна було б сказати, що її не зачепила ситуація з відімкненням світла» [74]. Також, за словами експертки, «підрахувати збитки бізнесу через відключення електроенергії важко. Так, наприклад, одна з великих торговельних мереж порахувала, що за один день простою магазину вони втрачають близько 10 мільйонів гривень» [74].

Відтак досвід роботи суб'єктів господарювання 2022 року показав, що відключення електроенергії є серйозною загрозою для економічної безпеки підприємств. У той період український бізнес не був повною мірою готовий до схожих труднощів, внаслідок чого було понесено значні фінансові збитки. Задля уникнення подібних сценаріїв у майбутньому доцільним є перегляд стратегії безпеки підприємств з урахуванням нових можливих загроз.

Зокрема, вітчизняні вчені О. Мінц і Г. Дорошкевич пропонують три сценарії, реалізація яких здатна зменшити негативний вплив відсутності електропостачання на діяльність підприємств.

Перший сценарій полягає в тому, аби підприємства за необхідності використовували бензиновий чи дизельний генератори. Суттєвим недоліком такого альтернативного джерела електричного живлення є вартість його денної експлуатації, яка при ціні 1 літру бензину 50 гривень варіюється в межах 300 гривень. При цьому безспірною перевагою використання генераторів є, по-перше, їх вартість, яка в середньому складає 20000 гривень і, по-друге, невеликий термін окупності – орієнтовно 21 день [11, с. 64-65].

Другим сценарієм, який запропонували та дослідили О. Мінц і Г. Дорошкевич, є використання систем живлення на основі сонячної енергії. Цей варіант заміни електроенергії вважається найдорожчим і здатен окупитися лише через 92 дні, але разом з тим є екологічним, гарантує підприємству повну автономність, а також практично не несе за собою витрат на подальше утримання протягом всього терміну служби (до 10 років) [11, с. 64-67].

Тим часом третім сценарієм є сценарій використання підприємством акумуляторної системи живлення із підзарядкою від мережі. Таке альтернативне джерело електричного живлення здатне забезпечити функціонування основних приборів, переважно тих, які не споживають надто багато електроенергії, але потребує періодичної підзарядки, що може призвести до виникнення проблем у забезпеченні електрикою в період екстрених відключень, коли відсутність електропостачання триватиме довше, аніж можна перебачити. Термін окупності акумуляторної системи живлення із підзарядкою

від мережі складає в середньому 32 дні, якщо враховувати, що ціна самої системи – 80000 гривень, а вартість денної експлуатації – 1 гривня 44 копійки [11, с. 65].

У період енергетичного колапсу у 2022 році більшість підприємств, як вже згадувалося раніше, обрали для себе все ж перший сценарій – використання автономних генераторів. Однак, погоджуючись із думкою О. Мінца і Г. Дорошкевич, ми також вважаємо, що на більш тривалий термін перспективнішим є все ж використання саме систем живлення на основі сонячної енергії, що здатні забезпечити і стабільну роботу, і більш екологічне ведення бізнесу [11, с. 67].

Отже, підсумовуючи сказане, зауважимо, що в умовах повної невизначеності, враховуючи наявність ризиків відключення електроенергії у майбутньому через терористичні акти Російської Федерації, підприємствам необхідно переглянути свою стратегію безпеки таким чином, щоб у оновленій стратегії передбачити:

– можливість забезпечення резервного джерела електропостачання;

– обов’язкову розробку плану дій на випадок відключення електроенергії, що включатиме порядок реагування на планові та позапланові відключення, алгоритм забезпечення безпеки працівників та процедуру відновлення роботи виробництва;

– організацію навчання працівників з питань безпеки в умовах відключення електроенергії задля мінімізації ризиків для себе та підприємства.

3.3. Впровадження зарубіжного досвіду щодо стратегічного управління безпекою організацій

Одним із можливих напрямків вдосконалення стратегічного управління безпекою українських підприємств є вивчення та імплементація зарубіжного досвіду в цій сфері.

Переймаючи кращі практики та стратегії з інших країн, вітчизняні підприємства можуть збагатити свій підхід до забезпечення безпеки, зокрема, пристосувати свої методики до глобальних тенденцій і вимог, підвищити конкурентоспроможність та зменшити ризики. Так, імплементація світового досвіду в стратегічному управлінні безпекою може стати ефективним кроком для підвищення стійкості та адаптивності українських підприємств у сучасних умовах глобальної нестабільності.

Як доречно відзначає О. Продіус, «для політики розвинутих країн характерна розробка стратегічних планових документів щодо зміцнення безпеки підприємств та країни в цілому» [75, с. 79]. Зокрема, у багатьох державах наразі стратегічне планування безпекою суб'єктів господарювання здійснюється як на мікрорівні, тобто безпосередньо на тому чи іншому підприємстві, так і на макрорівні (шляхом впровадження державних заходів забезпечення безпеки підприємств).

Досліджуючи світовий досвід у забезпеченні економічної безпеки підприємств, А. Милка та Л. Артеменко визначили, що більшість компаній будують свою діяльність на основі певних концепцій, які, як правило, ґрунтуються на традиційних принципах підприємництва та мають тісний зв'язок із країною, де було засновано ту чи іншу організацію. З огляду на це вчені виділили дві широко поширені стратегії управління та забезпечення сталого розвитку підприємства – «американську» (США, Канада та країни ЄС) та «японську» (Японія, Китай) [76, с. 48].

Що стосується «американської» стратегії, то для неї характерним є закритість системи забезпечення безпеки підприємств і дотримання таких принципів, як: зниження витрат за допомогою виявлення внутрішніх ризиків, раціональна організація виробництва, ефективне використання всіх ресурсів і підвищення продуктивності праці співробітників [76, с. 48].

Назва першої концепції дає чітко та безпомилково зрозуміти, що при вивченні цього підходу до управління безпекою підприємств варто насамперед дослідити досвід Сполучених Штатів Америки, де діє «широкомасштабна система державної підтримки безпеки бізнесу» [75, с. 80].

Відтак варто зауважити, що на макрорівні держава забезпечує збереження секретної інформації на базі жорстких стандартів, вимог і процедур по захисту цінної науково-технічної, технологічної та комерційної інформації приватного сектора. Водночас на мікрорівні характерними особливостями є:

– використання програм профілактики і боротьби з економічними злочинами, які реалізовуються за допомогою взаємодії правоохоронних органів країни з державними та приватними установами охоронних і детективних бюро;

– тенденція безконфліктного вирішення проблем у сфері безпеки;

– призначення особи, відповідальної за вирішення питань безпеки (якщо фірма має місячний дохід понад 10 тис. доларів, а штат фірми перевищує три людини);

– проведення для майбутніх співробітників служби безпеки підприємств 8-годинних тренінгів до початку виконання своїх обов’язків і 40-годинних тренінгів протягом 9 перших днів роботи;

– поділ конфіденційної інформації підприємств на блоки, кожному з яких присвоюється свій код, та розробка карток-приписів для працівників з переліком тих кодів, які необхідні для нормального виконання посадових обов’язків [75, с. 80].

Ми вважаємо, що підхід Сполучених Штатів Америки до забезпечення безпеки бізнесу є ретельним та високоорганізованим. Так, реалізація

широкомасштабної системи підтримки безпеки бізнесу на різних рівнях – від національного до мікрорівня підприємства – демонструє відповідальне ставлення до управління ризиками та свідчить про зацікавленість держави і бізнесу у стабільності економічного середовища.

Отож не дивно, що в країнах Європейського Союзу більш поширеною стала саме «американська» стратегія. Зокрема, у Німеччині, як у країні-представниці саме цієї концепції, також можна побачити організований підхід до управління безпекою підприємств. Зокрема, на макрорівні забезпечення безпеки представлено, по-перше, чинним законодавством, приміром, Законами «Про заборону обмежень конкуренції» від 19 жовтня 1992 року і «Про заборону недобросовісної конкуренції» від 7 липня 1909 року (зараз діє у редакції 2008 року) [77, с. 143] та, по-друге, створеними урядом національними спецслужбами для контролю за ситуацією на економічно важливих об’єктах країни. Тим часом на мікрорівні німецькі підприємства самостійно формують певні контрольно-розвідувальні підрозділи, які уповноважені виконувати функцію забезпечення безпеки фірми, її керівництва, окремих працівників і клієнтів [75, с. 80]. Зазначений досвід демонструє, що для Німеччини найбільш характерною є взаємодія державних і приватних структур для забезпечення повноцінної безпеки бізнесу.

Аналогічною є і система забезпечення безпеки підприємств Франції. У цій країні державні органи також співпрацюють з приватними агентствами, таким чином забезпечуючи високий рівень захисту. Однак на мікрорівні стратегії більшості французьких підприємств, на нашу думку, є більш продуманими, ніж вже згадані німецькі, адже вони передбачають, що основна відповідальність за перевірку, відбір, прийняття на роботу працівників, збирання відомостей про родинні, дружні та інші зв’язки персоналу та контроль за їх звільненим здійснюється переважно виключно спеціалістами службами безпеки підприємства [75, с. 80]. Такий підхід гарантує як впевненість підприємства у своїх кадрах, так і забезпечення належного рівня збереження комерційних таємниць та конфіденційних даних співробітників.

Отже, проаналізований досвід Сполучених Штатів Америки, Німеччини та Франції яскраво демонструє стабільність «американської» концепції протягом тривалого часу. Водночас ще одним доказом, який доводять, що ця стратегія є збалансованою та дієвою, є її використання такими відомими та успішними компаніями, як: мережею магазинів роздрібної торгівлі Target (шостий найбільший ретейлер у США), найбільшою у світі мережею оптової та роздрібної торгівлі Walmart, торговою мережею з продажу обладнання для ремонту та будматеріалів HomeDepot, американською мережею супермаркетів Kroger (другий найбільший роздрібний продавець у США після Walmart), американською компанією, яка управляє кількома міжнародними мережами роздрібної торгівлі, Sears [76, с. 48].

Проаналізувавши особливості «американського» підходу до управління та забезпечення сталого розвитку підприємств, варто дослідити і «японський» підхід. Відтак його сутність полягає в тому, що ідеальне підприємство не повинне мати жодної структури, навіть офіційної. При цьому управління безпекою розглядається спеціалістами як засіб досягнення максимальної гармонійності та мобільності підприємства у сучасному динамічному світі [76, с. 49].

Характерною рисою «японської» стратегії є і система забезпечення кадрового потенціалу. Зокрема, на підприємствах, які при здійсненні своєї діяльності дотримуються цієї концепції, діє особлива система довічного найму та просування працівників залежно від стажу роботи та віку. Основною перевагою такої організації процесу формування та управління кадровим складом, на думку А. Милки та Л. Артеменко, є високий рівень лояльності персоналу та зниження операційних ризиків (людського фактору) [76, с. 49].

Яскравим прикладом держави, де більшість підприємств дотримується саме «японської» концепції, цілком передбачувано є Японія. Для цієї країни, як зазначає вітчизняна дослідниця О. Продіус, на макрорівні усталеною є практика врахування державою інтересів бізнесу, проведення економічної розвідки, заснованої на ефективному розподілі ролей між великим числом організацій

орієнтованих на експорт, та підтримки державними органами узгоджених дій між усіма суб'єктами ринку, що дозволяє зберігати високий рівень економічної безпеки [75, с. 80].

На мікрорівні задля забезпечення безпеки підприємств у Японії застосовують такі підходи:

по-перше, на департаменти кадрів, які наявні у кожній фірмі, покладаються функції контролю за неухильним дотриманням режиму секретності, що ґрунтується на кодексі поведінки службовців;

по-друге, забороняється передача інформації, що містить комерційну таємницю, стороннім особам та укладання угод, які можуть підірвати довіру до компанії з боку клієнтів;

по-третє, суворо контролюється робота за сумісництвом;

по-четверте, забороняється навмисне нанесення підприємствам економічних збитків;

по-п'яте, працівникам забороняється давати і отримувати хабарі [75, с. 80].

І хоча дотримання всіх цих правил є обов'язковим, варто зазначити, що виходячи зі своїх традицій, японські підприємства виховують у співробітників почуття патерналізму, а тому не встановлюють відповідальності за розголошення комерційної таємниці [75, с. 80]. Відтак основним завдання керівництва підприємств у Японії є попередження настання потенційних небезпек.

Таким чином, проаналізувавши досвід Японії, можна дійсно побачити підтвердження слів А. Милки та Л. Артеменко , що за «японською» концепцією визначальним фактором при розробці стратегій та прийняття управлінських рішень є саме поліпшення роботи всієї виробничої системи як цілісності [76, с. 49].

Що стосується ефективності такого підходу, то в Японії він, на нашу думку, виявився дуже успішним з огляду на те, які компанії застосовують його у своїй діяльності, а саме це: найбільша японська автомобілебудівна

корпорація, що також надає фінансові послуги і має кілька додаткових напрямів у бізнесі, Toyota Motor Corporation, велика японська машинобудівна корпорація й один із найбільших у світі виробників побутової техніки і електронних товарів Panasonic Corporation, велика транснаціональна корпорація Toshiba Corporation та японська корпорація, виробник електроніки й IT-компанія Fujitsu Limited [76, с. 49].

Отже, можна зробити висновок, шо як «американська», так і «японська» стратегії мають свої особливості, врахування яких може встати корисним для України. Зокрема, на макрорівні доцільним було б забезпечення дієвого механізму державної підтримки бізнесу. Водночас на мікрорівні ми пропонуємо керівникам підприємств впровадити такі заходи:

1. Призначення особи або створення штатної структури, відповідальної за вирішення питань безпеки;

2. Проведення навчання (тренінгів) для майбутніх працівників для їх ознайомлення з основними правилами забезпечення безпеки підприємства;

3. Здійснення поділу конфіденційної інформації підприємств на блоки і допуск до них (в разі необхідності) лише через коди доступу;

4. Організація Контролю роботи працівників за сумісництвом (для недопущення конфлікту інтересів і витоку даних).

Так, врахування вказаних пропозицій допоможе підприємствам покращити свою політику безпеки та розробити дієву стратегію безпеки.

З огляду на те, що ми вже визначили загальні риси світового досвіду щодо стратегічного управління безпекою підприємств, вважаємо, що показовим буде також аналіз та порівняння стратегій безпеки конкретних зарубіжних підприємств.

Для проведення цього дослідження ми вибрали декілька іноземних стратегій безпеки, а саме: стратегії безпеки приватної охоронної служби Private Security Authority, яка надає послуги з охорони майна та людей, некомерційної організації Warren Community Food Security, що бореться з голодом та продовольчою небезпекою, поштової та логістичної компанії DHL Group та

державної програми, спрямованої на забезпечення безпеки жителів штату Міннесота. Вибір саме цих стратегій був обумовлений тим, що вони представляють різні галузі, що відповідно дозволяє провести більш ґрунтовний аналіз.

Отже, першою досліджуваною нами стратегією є стратегічний план Private Security Authority (Приватної служби охорони) на 2023-2025 роки. Структура цього плану складається з п’яти основних елементів: передмови, детального опису повноважень, дослідження зовнішнього середовища, визначення місії та цілей, а також визначення порядку реалізації та кінцевого звітування щодо результатів роботи [78, с. 2].

Так, передмова і перший розділ «Повноваження» висвітлюють загальну інформацію про охоронну службу «Private Security Authority» та опис плану роботи підприємства упродовж наступних трьох років [78, с. 3-5]. Тим часом наступний ключовий елемент стратегічного плану – «Аналіз зовнішнього середовища» – розглядає фактори, які можуть впливати на діяльність Приватної служби охорони. Цей розділ охоплює оцінку економічного, політичного, соціокультурного та технологічного контексту, врахування якої допоможе підприємству в майбутньому адекватно реагувати на зміни у зовнішньому середовищі та визначати стратегічні переваги [78, с. 7-8]. Формулювання місії та цілей є четвертим етапом стратегічного плану Private Security Authority. У цьому розділі, зокрема, конкретизуються основні завдання та цілі, які підприємство прагне досягти протягом 2023-2025 років [78, с. 11-15]. Такий підхід, зі свого боку, визначає напрямки розвитку та створює основу для подальших стратегічних рішень. І завершальний елемент стратегічного плану – розділ четвертий «Визначення порядку впровадження та звітування про результати роботи» – розглядає конкретні дії та кроки, які планується вжити для впровадження стратегії. Відтак розділ визначає терміни, відповідальних за виконання завдань осіб та механізми моніторингу прогресу [78, с. 11-15].

Варто зауважити і на тому, що додатками до цього стратегічного плану виступають аналіз секторів, ліцензованих службою станом на вересень 2022

року та витяги з законодавчих положень, що регулюються сферу діяльності цього підприємства [78, с. 18-20]. Зазначені елементи також відіграють вагоме значення в підготовці та виконанні стратегічного плану цієї приватної служби охорони, адже не лише створюють фундамент та надають підтримку плану, але й визначають рамки, в яких підприємство повинно оптимізувати свою стратегію, щоб ефективно відповідати на виклики і можливості ринку охоронних послуг.

На нашу думку, стратегія Private Security Authority є передусім саме стратегією економічної безпеки, оскільки з її змісту яскраво видно, що основна мета плану – забезпечення економічної стійкості та стабільного прибутку підприємства. Така ж ситуація спостерігається і зі стратегіями безпеки організації Warren Community Food Security та компанії DHL Group.

Отож перша складається з таких елементів, як: вступ, передмова (історія створення), оцінка діяльності, результати роботи та рекомендації [79, с. 1-23]. Очевидно, що структура стратегії Private Security Authority суттєво відрізняється від структури стратегії Warren Community Food Security. Так, остання не містить ні чіткого визначення майбутніх цілей, ні детального аналізу зовнішнього середовища. Однак слід зауважити і на перевагах стратегії Warren Community Food Security, які полягають в тому, що її розробники ретельно проаналізували рівень бідності у регіоні, спроможність населення забезпечити себе необхідним обсягом та асортиментом продуктів харчування, середню наявність продуктових товарів у мікрорайонах та багато інших питань, що демонструє наявність у стратегії глибокого розуміння соціально-економічної ситуації у Воррені.

Що стосується стратегії DHL Group, то її теж доречно назвати саме стратегією економічної безпеки. На противагу Private Security Authority та Warren Community Food Security, стратегічний план поштової та логістичної компанії DHL є доволі коротким і складається переважно з визначення основної тріади – мети, бачення та цінностей. І хоча лише цих компонентів недостатньо, щоб сформувати ефективну стратегію, однак і вони розкривають

такі важливі елементи безпеки, як: якісний відбір працівників, вибір постачальників та інвестицію вибору клієнта (клієнтоорієнтованість). Таким чином, відповідно до інформації на офіційному сайті підприємства, «Стратегії 2025 – Досконалість у цифровому світі» закладає основу для продовження траєкторії успішного зростання провідної світової логістичної компанії DHL Group [80].

Водночас найбільш відмінним від усіх проаналізованих можна назвати саме стратегічний план безпеки підприємства (Enterprise Security Strategic Plan), розроблений Членами Ради інформаційної безпеки та Офісом безпеки підприємства (Office of Enterprise Technology – Enterprise Security Office). Особливість цієї стратегії полягає у тому, що вона є першим стратегічним планом безпеки підприємства для штату Міннесота, який визначив пріоритети для управління, контролю та захисту інформаційних активів [81, с. 2].

Традиційно структура цієї стратегії, як і більшості інших, складається з вступу, у якому визначаються основні стейтхолдери, план навігації і склад управлінських органів, та розділів, присвячених формуванню місії і базових цінностей програми безпеки, опису очікуваних стратегічних результатів і ключових ініціатив [81, с. 1]. Однак, навіть попри наявність звичайної структури, стратегія штату Міннесота на 2009-2013 роки є надзвичайно актуальною, адже демонструє, що безпека підприємств – це сфера відповідальності не лише бізнесу, а й держави.

Якщо порівняти складові, які ми, на основі праці Л. Лаврентьєвої, визначили основними при розробці стратегії безпеки підприємства (аналіз глобальної цілі, резервів підвищення ефективності діяльності, зовнішніх небезпек, локальних цілей, тактичного планування, контролю за виконанням та результатами реалізації, надання оцінки ефективності та інші конкретні елементи, які стратегія залежно від виду діяльності має містити) з елементами стратегій безпеки підприємств штату Міннесота, приватної охоронної служби Private Security Authority, некомерційної організації Warren Community Food Security та поштової і логістичної компанії DHL Group, то можна спостерігати,

що в загальному як у вітчизняній науці, так і у зарубіжній практиці базові елементи ефективної стратегії безпеки є незмінними.

А відтак в Україні доцільним було б запозичення практики розробки загальних стратегічних планів безпеки підприємств на загальнодержавному та обласному рівнях, які б частково стали основною для стратегій безпеки окремих суб'єктів господарювання.

Таким чином, зарубіжний досвід у сфері стратегічного управління безпекою підприємств є цінним джерелом знань та інформації. Він може допомогти українським підприємствам як взяти на озброєння передові методи й інструменти управління ризиками, забезпечення безпеки, та адаптації до змін у глобальному економічному середовищі, так і загалом розробити ефективні стратегії безпеки, які відповідатимуть їхнім конкретним потребам і вимогам. Проте важливо враховувати, що кожна країна має свої особливості, а тому будь-який зарубіжний досвід перед імплементацією слід адаптувати до внутрішніх реалій та специфіки українського бізнес-середовища.

ВИСНОВКИ

На сьогодні стратегія безпеки підприємства є ключовим елементом ведення ефективної діяльності бізнесу. Проте під зазначеним поняттям розуміється не лише статичний документ, а «живий» інструмент, який повинен адаптуватися до змін у економічному середовищі. Відтак з огляду на динамічність сучасного світу, актуальність вивчення питання стратегічного управління підприємством й зумовлює підвищену зацікавленість вчених і практиків до цієї теми.

Отже, виходячи з поставлених завдань, при здійсненні цього дослідження ми:

– визначили, що дослідження особливостей формування стратегії безпеки підприємства в сучасних умовах є критично важливим напрямом, який має практичне значення для сучасного бізнесу, особливо з огляду на появу нових ризиків ведення підприємницької діяльності;

– дослідили теоретичні основи формування стратегії безпеки підприємства та з'ясували, що безпека охоплює багато різноманітних факторів, однак при цьому в вітчизняній науковій літературі прийнято ототожнювати терміни «стратегія безпеки підприємства» та «стратегія економічної безпеки підприємства», адже саме економічні інтереси є основою існування та розвитку будь-якого суб'єкта господарювання;

– на основі праць вітчизняних та зарубіжних вчених виокремили основні принципи формування стратегії безпеки підприємства, зокрема: законність, системність, адаптивність, раціональність, доцільність, стратегічна орієнтація, скоординованість, плановість, конфіденційність і захист даних та принцип проведення контролю (аудиту, моніторингу). При цьому виявили, що усі вищезазначені принципи є взаємопов'язаними та доповнюють один одного, а їх дотримання дозволяє забезпечити формування ефективної стратегії безпеки підприємства, яка в подальшому забезпечить стійкість, конкурентоспроможність та успішний розвиток організації;

– проаналізували різні класифікації стратегій безпеки підприємств і дійшли висновку, що всі вони, по-перше, розглядають загальну стратегію безпеки та стратегію економічної безпеки як багатогранні та складні поняття та, по-друге, вказують на те, що вибір стратегії безпеки має залежати від особливостей, притаманних тому чи іншому підприємству.

– виокремили вісім етапів розробки стратегії економічної безпеки, а саме: формування робочої групи; визначення глобальної цілі діяльності підприємства; виявлення резервів підвищення ефективності можливостей операційної діяльності і врахування зовнішніх небезпек; вибір елементів, які включатиме сама стратегія; визначення локальних цілей діяльності підприємства; тактичне планування і розроблення альтернативних варіантів тактичних дій; контроль за виконанням та результатами реалізації стратегії; оцінка ефективності стратегії економічної безпеки.

– проаналізували значення кадрового потенціалу як елемента формування стратегії економічної безпеки підприємства, а відтак зробили висновок, що суб’єкти господарювання мають приділяти особливу увагу управлінню персоналом та виробленню довгострокових планів розвитку кадрів, що враховуватимуть динаміку сучасного бізнес-середовища;

– охарактеризували роль логістичної стратегії у системі забезпечення економічної безпеки та розробили рекомендації для керівників підприємств щодо того, як ефективно інтегрувати логістичну стратегію у загальну стратегічну концепцію підприємства;

– окреслили основні риси нормативно-правового забезпечення безпеки підприємств в Україні та дослідили основні законодавчі акти, що регулюють зазначену сферу, зокрема: Кодекс цивільного захисту України, Кримінальний кодекс України, Кодекс України про адміністративні правопорушення, Закони України «Про охорону праці», «Про охорону навколишнього природного середовища», «Про оцінку впливу на довкілля», «Про управління відходами», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних

даних» і «Про інформацію», постанову Кабінету Міністрів України «Деякі питання ідентифікації об'єктів підвищеної небезпеки», укази Президента України «Про Положення про технічний захист інформації в Україні», «Про введення воєнного стану в Україні» та інші;

– визначили вплив воєнного стану на роботу підприємства і розробку його стратегії безпеки, а також сформували пропозиції щодо перегляду стратегій безпеки таким чином, щоб у оновлених варіантах передбачити: можливість забезпечення резервного джерела електропостачання; обов'язкову розробку плану дій на випадок відключення електроенергії, що включатиме порядок реагування на планові та позапланові відключення, алгоритм забезпечення безпеки працівників та процедуру відновлення роботи виробництва; організацію навчання працівників з питань безпеки в умовах відключення електроенергії задля мінімізації ризиків для себе та підприємства.

– у процесі дослідження основних елементів зарубіжного досвіду щодо стратегічного управління безпекою підприємств охарактеризували основні світові практики, які варто впровадити в Україні, а саме з'ясували, що на макрорівні доцільним було б забезпечення дієвого механізму державної підтримки бізнесу, а на мікрорівні запропонували імплементувати такі заходи: призначення особи або створення штатної структури, відповідальної за вирішення питань безпеки; проведення навчання (тренінгів) для майбутніх працівників для їх ознайомлення з основними правилами забезпечення безпеки підприємства; здійснення поділу конфіденційної інформації підприємств на блоки і допуск до них (в разі необхідності) лише через коди доступу; організація контролю роботи працівників за сумісництвом (для недопущення конфлікту інтересів і витоку даних);

– проаналізували стратегії безпеки охоронної служби Private Security Authority, некомерційної організації Warren Community Food Security, поштової та логістичної компанії DHL Group та державної програми, спрямованої на забезпечення безпеки жителів штату Міннесота, а відтак визначили, що в Україні доречним було б запозичення практики розробки загальних

стратегічних планів безпеки підприємств на загальнодержавному та обласному рівнях, які б частково стали основною для стратегій безпеки окремих суб'єктів господарювання.

Таким чином, ми досягли мети роботи: здійснили глибинне дослідження особливостей формування стратегії безпеки підприємства в сучасних умовах, а також напрацювали рекомендації щодо розробки та ефективної реалізації таких стратегій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сабецька Т.І. Особливості формування організаційно-економічного механізму забезпечення економічної безпеки сучасного підприємства. *Бізнес-навігатор*. 2019. Вип. 3-1 (52). С. 118-123.

2. Сабецька Т.І., Сабецький В.Б. Теоретичні засади стратегічного планування економічної безпеки підприємства. *Вісник Одеського національного університету. Серія: Економіка.* 2019. URL: http://surl.li/ouwdk (дата звернення: 22.12.2023).

3. Вакарчук А.В., Сабецька Т.І. Поняття та класифікація інноваційних стратегій економічної безпеки підприємства. *Пріоритети економічної науки XXI століття*: зб. тез доп. наук.-практ. конф., м. Івано-Франківськ, 17 черв. 2020 р. Івано-Франківськ: НАІР, 2020. Т. 2. С. 130-132.

4. Міщенко С.П. Концептуальні аспекти економічної безпеки підприємств у ринковій економіці. *Маркетинг і менеджмент інновацій*. 2011. № 2. С. 190-195.

5. Орлик О.В. Концептуальні основи стратегії забезпечення фінансово-економічної безпеки підприємства. *Сталий розвиток економіки*. 2016. № 1 (30). С. 67-73.

6. Vasilieva L. Theoretical fundamentals of the mechanism of formation of strategy for ensuring economic security of the enterprise. *Scientific and methodological principles of accounting, financial, informational and language and communication support for sustainable development of agribusiness entities and rural territories :* a collective monograph / edited by H. Pavlova and L. Vasilieva. Dnipro : Printing house «Standard», 2022. Pp. 5-28. URL : https://dspace.dsau.dp.ua/handle/123456789/6605 (дата звернення: 22.12.2023).

7. Ковальська Л., Голій О., Голій В. Економічна безпека підприємства: сутність, структура та механізм забезпечення. *Економічний форум.* 2023. № 1. С. 126-137.

8. Oehlert P. 4 Critical Principles of Enterprise Security: A Smartsheet Report. 2019. 9 с. URL : http://surl.li/oyvbe (дата звернення: 04.01.2024).

9. Sirosh D. Enterprise IT Security: How to Reorganize and Centralize Your Cybersecurity System. *Infopulse*. URL : https://www.infopulse.com/blog/how-to-centralize-enterprise-security-system (дата звернення: 04.01.2024).

10. Майстро Р.Г., Більовська О.О. Конкурентоспроможність бізнесу в умовах війни в Україні. *Вісник НТУ «ХПІ» (економічні науки)*. 2023. № 3. С. 21-25.

11. Мінц О.Ю., Дорошкевич Г.В. Аналіз сценаріїв подолання енергетичного колапсу підприємствами малого бізнесу України. *Вісник Приазовського Державного Технічного Університету. Серія: Економічні науки*. 2023. № 1 (38). С. 61-68.

12. Кримчак Л.А. Трансформація ризиків та загроз економічної безпеки вітчизняних суб'єктів господарювання. *Development service industry management*. 2023. № 1. С. 56-60.

13. Вітковська О.В., Панченко І.В. Особливості підбору персоналу на українському ринку праці в умовах воєнного стану. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2022. № 2 (14). С. 200-204.

14. Фальченко О.О., Глушач Ю.С. Стратегія забезпечення економічної безпеки підприємств. *Вісник НТУ «ХПІ».* 2013. № 66 (1039). С. 157-160.

15. Захаров О.І. Стратегія економічної безпеки підприємства. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. № 2. С. 272-282.

16. Лаврентьєва Л.В. Стратегія економічної безпеки корпоративного підприємства. *Збірник наукових праць професорсько-викладацького складу ДонНУ імені Василя Стуса за 2015-2016 рр.* Донецьк, 2017. С. 51-52.

17. Швець Ф.В. Сутність стратегії безпеки організації. Збірник матеріалів круглого столу «Філософія публічного управління, менеджменту та функціонування медіа» (Вінниця, 18.11.2024 р.) Вінниця, 2024 С. 37-43

18. Данченко О.Б., Поскрипко Ю.А., Занора В.О. Стратегічне управління у сфері фінансово-економічної безпеки підприємства: методичні положення щодо забезпечення. *Економіка і суспільство*. 2016. № 6. С. 112-116.

19. Стеклова Н.В. Механізм стратегічного управління економічною безпекою підприємства. *Обліково-аналітичне забезпечення системи фінансово-економічної безпеки*: *інформаційно-комунікаційні технології та антикорупційний менеджмент:* матеріали VIII міжнар. наук.-практ. інтернет-конф. для здобувачів вищ. освіти і молодих науковців, Харків, 07 листопада 2019 р. Харків : ХНУМГ ім. О. М. Бекетова, 2019. С. 225-227.

20. Доценко І.О., Мельничук О.П. Стратегічне управління фінансово-економічною безпекою підприємства. *Держава та регіони. Серія: Економіка та підприємництво.* 2018. № 3 (102). С. 79-84.

21. Панченко В.А. Основні елементи системи економічної безпеки підприємства. *Ефективна економіка.* 2018. № 3. URL : http://www.economy.nayka.com.ua/pdf/3_2018/74.pdf (дата звернення: 04.01.2024).

22. Enterprise security system. *DeltaGuard international security agency*. URL : http://surl.li/oyuyq (дата звернення: 04.01.2024).

23. Борисюк О.В., Маленицький Д.С. Сутність стратегії та її значення для безпеки підприємства. *Глобальні та національні проблеми економіки*. 2018. Вип. 23. С.160-164.

24. Роженко О.В. Стратегії економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2015. № 51. С. 51-55.

25. Коптєва Г.М. формування стратегій забезпечення економічної безпеки підприємства. *Сучасні проблеми правового, економічного та соціального розвитку держави* : тези доп. X Міжнар. наук.-практ. конф., присвяч. 27-й річниці створення Харків. нац. ун-ту внутр. справ (м. Харків, 19 листоп. 2021 р.) / МВС України, МОН України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». – Харків : ХНУВС, 2021. С. 217-219.

26. Гавриш О.А., Черняк Г.М. Розроблення стратегії забезпечення економічної безпеки підприємств енергетичної галузі. *Економічний вісник НТУУ «КПІ»*. 2016. № 13. URL : http://ev.fmm.kpi.ua/article/view/80113 (дата звернення: 06.01.2024).

27. Пуцентейло П., Гуменюк О. Основні аспекти формування ефективної системи економічної безпеки підприємства. *Економічний дискурс*. 2017. Вип. 2 С. 37-47.

28. Бортнік С.М. Стратегічне управління розвитком персоналу в контексті забезпечення кадрової безпеки підприємства. *Економічний форум*. 2018. № 2. С. 331-338.

29. Гетьман О.О., Царюк С.Ю. Управління підбором і наймом персоналу на підприємстві (організації). *Глобальні та національні проблеми економіки.* 2018. № 2. С. 536-541.

30. Кубіній Н.Ю., Варга В.П. Сучасні підходи до відбору персоналу на підприємстві. *Науковий вісник Ужгородського Університету. Серія Економіка.* 2020. Вип. 2 (56). С. 108-113.

31. Приймак В., Москальчук В. Методи підбору та відбору персоналу на підприємстві. *Проблеми становлення інформаційної економіки в Україні*: матеріали V Міжнар. наук.-практ. конф., м. Львів, 18-19 листоп. 2022 р. Львів: Растр-7, 2022. С. 170-173.

32. 17 Effective Employee Selection Methods To Consider. *Indeed*. URL : http://surl.li/pgbha (дата звернення: 10.01.2024).

33. Якимова Н.С., Марценюк О.В., Мойсєєва В.О. Удосконалення системи розвитку персоналу на підприємстві. *Економіка та суспільство*. 2021. № 32. http://www.economyandsociety.in.ua/index.php/journal/article/view/743/714 (дата звернення: 12.01.2024).

34. Про професійний розвиток працівників : Закон України від 12.01.2012 р. № 4312-VI : станом на 27 груд. 2019 р. URL: https://zakon.rada.gov.ua/laws/show/4312-17#Text (дата звернення: 12.01.2024).

35. Швець Ф.В. Розробка стратегії економічної безпеки організації та забезпечення її кадрового потенціалу. Збірник матеріалів Науково-практичного симпозіуму «Ринок праці, людський капітал та професійна орієнтація молоді в умовах війни» (Вінниця, 10.05.2024 р.). Вінниця, 2024. С.45-49

36. Вівчар О., Зяйлик М., Горин Р. Логістична стратегія у системі забезпечення економічної безпеки підприємства. *Трансформація бізнесу для сталого майбутнього: дослідження, діджиталізація та інновації*: зб. тез доп. II Міжнар. наук.-практ. конф., м. Тернопіль, 23-24 листоп. 2022 р. Тернопіль, 2022. С. 33-35.

37. Шостак Л., Носалюк В. Логістична стратегія підприємства як новий підхід в управлінні. *Проблеми раціонального використання соціально-економічного, еколого-енергетичного потенціалу України та її регіонів*: матеріали V Міжнар. наук.-практ. конф. ГО «ІЕЕЕД», (15 лют. 2023 р.), м. Луцьк: ФОП Мажула Ю.М., 2023. С. 156-157.

38. Дуда С., Шостак Л. Формування логістичної стратегії вітчизняних підприємств. *Інноваційний розвиток та безпека підприємств в умовах неоіндустріального суспільства*. С. 66-67.

39. Крамар Р.І. Безпека підприємства в політико-правовій сфері. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2021. Вип. 29. С. 4-10.

40. Кодекс цивільного захисту України : Кодекс України від 02.10.2012 р. № 5403-VI : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text (дата звернення: 14.01.2024).

41. Хитра О.Л. Особливості діяльності державної служби з надзвичайних ситуацій щодо реалізації державної політики у сфері цивільного захисту населення. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2022. Вип. 32. С. 212-219.

42. Про охорону праці : Закон України від 14.10.1992 р. № 2694-XII : станом на 1 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення: 14.01.2024).

43. Деякі питання ідентифікації об'єктів підвищеної небезпеки : Постанова Каб. Міністрів України від 13.09.2022 р. № 1030 : станом на 11 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1030-2022-п#Text (дата звернення: 14.01.2024).

44. Про затвердження Правил пожежної безпеки в Україні : Наказ М-ва внутр. справ України від 30.12.2014 р. № 1417 : станом на 7 квіт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0252-15#Text (дата звернення: 14.01.2024).

45. Про затвердження Типового положення про службу охорони праці. (НПАОП 0.00-4.35-04) : Наказ Держ. ком. України з нагляду за охорон. пр. від 15.11.2004 р. № 255 : станом на 14 квіт. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/z1526-04#Text (дата звернення: 14.01.2024).

46. Про охорону навколишнього природного середовища : Закон України від 25.06.1991 р. № 1264-XII : станом на 8 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1264-12#Text (дата звернення: 16.01.2024).

47. Про оцінку впливу на довкілля : Закон України від 23.05.2017 р. № 2059-VIII : станом на 4 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2059-19#Text (дата звернення: 16.01.2024).

48. Про управління відходами : Закон України від 20.06.2022 р. № 2320-IX : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2320-20#Text (дата звернення: 16.01.2024).

49. Кривокульська Н.М., Богач Ю.А., Крисько Ж.Л. Стратегічне і екологічне управління як сучасні тренди управління комерційною діяльністю. *Економіка та суспільство*. 2022. Вип. 41. URL: http://surl.li/qitew (дата звернення: 16.01.2024).

50. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 31 груд. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 17.01.2024).

51. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.01.2024).

52. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 17.01.2024).

53. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 17.01.2024).

54. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99 : станом на 4 трав. 2008 р. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 17.01.2024).

55. Кодекс України про адміністративні правопорушення (статті 1 - 212-24) : Кодекс України від 07.12.1984 р. № 8073-X : станом на 14 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 17.01.2024).

56. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 17.01.2024).

57. Зубрицька М.В. Недоліки сучасного стану правового регулювання кримінальної відповідальності роботодавця за порушення трудового законодавства. *Юридична наука*. 2020. № 10(112). С. 152-157.

58. Вирок Слов`янського міськрайонного суду Донецької області від 27.05.2019 р. у справі № 243/4624/19. URL: https://reyestr.court.gov.ua/Review/82021579 (дата звернення: 18.01.2024).

59. Вирок Лозівського міськрайонного суду Харківської області від 28.01.2020 р. у справі № 629/5515/19. URL: https://reyestr.court.gov.ua/Review/87195966 (дата звернення: 18.01.2024).

60. Вирок Луцького міськрайонного суду Волинської області від 15.06.2020 р. у справі № 161/6422/20. URL: https://reyestr.court.gov.ua/Review/89800532 (дата звернення: 18.01.2024).

61. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. № 64/2022 : станом на 10 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення: 18.01.2024).

62. Штоляр О. Планування дій у надзвичайних ситуаціях. *Охорона праці*. URL: https://ohoronapraci.kiev.ua/article/news/planuvanna-dij-u-nadzvicajnih-situaciah (дата звернення: 22.01.2024).

63. Про затвердження Плану реагування на надзвичайні ситуації державного рівня : Постанова Каб. Міністрів України від 14.03.2018 р. № 223 : станом на 3 трав. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/223-2018-п#Text (дата звернення: 22.01.2024).

64. Дії роботодавця під час повітряної тривоги. *Ок. Кадровик*. URL: http://surl.li/pqvaj (дата звернення: 22.01.2024).

65. Як діяти під час сигналу «Повітряна тривога!». *Державна служба України з надзвичайних ситуацій*. URL: http://surl.li/pqvgm (дата звернення: 22.01.2024).

66. Робимо все, щоб відновити наші сервіси після хакерської атаки. *Київстар*. URL: http://surl.li/pqvjj (дата звернення: 22.01.2024).

67. У Monobank заявили про масовану кібератаку (оновлено). *Слово і Діло*. URL: http://surl.li/pqvnr (дата звернення: 22.01.2024).

68. Васьків О. Monobank знову зазнав масштабної DDoS-атаки. Гороховський заявив про 580 млн запитів на сервіс та нову хвилю. *Суспільне Новини*. URL: http://surl.li/pqvpb (дата звернення: 22.01.2024).

69. DDoS-атака на ЦСК «Україна». Головні події та новини у сфері КЕП і ЕДО в Україні. *ЦСК «Україна»*. URL: http://surl.li/pqvtg (дата звернення: 22.01.2024).

70. Чергова DDOS-атака на ЦСК «Україна». Головні події та новини у сфері КЕП і ЕДО в Україні. *ЦСК «Україна»*. URL: http://surl.li/pqvtx (дата звернення: 22.01.2024).

71. Шкальова А. Із початку війни кібератаки на «Нову Пошту» посилилися у п’ять-шість разів. *Forbes*. URL: http://surl.li/ptspp (дата звернення: 22.01.2024).

72. Жирій К. Життя у темряві: як бізнес виживає у часи постійних відключень світла та інтернету. *УНІАН*. URL: http://surl.li/pryeg (дата звернення: 23.01.2024).

73. Як відключення електроенергії впливає на роботу бізнесу? *Дебет-Кредит*. URL: http://surl.li/przhj (дата звернення: 23.01.2024).

74. Прищепа Я., Матвіїшина Г. «Велике випробування»: експертка розповіла про наслідки відключень електрики для бізнесу. *Суспільне Новини*. URL: http://surl.li/prlfy (дата звернення: 23.01.2024).

75. Продіус О.І. Особливості забезпечення економічної безпеки підприємств в розвинених країнах. *Науковий вісник Міжнародного гуманітарного університету*. 2016. № 19. С. 79-82.

76. Милка А.С., Артеменко Л.П. Світовий досвід забезпечення економічної безпеки. *Бізнес, інновації, менеджмент*: проблеми та перспективи: IV Міжнар. наук.-практ. конф., м. Київ, 20 квіт. 2023. Київ, 2023. С. 48-49.

77. Потюк В.М. Зарубіжний досвід формування економічної безпеки суб’єктів підприємницької діяльності. *Причорноморські економічні студії*. Вип. 38-1. 2019. С. 140-146.

78. Strategic Plan 2023-2025. *The Private Security Authority*. 2022. 21 с. URL: http://surl.li/qfjao (дата звернення: 01.02.2024).

79. Warren Community Food Security Strategic Plan. 2017. 24 с. URL: http://surl.li/qfjcy (дата звернення: 02.02.2024).

80. Strategy 2025 Delivering excellence in a digital world. *DHL Group*. URL: https://group.dhl.com/en/about-us/the-group/strategy.html (дата звернення: 02.02.2024).

81. State of Minnesota Enterprise Security Strategic Plan. Office of Enterprise Technology – Enterprise Security Office, Members of the Information Security Council. 13 с. URL: http://surl.li/qfjne (дата звернення: 02.02.2024).

ДОДАТКИ

Додаток 1

№ з/п	Принцип	Автор								Разом
		Л. Ковальська, О. Голій, В. Голій	О. Данченко, В. Занора Ю. Поскрипко	С. Міщенко	Н. Стеклова	І. Доценко, О. Мельничук	В. Панченко	DeltaGuard	П. Олерта	
1.	Законність		+			+	+	+		4
2.	Системність	+	+	+			+	+		5
3.	Адаптивність	+			+	+				3
4.	Раціональність та доцільність	+	+		+		+	+		5
5.	Стратегічна орієнтація	+			+	+	+			4
6.	Скоординованість		+			+		+		3
7.	Плановість		+	+			+	+		4
8.	Конфіденційність та захист даних						+		+	2
9.	Принцип проведення контролю (аудиту, моніторингу)				+				+	2