

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра економічної кібернетики та управління економічною безпекою
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти другий (магістерський)

Організація та управління системою економічної безпеки підприємства
(тема)

Виконав:
студент 2 курсу, групи УФЕБзм-20-1
Мандзіна В.І.
(прізвище, ініціали)

Спеціальність 073 Менеджмент
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління
фінансово-економічною безпекою
(повна назва освітньої програми)

Керівник доц. Мусієнко В.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____
(підпис)

Полозова Т. В.
(прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет Навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра економічної кібернетики та управління економічною безпекою
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 073 Менеджмент
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління фінансово-економічною безпекою
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
« _____ » _____ 20 ____ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Мандзіній Вірі Ігорівні
(прізвище, ім'я, по батькові)

1. Тема роботи Організація та управління системою економічної безпеки підприємства

затверджена наказом по університету від 23 жовтня 2021 р. № 159 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 14 грудня 2021 р.

3. Вихідні дані до роботи Наукові інформаційні джерела, періодичні видання, теоретичні та методичні розробки вчених в області управління економічною безпекою підприємства, статистичні дані досліджуваного підприємства, інформаційні джерела

4. Перелік питань, що потрібно опрацювати в роботі _____

Вступ. 1 Теоретичні засади організації та управління системою економічної безпеки підприємства. 2 Аналіз показників діяльності та напрямів організації економічної безпеки ТОВ «Каспер». 3 Удосконалення напрямів організації та управління системою економічної безпеки підприємства. Висновки. Перелік джерел посилання. Додаток.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій _____

1. Об'єкт, предмет, мета і завдання роботи. 2. Основні підходи щодо визначення сутності категорії «економічна безпека підприємства». 3. Взаємозв'язок структурних складових економічної безпеки підприємства. 4. Підходи до визначення економічної безпеки підприємства. 5. Послідовність формування системи роботи з персоналом на підприємстві. 6-8. Показники діяльності ТОВ «Каспер». 9. Основні функції підрозділу безпеки підприємства. 10. Організація експрес-аналізу економічної безпеки підприємства. 13. Джерела загроз діяльності ТОВ «Каспер». _____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	25.10.21-31.10.21	виконано
2	Виконання другого розділу роботи	01.11.21-15.11.21	виконано
3	Виконання третього розділу роботи	16.11.21-30.11.21	виконано
4	Оформлення роботи	01.12.21-05.12.21	виконано
5	Перевірка роботи на плагіат	06.12.21-08.12.21	виконано
6	Підготовка доповіді та ілюстративного матеріалу	09.12.21-10.12.21	виконано
7	Рецензування роботи	11.12.21-13.12.21	виконано
8	Подання роботи до екзаменаційної комісії	14.12.2021	

Дата видачі завдання 25 жовтня 2021 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Мусяєнко В.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 93 с., 14 табл., 10 рис., 56 джерел, 1 додаток.

ЕКОНОМІЧНА БЕЗПЕКА, ОРГАНІЗАЦІЯ, УПРАВЛІННЯ,
АНАЛІТИЧНА РОБОТА, ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗВИТОК
ПЕРСОНАЛУ.

Об'єктом дослідження є управління системою економічної безпеки підприємства.

Метою дослідження є теоретичне обґрунтування та розробка напрямів удосконалення організації та управління системою економічної безпеки підприємства.

Розкрито сутність та функціональні складові системи економічної безпеки підприємства. Розкрито зміст організації роботи з персоналом як складової системи економічної безпеки підприємства. Розглянуто особливості організації інформаційної безпеки підприємства. Здійснено аналіз показників діяльності та напрямів організації економічної безпеки ТОВ «Каспер». Розроблено рекомендації щодо формування механізму управління економічною безпекою підприємства. Запропоновано напрями удосконалення організації системи економічної безпеки ТОВ «Каспер».

ABSTRACT

Master thesis: 93 p., 14 tables, 10 fig., 56 sources, 1 exhibit.

ECONOMIC SECURITY, ORGANIZATION, MANAGEMENT,
ANALYTICAL WORK, INFORMATION SECURITY, PERSONNEL
DEVELOPMENT.

The object of the research – the management of economic security of enterprises.

The purpose of the research – a theoretical justification and development of ways to improve the organization and management of economic security of the enterprise.

The essence and functional components of the economic security system of the enterprise are revealed. The content of the organization of work with personnel as a component of the system of economic security of the enterprise is revealed. The peculiarities of the organization of information security of the enterprise are considered. The analysis of indicators of activity and directions of the organization of economic security of «Casper» LLC is carried out. Recommendations for the formation of a mechanism for managing the economic security of the enterprise have been developed. The directions of improvement of the organization of the system of economic security of «Casper» LLC are offered.

ЗМІСТ

Вступ.....	6
1 Теоретичні засади організації та управління системою економічної безпеки підприємства.....	9
1.1 Сутність та функціональні складові системи економічної безпеки підприємства.....	9
1.2 Організація роботи з персоналом як складова системи економічної безпеки підприємства.....	20
1.3 Особливості організації інформаційної безпеки підприємства.....	30
2 Аналіз показників діяльності та напрямів організації економічної безпеки ТОВ «Каспер».....	42
2.1 Характеристика фінансово-економічних результатів діяльності підприємства.....	42
2.2 Аналіз показників рентабельності.....	51
2.3 Напрями організації економічної безпеки на підприємстві.....	55
3 Удосконалення напрямів організації та управління системою економічної безпеки підприємства.....	60
3.1 Формування механізму управління економічною безпекою підприємства.....	60
3.2 Напрями удосконалення організації системи економічної безпеки ТОВ «Каспер».....	70
Висновки.....	83
Перелік джерел посилання.....	87
Додаток А Копії публікацій.....	94

ВСТУП

Ринково-орієнтована система управління не лише сприяє розвитку українського підприємництва, а й висуває певні вимоги до діяльності корпоративної структури. Зовнішнє середовище все більше впливає на рівень відповідальності керівників підприємств за прийняття управлінських рішень. Тому формування корпоративної економічної безпеки є особливо важливим. З цією метою кожне підприємство використовує свій набір виробничих ресурсів (земля, капітал, інформація, технології, інтелектуальна власність тощо).

Теоретичні та прикладні аспекти забезпечення економічної безпеки підприємства досліджувалися у роботах багатьох науковців, серед яких В. В. Євдокимов, О. В. Олійник, Д. О. Грицишен, О. О. Грищенко, Р. Г. Майстро, Т. В. Полозова, Л. В. Шмалій, М. В. Ількевич, Т. О. Меліхова, І. В. Новик та інші.

Проблематика забезпечення економічної безпеки підприємств в умовах цифрових технологій і пандемії COVID-19 знайшла відображення у роботах таких авторів, як К. С. Жадько, Д. М. Самойленко, В. Й. Бакай, О. В. Ольшанський, М. Д. Крамчанінова та інших.

Особливості економічної поведінки підприємства в контексті безпекоорієнтованого управління досліджувалися таким науковцями, як А. М. Штангрет, М. М. Караїм, І. А. Штангрет та іншими.

Особливості формування механізмів забезпечення економічної безпеки підприємств розглядалися у роботах таких учених, як В. О. Христофоров, Є. Г. Андрющенко та інших.

Проте існуючі теоретичні підходи до організації та управління системою економічної безпеки підприємства потребують подальшого удосконалення.

Об'єктом дослідження є управління системою економічної безпеки підприємства.

Предметом дослідження є підходи до організації та управління системою економічної безпеки підприємства.

Метою дослідження є теоретичне обґрунтування та розробка напрямів удосконалення організації та управління системою економічної безпеки підприємства.

Завдання дослідження:

- розкрити сутність та функціональні складові системи економічної безпеки підприємства;
- розкрити зміст організації роботи з персоналом як складової системи економічної безпеки підприємства;
- розглянути особливості організації інформаційної безпеки підприємства;
- здійснити аналіз показників діяльності та напрямів організації економічної безпеки ТОВ «Каспер»;
- розробити рекомендації щодо формування механізму управління економічною безпекою підприємства;
- запропонувати напрями удосконалення організації системи економічної безпеки ТОВ «Каспер».

Методичною та інформаційною основою для проведення досліджень були періодичні наукові видання, законодавство України, фінансова звітність досліджуваного підприємства.

Під час дослідження були використані методи аналізу, синтезу, графічний, порівняння, факторний аналіз, узагальнення показників.

Практична значущість отриманих результатів полягає у тому, що запропоновані практичні рекомендації можуть бути використані підприємствами будь-якої галузі для підвищення рівня організації та управління економічною безпекою підприємства.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на II Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків, 2021).

Публікації. Результати досліджень опубліковано у 2 наукових працях, у тому числі 1 стаття у колективній монографії, 1 тези конференції.

1 ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Сутність та функціональні складові системи економічної безпеки підприємства

Поняття «безпека» широко використовується практично у всіх сферах будь-якої діяльності, і воно глибоко увійшло в сучасне життя. У свою чергу, економічна безпека підприємства (ЕБП) тісно пов'язана з виробництвом, інженерними показниками та наданням послуг. Від ефективності їхньої роботи залежить економічний стан всієї країни. Наразі більшість українських компаній зазнали глибокого спаду виробництва і перебувають у критичному стані або банкрутстві. Така ситуація становить певну небезпеку для потенціалу та працівників області та кожного підприємства. Адже, будучи основним структурним елементом економіки, будь-яке підприємство не лише бере на себе виробничі функції, а й забезпечує життєдіяльність багатьох людей, несе соціальний тягар і відповідальність.

Крім того, концепція системи корпоративної економічної безпеки не є досконалою, а відсутність системи вимірювання та управління корпоративною економічною безпекою також є причиною недосконалості методу визначення сутності економічної безпеки. Для промислових підприємств дуже важливою є оцінка економічної безпеки, оскільки потенціал активної участі є вирішальним і стабільним чинником антикризового розвитку, гарантією економічного зростання, підтримкою національної економічної незалежності та безпеки. Крім того, забезпечення статусу та тенденції розвитку ЕВР залежить не лише від потенціалу окремого підприємства, а й усуває або мінімізує збитки в усій економіці. Це основна функція економічної безпеки.

Економічна безпека підприємства – це комплексне поняття, що включає низку факторів, пов'язаних із внутрішнім станом підприємства та впливом зовнішнього середовища, а також основного органу, що взаємодіє з підприємством. Зараз великі вітчизняні підприємства, у тому числі більшість провідних груп підприємств (холдингів), створили у своїх структурах спеціалізовані підрозділи для забезпечення економічної безпеки цих підприємств. Проте на практиці у значній кількості керівників цих новостворених служб ще не сформовано розуміння того, що безпека є однією з основних видів економічної діяльності. Не існує єдиної розробленої та ефективної наукової системи оцінки та забезпечення економічної безпеки. працювати.

Економічна безпека підприємства – це система, яка забезпечує мобілізацію та оптимальне управління ресурсами підприємства для забезпечення його сталої діяльності та активного реагування на будь-які негативні впливи навколишнього середовища [1]. Тому економічну безпеку підприємств слід розглядати з трьох аспектів. Перший – економічна безпека – стан найбільш ефективного використання ресурсів підприємства, що гарантує запобігання зовнішнім екологічним загрозам, стабільну роботу підприємства зараз і в майбутньому (фінансові аспекти). По-друге, економічну безпеку можна розглядати як систему оцінки та забезпечення економічної безпеки (економічні аспекти). Проте завдання підприємців – не лише аналізувати й оцінювати економічну безпеку, а й вміти робити прогнози. По-третє, економічна безпека полягає у забезпеченні сталого функціонування підприємств в умовах негативного впливу навколишнього середовища шляхом мобілізації ресурсів підприємства та оптимального управління.

Під економічною безпекою підприємства слід розуміти захист його науково-технічного, технологічного, виробничого та людського потенціалу від прямих (активних) або непрямих (пасивних) економічних загроз,

наприклад неефективних країн чи сформованої науково-виробничої політики, а також адаптуватися під несприятливе зовнішнє середовище та здатність його гнучко реагувати на його зміни [1-3].

Основною метою економічної безпеки підприємства є забезпечення його стабільної та найбільш ефективної роботи та великого потенціалу для майбутнього розвитку.

Очевидно, що забезпечення економічної безпеки є безперервним циклом. Тому економічну безпеку підприємств можна розглядати як систему заходів щодо забезпечення стабільності конкуренції підприємств та економічної стабільності, і водночас вона не матиме негативного впливу на стан та умови життя зайнятого населення республіки. підприємство. І населення, яке проживає в містах області.

Теоретичний виклад існуючих тлумачень поняття «економічна безпека фірми» та аналіз компонентів цих визначень дозволяють виділити шість методів, з яких можна розглянути сутність терміна (рис. 1.1).

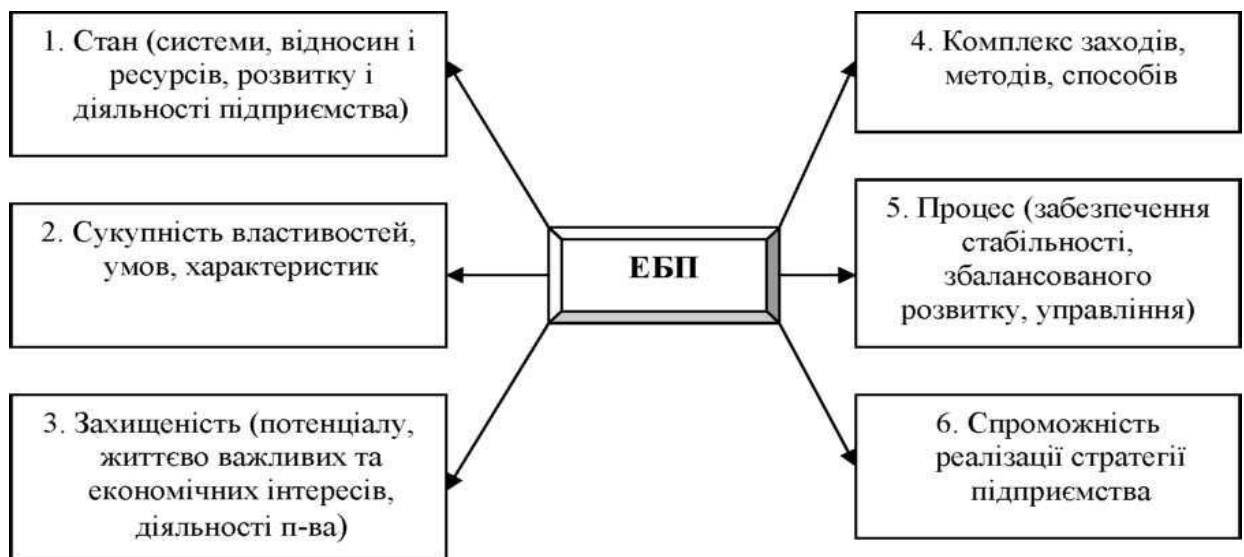


Рисунок 1.1 – Основні підходи до визначення сутності категорії «економічна безпека підприємства» [1-10]

Рівень економічної безпеки залежить від здатності служб підприємства ефективно запобігати загрозам та усувати збитки, спричинені негативним впливом на всі аспекти економічної безпеки. Джерелом такого негативного впливу може бути навмисна чи ненавмисна поведінка людей та організацій (у тому числі органів державної влади, міжнародних організацій чи конкурентів), а також збіг таких об'єктивних обставин: фінансовий стан корпоративного ринку, наукові відкриття та збіг технологічних розробки та форс-мажорні обставини.

Враховуючи структуру економічної безпеки підприємства, різні вчені відносять до цієї категорії дуже різноманітний перелік функціональних компонентів.

Взаємозв'язок між структурними елементами економічної безпеки підприємства (ЕБП) показано на рис. 1.2.

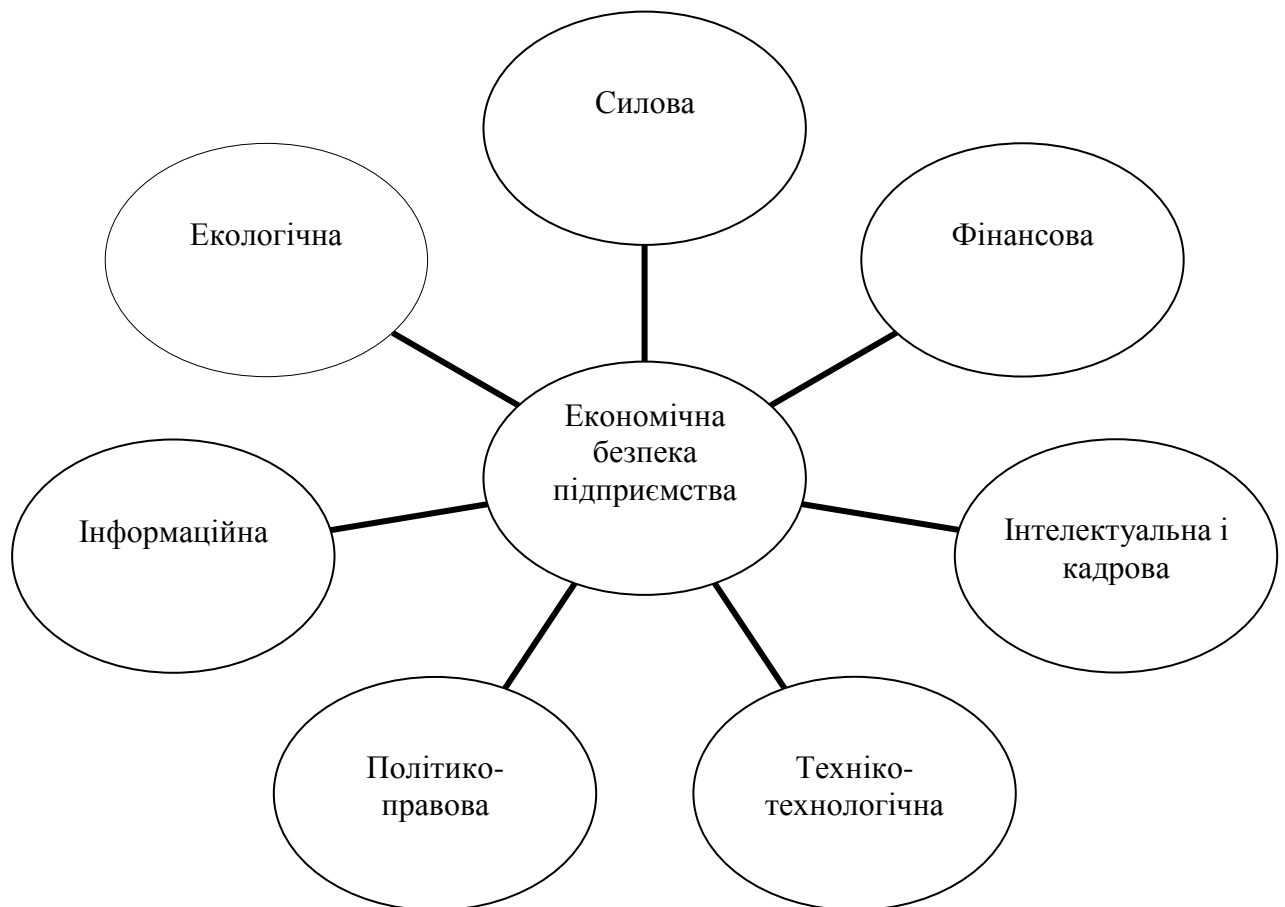


Рисунок 1.2 – Взаємозв'язок структурних складових економічної безпеки підприємства (ЕБП) [1-10]

Як показано на рисунку, в модульному представленні системи ЕБП виділені основні функціональні компоненти узгоджені між собою. Усі компоненти є окремими підсистемами, і вони працюють разом – кожна підсистема має своє завдання, але всі вони служать одній меті. Кожна підсистема має свій власний індекс оцінки параметрів. Система ЕБУ базується на технологіях і технологіях, кадрових, інформаційних та корпоративних компонентах – ресурсній основі.

Основні функціональні складові економічної безпеки підприємства:

- фінансова частина – для досягнення максимально ефективного використання ресурсів компанії;

- інтелектуальна та кадрова складові – захист та розвиток інтелектуального потенціалу підприємства ефективного управління персоналом;

- технологія та технічні складові – ступінь відповідності між технологією, що використовується підприємством, і його аналогами в сучасному світі для оптимізації витрат ресурсів;

- політико-правова частина-Повне юридичне забезпечення діяльності підприємства та дотримання чинного законодавства;

- інформаційно-компонентне ефективно інформаційно-аналітичне забезпечення господарської діяльності підприємства;

- екологічні фактори-Дотримуватися чинних екологічних законів та нормативних актів, щоб мінімізувати витрати на забруднення навколишнього середовища;

- компоненти живлення – для забезпечення особистої безпеки співробітників компанії та збереження їх майна.

Усі великі та середні підприємства створили автономні служби безпеки, а безпеку малих підприємств можуть гарантувати регіональні чи муніципальні служби, в яких на підприємстві працює один або кілька працівників охорони.

Такі служби безпеки зазвичай створюються місцевими правоохоронними органами або органами національної служби безпеки. Пріоритетним принципом організації та функціонування системи безпеки підприємства слід враховувати її комплексність. Конкретний набір завдань, які стоять перед службою безпеки компанії, визначає конкретний набір функцій, які вона виконує.

Загальні функції, які покладаються на служби корпоративної безпеки:

- організація та забезпечення відвідувань та внутрішньооб'єктних систем у межах приміщень, замовлення послуг;
- участь у формуванні основних документів для відображення вимог охоронних організацій та захисту комерційної таємниці;
- розробити та впровадити заходи щодо забезпечення обробки документів, що містять інформацію про комерційну таємницю, та контролю за дотриманням вимог інструкційних матеріалів;
- виявлення та блокування каналів, які можуть розкривати конфіденційну інформацію, та проведення статистики та аналізу вразливостей безпеки співробітників, клієнтів та конкурентів;
- організувати та проводити службові розслідування щодо розголошення або втрати документів та інших фактів, що порушують корпоративну безпеку;
- формувати, оновлювати та доповнювати перелік відомостей, що становлять комерційну таємницю, та інші нормативно-правові акти, що регулюють діяльність організацій з безпеки та захисту інформації;
- забезпечити дотримання вимог нормативно-правових актів про захист комерційної таємниці;
- організувати та регулярно навчати працівників підприємства та підрозділів безпеки з усіх напрямків захисту комерційної таємниці;

- вести облік сейфів і металевих шаф, що дозволяють постійно або тимчасово зберігати конфіденційні документи, а також обліковувати та охороняти спеціальні місця та технічні засоби;

- підтримувати зв'язок з правоохоронними органами та підрозділами безпеки сусідніх підприємств (організацій) для вивчення криміногенної ситуації в районі.

У нормативних документах, що визначають організацію служби безпеки підприємства, є певні об'єкти, які потребують захисту від потенційних загроз та протиправних розкрадань. Вони включають:

- персонал;
- матеріальна трудова інформація та фінансові ресурси;
- обмеження доступу до інформаційних ресурсів;
- комп'ютеризовані інструменти та системи компанії;
- технічні засоби та системи захисту та захисту матеріальних та інформаційних ресурсів.

Служби безпеки компанії завжди повинні бути готові до подолання критичних (кризових) ситуацій, які можуть виникнути через конфлікт інтересів між компанією та злочинним світом. Для управління безпекою багато компаній створили так звані кризові групи, до складу яких входять керівники компаній, юристи, фінансисти та керівники відділів безпеки. Основна мета антикризової команди – протидія зовнішнім загрозам безпеці компанії.

За оцінками експертів, витрати на створення системи безпеки підприємства та її оптимізацію роботи можуть досягати 25% вартості всього виробничого процесу. До ресурсів забезпечення надійного виживання та поступового розвитку підприємства належать: кадри підприємства, матеріальні та інтелектуальні (інформаційні) ресурси. З огляду на це, діяльність із забезпечення економічної безпеки підприємств включає чотири основні напрямки: захист матеріально-фінансової цінності; захист персоналу; захист прав інтелектуальної власності (у тому числі комерційної таємниці);

інформаційне забезпечення підприємницької діяльності підприємств під ринкові умови.

Отже, результатом забезпечення економічної безпеки підприємства є стабільність функціонування підприємства (надійність), ефективність фінансово-господарської діяльності (рентабельність), особиста безпека працівників.

Тому всі компоненти системи ЕБП тісно пов'язані між собою. Основними показниками його впливу є формування додаткового грошового потоку (приплив чи відтік), фінансові результати (прибуток і збиток), а також формування ефективного загального показника – ринкової вартості підприємства.

Розберемо більш детально існуючі методи визначення поняття «економічна безпека підприємства» (ЕБП) (табл. 1.1).

Підприємство працює в невизначених і ризикованих умовах, залучає ресурси для виробничо-господарської діяльності, виходить на ринок з метою отримання прибутку.

На трактування поняття «економічна безпека» впливає зовнішнє середовище. В умовах ринкової економіки зовнішнє середовище постійно змінюється і ніколи не залишиться стабільним. У контексті негативного впливу зовнішнього середовища на корпоративну діяльність слід розглянути зміст концепції економічної безпеки.

З даних, наведених у табл. 1.1 з точки зору очікуваних результатів, можна виділити шість загальнонаукових напрямів, що визначають економічну безпеку. Відповідно до першого підходу економічна безпека підприємства розглядається як захист підприємства від негативного впливу (загрози) зовнішнього та внутрішнього середовища. При цьому під економічною безпекою підприємства слід розуміти захист потенціалу від негативного впливу зовнішніх і внутрішніх факторів, а також здатність суб'єкта до відтворення.

Таблиця 1.1 – Основні підходи до визначення «ЕБП»

Автори	Визначення
Покропивний С. Ф. [11, с. 334]	Певний стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації, технології, техніки та устаткування) і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування, динамічного науково-технічного й соціального розвитку, запобігання внутрішніх і зовнішніх негативних впливів (загроз)
Федоренко Р. М. [12, с. 224]	Сукупний динамічний стан підприємства, який дозволяє формувати та здійснювати власну стратегію розвитку
Козаченко Г. В. [13, с. 87]	Гармонізація в часі і просторі економічних інтересів підприємства з інтересами пов'язаних з ним суб'єктів зовнішнього середовища, що діють поза межами підприємства
Ареф'єва О. В. Кузенко Т. Б. [14, с. 18]	Стан ефективного використання ресурсів підприємства та наявних ринкових можливостей для запобігання внутрішнім і зовнішнім загрозам, і забезпечення тривалого виживання та стійкого розвитку на ринку відповідно до обраної господарюючим суб'єктом місії
Камлик М. І. [15, с. 39]	Стан розвитку господарюючого суб'єкта, який характеризується стабільністю економічного розвитку, ефективністю нейтралізації негативних факторів та протидії їх впливу на всіх стадіях його діяльності
Андрушків Б. М. [16, с. 23]	Економічний стан підприємства, сталий до внутрішніх і зовнішніх змін фінансово-господарської діяльності, не пов'язаний з форс-мажорними обставинами; створення таких умов його діяльності, за яких забезпечується надійний захист економічних інтересів від різних загроз
Пухальська Г. В., Христюк Г. О. [17, с. 198]	Комплексне поняття, яке включає відповідні системи інформаційно-аналітичного моніторингу, попереджувальних, профілактичних, поточних і прогнозованих заходів щодо впливу на можливості загрози і має на меті нейтралізацію негативних наслідків
Поснова Т. В. [18, с. 5]	Стан, за якого підприємство здатне створювати матеріальні та фінансові ресурси, що є достатнім для життя та розвитку особистості, соціальної, воєнно-політичної стабільності суспільства, а також створює умови для економічного зростання
Кошембар Л. О. [19, с. 5]	Стан розвитку підприємства, який характеризується стабільністю економічного й фінансового розвитку, ефективністю нейтралізації негативних факторів та протидія їх впливу на всіх стадіях його діяльності.
Ортинський В. Л. [20, с. 11]	Захищеність потенціалу підприємства (виробничого, організаційно-технічного, фінансово-економічного, соціального) від негативної дії зовнішніх і внутрішніх чинників, прямих або непрямих економічних загроз, а також здатність суб'єкта до відтворення
Зацеркляний М. М., Мельников О. Ф. [21, с. 6]	Стан функціонуючого підприємства, за якого потенційні економічні загрози урівноважені адекватною системою заходів протидії (діючою на підприємстві системою економічної безпеки)
Іванюта Т. М., Заїчковський А. О. [22, с. 9]	Система створення механізму мобілізації й найбільш оптимального управління корпоративними ресурсами підприємства з метою найбільш ефективного їх використання і забезпечення стійкого функціонування, його активної протидії будь-яким негативним чинникам впливу
Шемаєва Л. Г. [23, с. 12]	Забезпечення реалізації стратегічних інтересів підприємства на основі використання можливостей зовнішнього середовища з застосуванням продуктивної взаємодії із суб'єктами зовнішнього середовища
Соколенко Т. М. [24]	Стан, за якого стратегічний потенціал фірми знаходиться поблизу границь адаптивності, а загроза втрати економічної безпеки наростає в міру наближення ступеня адаптивності стратегічного потенціалу до граничної зони.
Мішин О. Ю., Мішина С. В. [25, с. 89]	Стан захищеності бізнес-процесів та їх ресурсного забезпечення, що сприяє уникненню або попередженню внутрішніх і зовнішніх загроз і дозволяє забезпечити стабільне функціонування та розширене відтворення з мінімальними втратами для підприємства

Еволюційний метод базується на припущенні, що метою економічної безпеки підприємства є стабільна робота підприємства, комерційний успіх, поступове застосування науки і техніки, динамічний і поступальний розвиток, підтримка потенціалу, рейтинг тощо. Цей метод тісно пов'язаний з першим, оскільки вчені в основному дивляться на еволюцію компаній, забезпечуючи захист їх потенціалу від негативних факторів навколишнього середовища.

Деякі автори розглядають економічну безпеку в контексті системного підходу, тобто як систему взаємопов'язаних елементів для вирішення питання формування, формування та забезпечення необхідних рівнів розвитку корпоративної безпеки від існуючих і потенційних загроз та мінімізації їх негативного впливу. Характеристиками цієї системи є логічна структура, принципи, функції, відповідні методи управління, завдання тощо. Основою методу синергії, що визначає сутність поняття «економічна безпека», є синергія, яка досягається шляхом формування стану, що захищає бізнес-процеси від загроз. Очікуваним результатом впровадження підприємством та розробки заходів економічної безпеки є розширення відтворення з найменшими витратами.

Останній метод полягає у визначенні сутності поняття «економічна безпека» як міри інтересів підприємств та взаємодії з навколишнім середовищем (з боку підприємств, споживачів, оподаткування, кредитних установ тощо). У цьому випадку можна визначити, що економічна безпека підприємства – це комплексне відображення ступеня надійності підприємства як партнера в економічних відносинах виробництва, фінансів і торгівлі в певний період часу. Виходячи з методу координації, що визначає сутність поняття «економічна безпека підприємства», передбачається, що менеджмент має сформувати свою систему пріоритетів, визначити переваги взаємодії з навколишнім середовищем та вибрати цю форму і спосіб координації для забезпечення прибутку.

Наприклад, експертні процедури можна використовувати для визначення ступеня відповідності шляхом порівняння показників діяльності підприємства (фактичних чи планових) з показниками кількісної оцінки. Чим ближче результат цього порівняння до одиниці, тим більші вигоди від підприємства. Завдяки такому порівнянню можна зробити відповідні висновки та побудувати систему економічної безпеки підприємства.

Статус економічної безпеки підприємства відображає узгодженість і збалансованість інтересів підприємства та інтересів навколишнього середовища, при цьому підприємство має враховувати різні інтереси більшості контрагентів. Отже, якщо більшість інтересів підприємства узгоджується з екологічними інтересами, а підприємство отримує прибуток під час взаємодії, необхідно додатково підтвердити, що підприємство знаходиться в стані економічної безпеки. Узгодити всі інтереси практично неможливо, хоча це і є основою стратегічних цілей компанії.

Виявлення та попередження небезпек і загроз, використання корпоративних ресурсів для запобігання незворотних збитків за непередбачених обставин, прийняття ризикованих рішень, боротьба з конкурентами тощо – створюють умови для досягнення корпоративних стратегічних цілей та забезпечення корпоративного сталого розвитку економічної незалежності.

У цьому визначенні економічною безпекою підприємства вважається такий стан ресурсів підприємства, який забезпечує найбільш ефективно використання ресурсів підприємства в подальшому стабільному функціонуванні та розвитку, а також має здатність усувати негативні впливи та загрози та приносити економічні вигоди для підприємства. Узгоджувати з інтересами пов'язані особи.

Тому, аналізуючи основні теоретичні методи та систематичні результати, що визначають поняття «економічна безпека фірми», можна трактувати економічну безпеку підприємств як стан, захищений від

зовнішніх і внутрішніх факторів, завдяки ефективному використанню виробничих ресурсів, формулюйте та реалізуйте стратегічні напрями розвитку для забезпечення сталого функціонування та координації власних інтересів та екологічних переваг. Авторське визначення цієї статті буде використано для подальшого вивчення економічної безпеки підприємств.

1.2 Організація роботи з персоналом як складова системи економічної безпеки підприємства

Сучасна економічна ситуація вимагає впровадження нових методів у процес управління персоналом. Успіх виробничо-господарської діяльності підприємства значною мірою залежить від ефективності роботи людських ресурсів, що визначає ефективність діяльності організації в цілому. Серед багатьох факторів, що забезпечують майбутню конкурентоспроможність та ефективність підприємства, важливе місце займає використання конкурентоспроможності працівників у економічному процесі. І навпаки, шляхом реалізації стратегій, що відповідають умовам діяльності працівників, може формуватися конкурентоспроможність працівників.

Ефективна діяльність підприємства залежить не лише від високого рівня конкурентоспроможності та достатнього майнового потенціалу, а й від можливостей працівників та ефективності внутрішньої організації. Ефективність роботи людських ресурсів виявляється в ефективному використанні та розвитку матеріалів матеріального виробництва для задоволення потреб і очікувань покупців. Для досягнення такого результату підприємство має бути оснащене відповідною кількістю працівників з необхідним потенціалом та створити їм необхідні умови для підвищення ефективності.

Сьогодні практика вимагає від працівників не лише отримання результатів професійної освіти, а й включає їх практичну підготовку та вміння розв'язувати проблеми в типових і нестандартних ситуаціях професійного життя.

Найближчим часом, як ключова складова загальної конкурентоспроможності підприємства, підвищення потенціалу працівників і надалі залишатиметься в центрі уваги науковців і практиків.

Стратегічний розвиток співробітників має на меті створення організацій та умов для навчання, розвитку та вдосконалення професійних навичок для підвищення рівня організаційної, командної та особистісної ефективності. Стратегічний розвиток співробітників включає впровадження, усунення, модифікацію, управління та керівництво процесами та обов'язками, щоб усі співробітники та члени команди мали знання, навички, здібності та можливості, необхідні для виконання поточних та потенційних завдань, поставлених організація. Цей розвиток базується на баченні майбутніх можливостей і потенціалу людей і відбувається в загальній стратегічній моделі організації.

Стратегія розвитку талантів впливає з бізнес-стратегії і підтримує її реалізацію. Завдяки використанню високоякісних людських ресурсів можна задовольнити поточні та майбутні потреби організації. Стратегічне планування має на меті створити загальну модель розвитку співробітників, більшість процесу – створити середовище, яке стимулює розвиток співробітників. Діяльність кадрової служби включає тренінгові проекти розвитку інтелектуального капіталу та організаційні, командні та особисті культурні тренінги. Створено освітню організацію із системним управлінням знаннями. Політика стратегічного планування передбачає інвестування в людські ресурси та людський капітал організації. Однією з головних цілей управління персоналом є створення умов для реалізації потенціалу співробітників, що, як правило, включає не тільки вміння здобувати та

використовувати нові знання, навички та вміння, а й накопичені нереалізовані уявлення про шляхи вдосконалення організації.

Формулювання стратегії корпоративної конкурентоспроможності талантів має базуватися на таких принципах [29]: інновувати напрямок розвитку корпоративної конкурентоспроможності талантів, запроваджувати механізми стимулювання, покращувати якість навчання. Порядок дій щодо вибору стратегії корпоративної конкурентоспроможності співробітників повинен включати: визначення корпоративної конкурентної стратегії; вибір стратегій розвитку конкурентоспроможності для кожного типу співробітників, що підтримує стратегію компанії; дії, що вживаються для підтримки конкурентних переваг; поточну намагання зміцнити конкурентні позиції та покращити показники ефективності.

Розробка стратегії конкурентоспроможності співробітників є способом досягнення корпоративних цілей шляхом зміни кількості та якості працівників, передбачає певну послідовність дій для формування та реалізації відповідних стратегій. Системне управління персоналом підприємства – це цілеспрямована діяльність лінійних і функціональних керівників і персоналу служби персоналу всіх рівнів (рисунок 1.3).

Для вдосконалення системи управління персоналом в сучасних умовах необхідно використовувати такі методи [30]: Економіка, заснована на застосуванні економічних законів: матеріальне стимулювання, економічний аналіз, планування, затвердження економічних норм і стандартів, соціальна психологія на основі соціологія та психологія Використання законів: соціальний аналіз у колективі, соціальний розвиток колективу, психологічний вплив на співробітників (формування колективу, створення доброї психологічної атмосфери), моральна мотивація, ініціативність та відповідальність.

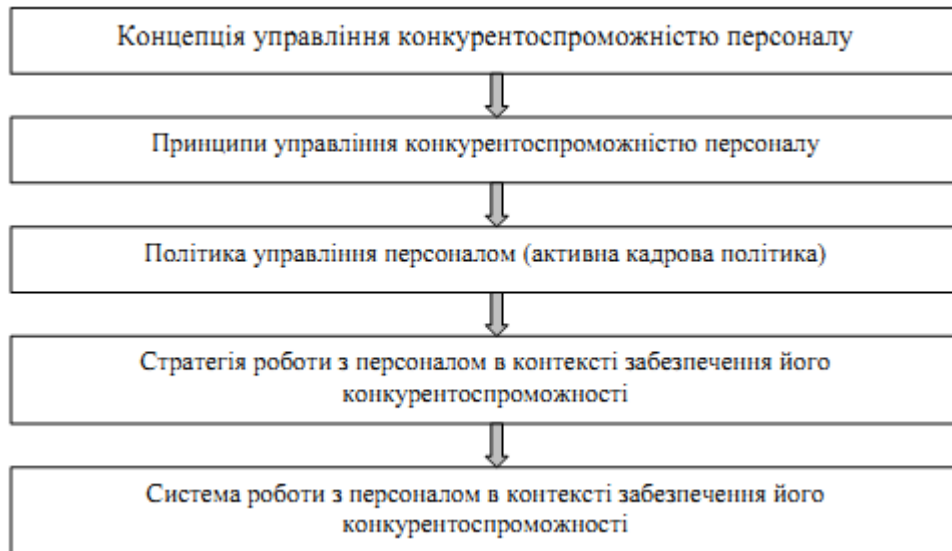


Рисунок 1.3 – Послідовність формування системи роботи з персоналом на підприємстві

Складовими стратегії управління персоналом є: умови і безпека праці, безпека персоналу; форми і методи налагодження трудових відносин; методи вирішення виробничих і соціальних конфліктів; встановлення норм і принципів етичних відносин у колективі, формування корпоративних кодексів (кодексів). ділової етики); політика зайнятості в організації, включаючи аналіз ринку праці, системи зайнятості та використання працівників, встановлення режиму праці та відпочинку, профорієнтацію та адаптацію персоналу; заходи щодо збільшення та кращого використання людських ресурсів; удосконалення методики прогнозування та планування потреби в кадрах на основі вивчення нових вимог до працівників і робочих місць; на основі систематичного аналізу та проектування різних посад і робочих місць у роботі; та кваліфікаційні вимоги до працівників, нові методи та нові форми відбору талантів, оцінки бізнесу та атестації; розробка концепції розвитку співробітників, включаючи нові форми і методи навчання, планування ділової кар'єри та розвитку кар'єри, формування кадрових резервів для прогнозування цих видів діяльності відповідно до

необхідного часу; удосконалення механізму управління стимулюванням персоналу; нові системи та форми оплати праці працівників забезпечують матеріальне та нематеріальне стимулювання, заходи щодо покращення трудових відносин та вирішення правових проблем у господарській діяльності; розробити нові та використовувати існуючі заходи організаційного соціального розвитку, покращити інформаційне забезпечення всього персоналу в рамках обраних стратегічних рамок, удосконалити всю систему управління персоналом або її різні підсистеми та елементи.

Отже, кадрова політика організації є похідною від стратегії організації, а її характеристики залежать від сфери стратегічного управління, що реалізується в організації (рис. 1.4) [25].

Основні завдання корпоративного стратегічного управління персоналом [27]: формулювання стратегій особистого навчання; покращення організаційного навчання та створення навчальних організацій; управління знаннями; формування інтелектуального капіталу; підвищення якості менеджерів; виховання «емоційної культури» та стратегічних можливостей.

Стратегія розвитку людських ресурсів. Особисті стратегії навчання. Організації керуються своїми вимогами до людських ресурсів, які виявляються у навичках, здібностях та поведінці, необхідних для досягнення організаційних цілей. Відправною точкою має бути метод надання можливостей навчання та розвитку.

Стратегія повинна відображати: метод визначення потреб у навчанні; роль планування особистісного розвитку та самонавчання; через керівництво, консультації, навчальний центр, репетиторство, позаорганізаційні курси (для задоволення конкретних потреб співробітників), внутрішні та зовнішні плани навчання та курси (для задоволення потреб команди) для підтримки особистого навчання.

Тип стратегії організації	Стратегія управління персоналом	Складові стратегії управління персоналом
<p>Підприємницька стратегія. Приймають проекти з високим ступенем фінансового ризику, мінімальною кількістю дій. Ресурсне забезпечення всіх вимог замовника. У центрі уваги – швидке здійснення найближчих заходів, навіть без відповідного опрацювання.</p>	<p>Пошук та залучення працівників-новаторів, ініціативних, контактних, з довготривалою орієнтацією, готових ризикувати, не бояться відповідальності. Важливо, щоб провідні співробітники не мінялися</p>	<p>Відбір і розстановка персоналу: пошук людей, здатних йти на ризик і доводити справу до кінця. Винагороди: на конкурентній основі, неупереджені, по можливості задовольняють смакам працівника. Оцінка: ґрунтується на результатах, не дуже жорстка. Розвиток особистості: неформальне, орієнтоване на наставника. Планування переміщень: в центрі - інтерес службовців. Підбір робочого місця, відповідного інтересам працівника.</p>
<p>Стратегія динамічного зростання. Ступінь ризику менша. Постійне зіставлення поточних цілей і створення фундаменту для майбутнього. Політика організації та процедури фіксуються письмово, оскільки вони тут необхідні і для більш суворого контролю, і як основа подальшого розвитку організації</p>	<p>Співробітники повинні бути організаційно закріплені, мати гнучкість в умовах, що змінюються, бути проблемно-орієнтованими і працювати в тісному співробітництві з іншими.</p>	<p>Відбір і розстановка персоналу: пошук гнучких і вірних людей, здатних ризикувати. Винагороди: справедливі. Оцінка: ґрунтується на чітко обумовлених критеріях. Розвиток особистості: акцент на якісному зростанні рівня і області діяльності. Планування переміщень: враховуються реальні сьогоденні можливості та різноманітні форми службового просування.</p>

Рисунок 1.4 – Взаємозв'язок стратегії організації та стратегії управління персоналом

Організаційні стратегії навчання. Організаційне навчання – процес координації змін системи з вбудованим механізмом доступу окремих осіб і груп до інформаційних ресурсів структурних і культурних підприємств, формування та використання їх для розвитку організаційних можливостей.

Стратегія організаційного навчання спрямована на розвиток ресурсних можливостей компанії. Це відповідає одному з основних принципів управління людськими ресурсами, тобто необхідності інвестувати в людей для розвитку людського капіталу, необхідного організації, і збільшення

кількості знань, умінь і навичок. Відповідно до теорії людського капіталу знання, вміння та навички, здобуті працівниками шляхом навчання та навчання, у тому числі професійні навички, набуті на основі особистого досвіду, утворюють певний обсяг виробничого капіталу.

Принципи організаційного навчання: передавати співробітникам чітке та загальне бачення організації, щоб покращити усвідомлення необхідності стратегічного мислення на всіх рівнях; стратегії мають бути сформульовані в рамках організаційного бачення, крім того, що вони переконливі, вони також повинні бути широко і ясно. Це допоможе розширити сферу стратегічних можливостей і розвитку мислення, визначити правильний напрямок генерації знань; в рамках бачення та цілей основним рушійним фактором організаційного навчання є процес регулярного діалогу, обміну та обговорення.

Організації з єдиним «циклом навчання» визначають себе як «провідні зміни», тобто те, чого вони очікують досягти. Потім вони контролюють та оцінюють переваги та вживають коригуючих дій, якщо це необхідно, завершуючи таким чином «цикл». Якщо елемент управління ініціює дію щодо перегляду «первинних змінних» через необхідність реагування на нові ситуації в системі, то можливий подвійний «цикл навчання». Зовнішнє середовище. Організація отримує нові настанови, засновані на змінах навколишнього середовища, тому вона може визначити шлях досягнення нових цілей. Процес організаційного навчання є основою концепції організації навчання, яка постійно вдосконалюється шляхом створення та розвитку навичок, необхідних для майбутнього успіху. Організація сприяє навчанню та безперервній трансформації всіх своїх кадрів. Вона повинна вміти адаптуватися до умов, що змінюються, і розвивати своїх співробітників. Організації, що навчаються, мають здатність створювати, здобувати та передавати знання, а також здатність змінювати поведінку з урахуванням нових знань та ідей. У ній реалізуються [31]:

– систематичний процес розв'язання проблем на основі концепцій і методів руху підвищення якості. Його основні ідеї: наукова аргументація, заміна припущень у діагностиці проблеми; припущення переваг фактичних даних як основи для прийняття рішень (управління на основі доказів); використання простих статистичних інструментів (гістограм, діаграм Парето та причинно-наслідкових діаграм) Побудувати дані та зробити висновки;

– експериментальна діяльність, що включає систематичні дослідження та перевірку нових знань. План постійного вдосконалення («Кайзер») – важлива особливість організації, що навчається;

– навчання, засноване на минулому досвіді. Організація переглядає успіхи та невдачі, систематично оцінює їх і фіксує отримані уроки таким чином, щоб співробітники могли отримати доступ;

– навчання за рахунок інших - вихід за межі найближчого оточення для отримання нових перспектив часто супроводжується видатним одкровенням («безсовісна крадіжка ідей»). Більш формальна назва цього процесу - «бенчмаркінг» описує організований процес виявлення компаній з «найкращими практиками» та подальшого аналізу можливості копіювання їх дій і внесення деяких модифікацій для внутрішнього використання компанією та доцільності;

– швидко та ефективно поширювати знання по всій організації, підтримуючи людей з новим досвідом або за допомогою освітніх і навчальних програм (якщо вони пов'язані з розкриттям інформації).

Зосередженість на колективному вирішенні внутрішніх проблем всередині організації досягається шляхом використання командного навчання та методів «гнучких систем». Тут розглядаються всі можливі причини проблеми, щоб провести межу між проблемою, яку можна вирішити, і проблемою, яка не може бути вирішена в принципі.

Стратегія управління знаннями. Управління знаннями бере знання як ключовий ресурс і перетворює базу знань ресурсів шляхом визначення

відповідної інформації, а потім обміну нею для стимулювання навчання. Мета полягає в тому, щоб створити потік знань і ще більше прискорити його передачу від організації до її членів.

Стратегія управління знаннями сприяє обміну інформацією через взаємодію між людьми та дає їм можливість отримувати необхідні ресурси. Знання містяться в презентаціях, звітах, базах даних, бібліотеках, організаційних політичних документах та керівних принципах дій. Його можна переміщати по організації за допомогою традиційних методів: зустрічей, робочих груп, курсів, семінарів, публікацій, відео- та аудіоінструментів.

Інтелектуальний капітал складається з «прихованих» активів організації, які можуть бути пов'язані зі споживачами (бренд, лояльність), організацією (експертиза компанії, накопичені знання, комерційні таємниці, системи та методи) та окремими співробітниками (технічні ноу-хау, здібності) Пов'язані, спеціальні навички та навички). Останній становить людський капітал організації, і тут фактично зосереджена кадрова стратегія. Стратегія розвитку інтелектуального капіталу спрямована на максимізацію активів і мінімізацію зобов'язань, яка має базуватися на інформації про наявні можливості та оцінці майбутніх потреб.

Визначаються можливості розвитку здібностей для задоволення майбутніх потреб організації та розробляється стратегія навчання.

Стратегія розвитку менеджменту. Менеджери зосереджуються на довгостроковому підході до підвищення ефективності організації: надають керівникам інформацію про їхні очікування; надають можливість порівняти та оцінити ефективність цілей менеджерів, а також виявити зони невідповідності для підвищення компетентності; дозволяє виявити керівників з певним потенціалом, мотивувати їх до формування та реалізації планів особистісного розвитку, а також забезпечити умови для розвитку, навчання та досвіду для підготовки до більш складних особистих та організаційних

завдань; створити умови для наступності лідерів та створити систему регулювання і контролювати цей процес.

Стратегії розвитку «емоційної культури». Поняття «емоційна культура» включає: здатність усвідомлювати власні почуття та почуття інших; мотивувати себе та інших, керувати власними емоціями та стосунками з іншими. Наявність високого ступеня «емоційної культури» є необхідною якістю для успішних лідерів. «Емоційна культура» має такі складові: 1) Саморегуляція – здатність контролювати чи перенаправляти деструктивні імпульси й емоції та регулювати власну поведінку, а також прагнення досягати цілей позитивно й довговічно; 2) Самосвідомість – здатність розпізнавати і розуміти власні емоції, емоції та мотивації, а також їх вплив на інших; 3) Соціальна орієнтація - здатність розуміти емоції та емоції інших і будувати стосунки з іншими на основі своїх емоційні реакції 4) Соціальні навички – здатність керувати міжособистісними стосунками та будувати мережі для отримання результатів від інших, здатність досягати особистих цілей, здатність знаходити спільну мову та будувати стосунки з іншими.

За сучасних соціально-економічних умов внески до працівників стали довгостроковим фактором конкурентоспроможності та виживання підприємств. Від обраної стратегії розвитку співробітників залежить ефективність кадрової складової успіху компанії. Вибір стратегічних альтернатив має базуватися на порівнянні стратегічних цілей та кінцевих результатів, яких можна досягти шляхом реалізації кожної стратегії.

Для розвитку співробітників компанії дуже важливим є вибір відповідної форми і методу стимулювання праці. Розвиток конкурентоспроможності співробітників – це шлях досягнення корпоративних цілей шляхом зміни кількості та якості працівників, передбачає певну послідовність дій для формування та реалізації відповідних стратегій. Стратегічний аспект розвитку талантів передбачає низку дій для

вибору стратегії конкурентоспроможності корпоративних талантів, включаючи: визначення корпоративної конкурентної стратегії; вибір стратегій конкурентного розвитку для всіх типів працівників, які підтримують корпоративну стратегію; заходи щодо підтримувати конкурентні переваги, зміцнювати конкурентні позиції та Поточні заходи щодо підвищення ефективності роботи співробітників.

1.3 Особливості організації інформаційної безпеки підприємства

За останні десятиліття розвиток інформатизації в глобальному суспільстві викликав нові проблеми глобальної інформаційної безпеки. Багато з найважливіших переваг компанії зараз значною мірою залежать від стану інформаційного середовища. Цілеспрямований або ненавмисний вплив зовнішніх або внутрішніх джерел на інформаційне поле може завдати серйозної шкоди цим інтересам, створювати загрози та ризики для безпеки. Тому інформаційна безпека за сучасних умов є однією з необхідних умов нормальної діяльності підприємств. Загальний рівень корпоративної економічної безпеки все більше залежить від інформаційних компонентів. Практика показала, що будь-яка недружня поведінка, яка завдає шкоди інтересам комерційних структур, починається зі збору інформації: навіть дрібні крадіжки, як правило, передують дослідженню можливості протиправної поведінки осіб із злочинним умислом, без належного інформаційного забезпечення, і не є деструктивним. перенесення проявів. Конфіскація майна підприємства або хижака. Не випадково інформаційна безпека вже давно є першочерговим завданням майже всіх великих компаній. Останнім часом все більше вітчизняних керівників малого та середнього бізнесу почали усвідомлювати реальну небезпеку ризиків, пов'язаних з

внутрішньою інформацією, системою її обробки та співробітниками, залученими до цього процесу.

Поняття інформаційної безпеки можна розглядати з багатьох сторін. Перш за все, це стан захисту соціального інформаційного середовища, забезпечення того, щоб його формування, використання та розвиток відповідали інтересам громадян, організацій та країни. По-друге, це держава, яка захищає інформаційні потреби людини, суспільства, країни, може забезпечити їх існування та поступовий розвиток незалежно від того, чи існують внутрішні та зовнішні інформаційні загрози. Стан свідомості визначає повну ступінь сприйняття навколишньої дійсності суб'єктом, а отже, визначає ефективність подальших рішень і дій. В інформаційному законодавстві інформаційна безпека – це аспект інформаційного законодавства, який розглядає інформаційні відносини з точки зору захисту життєво важливих інтересів особи, суспільства, країни, акцентуючи увагу на загрозах цим інтересам та механізмам усунення чи запобігання цим загрозам з допомогою законних засобів.

З розвитком науки і техніки значення інформаційної безпеки буде ставати все вищим. Інформація стала фактором, який може спричинити великі технологічні аварії, військові та політичні конфлікти, порушити державне управління та фінансові системи. Чим вищий рівень соціального інтелекту та інформатизації, тим надійніша інформаційна безпека. Через інформатизацію все більше реалізується реалізація благ, людей, країни.

Враховуючи, що під впливом інформаційних атак можуть цілеспрямовано змінюватися уявлення і мораль окремих людей і всього суспільства, нав'язувати іншим інтереси, мотиви, спосіб життя інших, характер і форми сучасних методів приховування. бути проаналізованим. Агресія – це прояв поведінки, що має цілеспрямований агресивний характер і порушує інтереси національної безпеки, розробка механізмів комплексної протидії цій поведінці.

Деякі вчені розглядають інформаційну безпеку як стан захисту життєво важливих інтересів особи, суспільства та країни, мінімізації шкоди, заподіяної неповною, несвоєчасною, недостовірною чи негативною інформацією, а також негативного впливу інформаційних технологій, а також як несанкціоноване поширення інформації.

Інформаційна безпека суспільства також визначається як соціальний нагляд, інформаційна інфраструктура та передана через неї інформація, яка не може завдати шкоди його духовній сфері, культурній цінності, поведінці людей. Вчені вважають, що передбачити всі можливі загрози у сфері інформаційної безпеки неможливо, оскільки вони можуть змінювати свій зміст і динаміку, а для правового нагляду необхідна стабільність.

Тому в центрі уваги політики інформаційної безпеки є не пошук відповідей на конкретні загрози, а створення безпечних умов функціонування інформаційного поля, за яких інформаційне поле буде захищене від можливих негативних впливів. Експерти по-різному розуміють термін «інформаційна безпека» і часто звертаються до одного аспекту проблеми.

Наприклад, з точки зору керівника підприємства існує серйозна загроза викрадення конфіденційних файлів, а з точки зору розробника антивірусної програми – ризик пошкодження цінних даних. Кожен з цих аспектів заслуговує на вивчення окремо, але для споживачів важливе забезпечення загальної безпеки, а не лише особистий ризик. Ми вважаємо, що інформаційна безпека компанії включає певні дії, які визначають, усувають та усувають негативні джерела, причини та умови, які впливають на інформацію. При цьому поняття «інформаційна безпека» характеризує статус захисту інформації суб'єктів господарювання, у якому загрози можуть здійснювати дії. Це досягається за допомогою системи заходів, спрямованих на запобігання, виявлення та усунення інформаційних загроз.

Погіршення параметрів корпоративної інформації, таких як конфіденційність, цілісність, доступність, надійність тощо, може призвести

до досить несприятливих наслідків: функціонального збою систем управління процесами та інших ключових систем, розголошення інформації, що становить комерційну та іншу таємницю, порушення, порушення фінансів Надійність файлів, несанкціонований доступ до персональних даних фізичних осіб тощо. Наслідком цього може бути: погіршення ділових відносин з партнерами; переривання переговорів і втрата вигідних контрактів; невиконання договірних зобов'язань; необхідні додаткові дослідження ринку; відмова від рішень, які втратили чинність через поширення інформації, а отже і фінансові втрати, пов'язані з новими розробками; втрачені можливості подавати заявки на отримання патентів або продавати ліцензії на досягнення науково-технічної діяльності; зниження цін або продажів; втрата ділової репутації; посилення умов кредитування; труднощі з постачанням та закупівлею обладнання тощо.

У деяких випадках ігнорування проблем інформаційної безпеки може призвести до повного банкрутства. Тому питання аналізу загроз і ризиків є вирішальними для побудови ефективної системи захисту інформації. Однак, за оцінками експертів, для кількісного аналізу та оптимізації підсистеми інформаційної безпеки власні методи аналізу ризиків використовують менше 5% підприємств. При цьому поведінка внутрішніх порушників, як-от халатність співробітників, крадіжка інформаційних ресурсів та ІТ-обладнання, фінансові та інші шахрайства при використанні інформаційних систем і ресурсів, рідко згадуються при вирішенні питань інформаційної безпеки. Розглядається окремо від загальної мети економічної безпеки.

Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, адже більшість нещасних випадків відбувається з вини працівників. Навмисні відтоки часто важко відрізнити від ненавмисних, але це не завжди є необхідним, оскільки в будь-якому з цих варіантів наслідки для компанії можуть бути катастрофічними. Більшість керівників не знають джерела внутрішніх загроз, що свідчить про те, що підприємства недостатньо

уваги приділяють інформаційній безпеці, а інформаційна безпека є одним із найважливіших факторів існування підприємств.

Аналіз, проведений у компанії середнього розміру, показує, що випадкові кібератаки відбуваються частіше і можуть завдати більшої шкоди, ніж навмисні інсайдерські атаки. Дослідження показали, що більшість компаній приділяють більше уваги запобіганню навмисних внутрішніх атак, ніж випадковим внутрішнім подіям, які є більш частими і потенційно більш руйнівними. Ігноруйте потенційні внутрішні ризики співробітників, які мають доступ до критичних систем і конфіденційної інформації. Хоча менеджери усвідомлюють пов'язані з цим ризики, побоювання щодо зовнішньої інформаційної безпеки часто переважають інші проблеми. Проте є велика кількість випадків порушень та несанкціонованого доступу та використання інформації працівниками, що загрожує основ бізнесу багатьох компаній. Серед 500 опитаних ІТ-менеджерів більшість сказали, що не знають джерела та причини інсайдерських загроз. При цьому компанія намагається оцінити потенційні фінансові збитки від цих загроз та їх вплив на підприємницьку діяльність.

Половина респондентів вважає, що більшість інсайдерських загроз спричинені ненавмисно, 20% вважають, що погрози є навмисними, 25% вважають, що навмисні та ненавмисні погрози приблизно однакові, а 5% вважають, що з ними важко впоратися. Однак, коли йдеться про важливість переліку найбільших загроз, майже 85% респондентів не змогли визначити, чи були навмисні чи ненавмисні внутрішні інциденти, спричинені підрядниками чи тимчасовими працівниками. Дослідження також виявило, що приблизно раз на місяць на підприємстві відбувається інцидент, який можна віднести до одного з 10 можливих типів загроз. Більшість випадків випадкової втрати даних через халатність співробітників – такі випадки трапляються 15-20 разів на рік. Внутрішні шкідливі атаки та шпигунство – 10 випадків на рік, зловживання доступу до інформації – 20 випадків на рік.

Якщо говорити про сферу діяльності, то в опитаних компаніях щорічно трапляється 20-30 інцидентів. Результати дослідження показують, що універсального рішення для усунення внутрішніх ризиків не існує. Кожна компанія повинна розробити власний комплексний підхід, враховуючи структуру та деталі діяльності. Хоча навмисних нападів з боку злочинців стає все більше, практика показує, що випадкові помилки та неувага до правил безпеки мають набагато більший вплив на корпоративну діяльність, ніж шахрайські атаки. Експерти з інформаційної безпеки дотримуються двох точок зору. Перше: інформаційна безпека підприємства просто не закріплена, і це не коштує грошей. У цьому випадку можна повністю виправдати ризик. Друга точка зору: потрібні великі кошти (навчання персоналу, програмне забезпечення тощо), щоб створити систему інформаційної безпеки для забезпечення належного рівня безпеки.

Але також будуть певні лазівки, які рано чи пізно призведуть до витоку чи крадіжки конфіденційної інформації. Для обґрунтування витрат на інформаційну безпеку можна використовувати наступні методи. Необхідно застосовувати інструменти визначення рівня інформаційної безпеки на практиці.

Керівництво компанії бере участь в оцінці вартості інформаційних ресурсів та визначенні оцінки потенційних збитків, завданих порушенням інформаційної безпеки. Від результатів цих оцінок багато в чому залежатиме подальша діяльність менеджерів у сфері інформаційної безпеки.

Якщо інформація нікчемна, не несе серйозної загрози інформаційним активам, а потенційна шкода невелика, то проблему інформаційної безпеки вирішити неможливо. Якщо вартість інформації висока, а загроза та потенційна шкода зрозумілі, то виникне проблема включення до бюджету вартості підсистеми інформаційної безпеки. У цьому випадку слід звернутися за підтримкою до керівництва компанії, розібратися в проблемах інформаційної безпеки, створити систему інформаційної безпеки.

Тільки на основі формування ефективної системи забезпечення інформаційної безпеки можна надійно захистити бізнес від перерахованих негативних явищ. Однак деякі проблеми, ймовірно, стосуються організації та фінансів. Першою і найбільшою проблемою створення системи інформаційної безпеки є нерозуміння необхідності створення такої системи. Багато керівників бізнесу не усвідомлюють, що створення системи інформаційної безпеки є дуже потрібним, адже своєчасне встановлення може врятувати збитки компанії, а іноді навіть врятувати підприємство. Другою проблемою створення системи інформаційної безпеки є відсутність достатніх коштів.

Третім найбільш небезпечним питанням є ситуація, коли створення системи інформаційної безпеки довіряють фахівцям, які не мають ні належної освіти, ні достатнього досвіду, коли є розуміння керівництва та необхідні кошти. Зазвичай це системні адміністратори або співробітники технічної підтримки. У свою чергу, вони розглядають це як встановлення та налаштування антивірусного програмного забезпечення. Зазвичай наявність інсайдерських зловмисників взагалі не враховується. За статистикою, 70% порушень здійснюють внутрішні зловмисники. Частіше каналам комунікації не приділяється належної уваги, а комунікації між керівництвом компанії та діловими партнерами та клієнтами не захищені. В результаті таких дій кошти витрачені, інформаційна безпека на тому ж рівні. У системі інформаційної безпеки багато керівників бізнесу можуть не бачити чіткого зв'язку між втраченим доходом і браком фінансових ресурсів. Тому спочатку проблему потрібно викласти у діловій формі. Це завдання покладається на службу інформаційної безпеки суб'єкта господарювання, яка має визначити та чітко відобразити власників усього спектру загроз в інформаційному полі та переконати їх, що лише на основі створення вони можуть протистояти та впроваджувати ефективну інформацію. система безпеки.

Створюючи таку систему, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів необхідно багато різних заходів, які можна поділити на три категорії: право, організація, економіка та технологія. По-друге, хоча для досягнення поставлених цілей ці три групи діяльності мають здійснювати експерти у відповідних галузях знань із застосуванням власних методів і технологій, кінцевий успіх значною мірою залежить від системного підходу до визначення та впровадження відповідних визначень, принципів, і методи і зв'язок між механізмами захисту.

Аналіз точок зору та концептуальних методів, що формують сучасну та ефективну систему інформаційної безпеки підприємства, дозволяє сформулювати основні функції та завдання та окреслити організаційні основи функціонування відділів, пов'язаних із інформаційною безпекою.

У сучасному уявленні про роль і функції служб інформаційної безпеки можна виділити чотири напрями: розробка методологій і методів аналізу загроз, оцінка рівня інформаційної безпеки підприємства та системи його обслуговування; організація та здійснення спеціальних заходів із захисту інформації; експлуатація технічних засобів захисту інформації Аудит і контроль системи інформаційної безпеки підприємства.

Перший напрям має вирішувати такі основні завдання: аналіз та узагальнення потенційних загроз та реалізованих загроз, а також причин порушення вимог інформаційної безпеки. Проаналізувати ступінь безперервності бізнес-процесів з використанням ІТ з точки зору інформаційної безпеки. Пошук нових загроз і вразливостей, пов'язаних з інформаційною взаємодією, побудова методів оцінки інформаційних ризиків, дослідження інформації підприємства та інформаційних ресурсів, розробка методів захисту інформації та ІТ та методів їх впровадження на підприємствах, розробка та модифікація концепцій і політик інформаційної безпеки.

Враховуючи комплексний підхід до економічної безпеки, створити локальну нормативну базу з цих питань; розробити методи оцінки рівня інформаційної безпеки та визначення адекватності захисту інформації та ІТ з урахуванням потреб бізнесу та існуючої та майбутньої нормативної бази; проаналізувати всі методи, які використовуються для створення, чи відповідають процедури обробки, надсилання, зберігання та знищення інформації вимогам інформаційної безпеки, зокрема: процедури обміну інформацією між різними підрозділами підприємства та зовнішніми організаціями; процедури доступу співробітників підприємств і пов'язаних з ними організацій і замовників; проекти розвитку ІТ, у тому числі телекомунікаційних і телекомунікаційних систем; угоди із зовнішніми організаціями щодо обміну інформацією Проект надавати проекти інших нормативних документів для обміну інформацією, готувати інструкції з аналізу, які містять висновки аналізу та рекомендації щодо впровадження інформаційної безпеки.

Другий напрям передбачає виконання таких основних завдань: планування забезпечення інформаційної безпеки підприємства на основі координації діяльності різних підрозділів, організація та участь у впровадженні методів інформаційної безпеки підприємства. Співпраця з співробітниками, партнерами та клієнтами, координація програм доступу співробітників і зовнішніх організацій і послідовності доступу до корпоративних інформаційних ресурсів; процедури обміну інформацією між відділом та зовнішніми організаціями, угоди про обмін інформацією, складання наказів, інструкцій та інших нормативно-розпорядчих документів, вирішення актуальних проблем інформаційної безпеки в поточному відділі.

Третій напрям має вирішувати такі основні завдання: підтримка ключової структури зовнішніх і вбудованих засобів захисту шифрування інформації, підтримка інших засобів захисту інформації.

Четвертий напрям передбачає вирішення таких основних завдань: перевірка відповідності корпоративним та іншим персоналом доступу до інформаційних ресурсів вимогам інформаційної безпеки; моніторинг поведінки користувачів ІТ (несанкціонована зміна інформації, використання різноманітних поштових та інших Інтернет-сервісів для розсилання конфіденційної інформації за межі компанії тощо); контроль за своєчасною зміною дозволів користувачів в інформаційній системі; запобігання звільненню (переміщенню в іншу) облікових записів користувачів робота); стежити за безпекою; відповідність налаштувань, включаючи політику паролів, інші вбудовані системи інформаційної безпеки, зовнішні засоби захисту інформації, моніторинг роботи систем виявлення (попередження) мережових атак, систем оцінки якості мережі та інших автоматизованих систем комп'ютерної безпеки, участь в аналізі виявлених порушень інформаційної безпеки та нормативних вимог. Готувати пропозиції щодо запобігання порушенням, проводити внутрішні перевірки з питань інформаційної безпеки. Будьте готові використати рекомендації зовнішніх аудитів; відстежуйте конфіденційну інформацію, яка може бути просочена через технічні канали.

Враховуючи міждисциплінарний характер питань, що містяться в підрозділі інформаційної безпеки, деякі з цих функцій можуть виконуватися лише в поєднанні з іншими структурованими службами підприємства (кадрові служби, юридичні, бізнес-послуги тощо). З цією метою необхідно визначити стратегію безпеки компанії - набір принципів, правил, процедур і практик з інформаційної безпеки для управління управлінням, захистом і розповсюдженням цінної інформації в компанії. Загалом, такий набір правил становить певні функції, необхідні для використання програмного продукту в конкретній організації. Якщо розглядати політику безпеки більш формально, то це набір конкретних вимог до функціональності системи безпеки, що містяться у відомчих документах. Основною причиною виникнення політик

безпеки зазвичай є вимоги організації до таких документів, що визначає правила роботи підприємств галузі. У цьому випадку відсутність політики може призвести до репресивних дій проти компанії або навіть до повного припинення її діяльності. Крім того, певні вимоги та рекомендації встановлюють галузеві або загальні, місцеві чи міжнародні стандарти.

Зазвичай це виражається у вигляді коментарів зовнішнього аудитора, який перевіряє компанію. Відсутність політики призводить до негативних відгуків, що, у свою чергу, впливає на громадську діяльність компанії – її позицію в рейтингу, рівень надійності тощо. Далі очевидно, наскільки серйозний втрата принесе компанії інформаційний ризик щодо кожного конкретного інформаційного об'єкта.

Варіантів розрахунку ризику багато, але на найпростіший варто звернути увагу. Збитки, спричинені настанням інформаційних ризиків, наведені в таблиці 1.2.

Таблиця 1.2 – Втрати від настання інформаційного ризику

Величина ризику	Опис
0,1 – 0,2	Оголошення інформації принесе незначні моральні і фінансові втрати підприємству
0,2 – 0,3	Втрати від інформаційної атаки є, але вони незначні, основні фінансові операції і стан підприємства на ринку не порушено
0,3 – 0,4	Фінансові операції не ведуться протягом деякого часу, підприємство зазнає збитків, але його стан кількість клієнтів змінюються мінімально
0,4 – 0,6	Значні втрати на ринку й у прибутку. Підприємство втрачає значну частину клієнтів
0,6 – 0,8	Втрати дуже значні, підприємство на період до року втрачає можливості для відновлення

Слід зазначити, що класифікацію шкоди, заподіяної атакою, повинен оцінювати власник інформації або персонал, який її використовує. Оцініть Імовірність атаки ще залежить від технічного персоналу підприємства.

З різних організаційних схем, якими керують різні відділи відповідає за інформаційну безпеку підприємства (функції підрозділу покладені на системного адміністратора, а підрозділ належить до структури служби

інформаційної безпеки та підпорядковується вищому рівню). служби економічної безпеки.

У цьому випадку найкраща можливість вирішення питань інформаційної безпеки створюється в контексті загальних завдань безпеки бізнесу. на закінчення. Тому в сучасних умовах інформаційна безпека є невід'ємною частиною корпоративної системи безпеки реальної економіки.

І навпаки, надійна інформаційна безпека є не лише окремого підприємства, а й передумовою переходу всієї національної економіки до моделі сталого розвитку. Особливу увагу слід приділяти реальній реалізації запропонованих заходів інформаційної безпеки, що має стати основою для формування та реалізації інформаційної політики підприємствами та захисту інформації від внутрішніх та зовнішніх загроз.

2 АНАЛІЗ ПОКАЗНИКІВ ДІЯЛЬНОСТІ ТА НАПРЯМІВ ОРГАНІЗАЦІЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТОВ «КАСПЕР»

2.1 Характеристика фінансово-економічних результатів діяльності підприємства

ТОВ «Каспер» заснована в 1991 році. На даний момент в компанії працює понад 100 співробітників.

Метою діяльності ТОВ «Каспер» є задоволення інтересів та вимог споживачів щодо якості та найменування продукції, термінів доставки та супроводу фінансово-економічних програмних продуктів компанії.

Основний бізнес ТОВ «Каспер» – постачання програмного, фінансово-економічного програмного забезпечення ERP-систем, розробка та налаштування сторонніх програм.

На рис. 2.1 наведена організаційна структура підприємства.

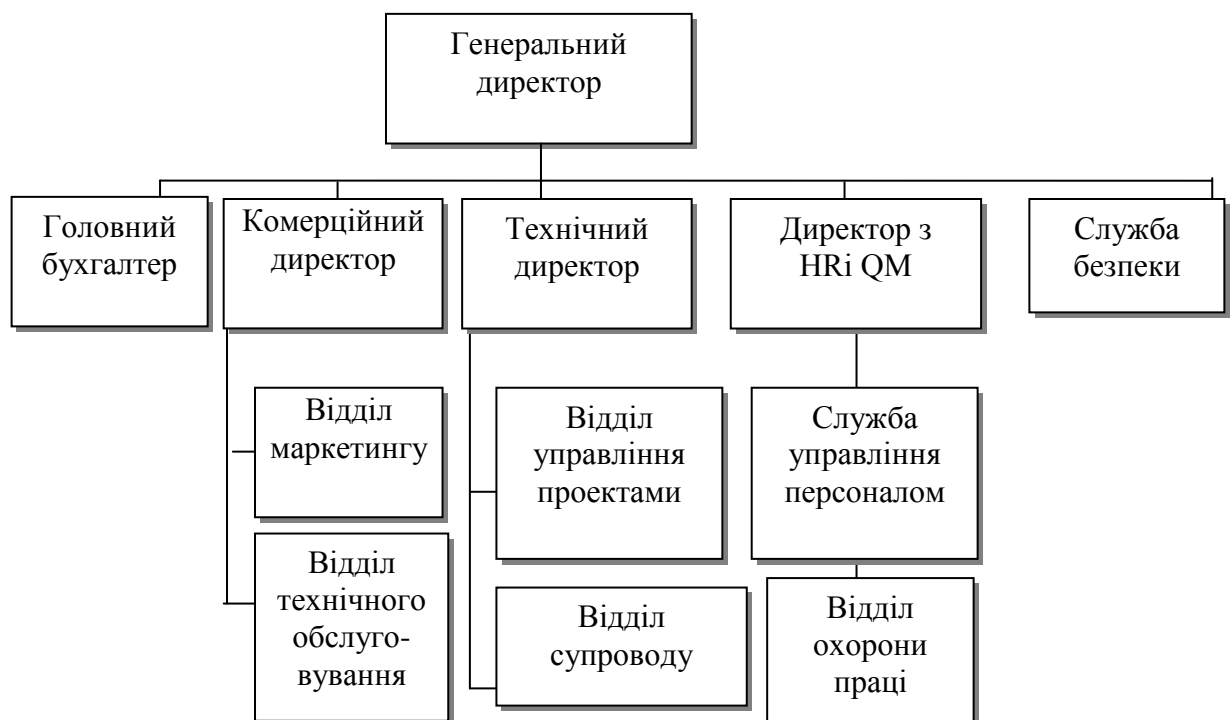


Рисунок 2.1 – Організаційна структура ТОВ «Каспер»

Фінансово-економічні результати діяльності підприємства відображені у таблиці 2.1.

Таблиця 2.1 – Структура майна підприємства та джерел його формування

Показник	Значення показника				Змінення	
	2019		2020		(гр.4- гр.2), грн.	(гр.4 : гр.2), %
	в грн.	в % до валюти балансу	в грн.	в % до валюти балансу		
Актив						
1. Імобілізовані кошти	336362	19,8	346647	18,6	10285	3,1
2. Оборотні активи, у загалі	1362347	80,2	1514819	81,4	152472	11,2
У тому числі: запаси (крім товарів відвантажених)	850180	50	904724	48,6	54544	6,4
в тому числі: - сировина і матеріали;	185627	10,9	171667	9,2	-13960	-7,5
- готова продукція (товари).	34013	2	30180	1,6	-3833	-11,3
витрати в незавершеному виробництві (витратах звернення) та витрати майбутніх періодів;	630540	37,1	698277	37,5	67737	10,7
ПДВ по придбаних цінностей	79536	4,7	89492	4,8	9956	12,5
ліквідні активи, всього	432631	25,5	520603	28	87972	20,3
з них: - кошти й короткострокові вкладення;	73317	4,3	54776	2,9	-18541	-25,3
- дебіторська заборгованість (термін платежу за якою не більше року);	358955	21,1	465507	25	106552	29,7
- товари відвантажені.	359	<0,1	320	<0,1	-39	-10,9
Пасив						
1. Власний капітал	453316	26,7	497642	26,7	44326	9,8
2. Позиковий капітал, всього	645264	38	684562	36,8	39298	6,1
з них: - довгострокові кредити і позики;	35270	2,1	38829	2,1	3559	10,1
- короткострокові кредити і позики.	609994	35,9	645733	34,7	35739	5,9
3. Залучений капітал	600129	35,3	679262	36,5	79133	13,2
Валюта балансу	1698709	100	1861466	100	162757	9,6

Активи організації на останній день аналізованого періоду мають такі характеристики: 18,6% основних фондів і 81,4% оборотних активів. Активи організації за аналізований період зросли на 162 757 грн. (9,6%). При цьому власний капітал організації майже пропорційний активам організації, збільшившись на 44 326 грн.

Збільшення вартості активів організації в основному пов'язане зі зростанням таких статей балансу (у дужках вказана частка змін цієї статті в загальній сумі всіх позитивних змін):

- дебіторська заборгованість (очікується до оплати протягом 12 місяців після звітної дати) – 106 552 грн. (44,3%);
- основні засоби – 45768 грн. (19%);

При цьому серед зобов'язань балансу найбільше приріст спостерігався у таких рядках:

- кредиторська заборгованість: інші кредитори – 118062 грн. (57,3%);
- нерозподілений прибуток (непокриті збитки) – 44474 грн. (21,6%);
- позики та кредити – 35739 грн. (17,3%).

До статей балансу з від'ємними змінами входять кредиторська заборгованість: податкова заборгованість у зобов'язаннях (40215 грн.).

Крім того, в таблиці 2.2 відображено оцінку собівартості чистих активів, а також аналізуються зміни в діяльності, а результати розрахунку відображаються у відсотках.

Таблиця 2.2 – Оцінка вартості чистих активів організації

Показник	Значення показника				змінення	
	2019		2020		грн. (гр.4- гр.2)	± % ((4-2) : 2)
	в грн.	в % до валюти балансу	в грн.	в % до валюти балансу		
1	2	3	4	5	6	7
1. Чисті активи	453316	26,7	497642	26,7	44326	9,8
2. Статутний капітал	294034	17,3	294034	15,8	–	–
3. Перевищення чистих активів над статутним капіталом	159282	9,4	203608	10,9	44326	27,8

Чисті активи цієї установи на останній день звітного періоду значно (69,2%) перевищували статутний капітал. Цей коефіцієнт активно характеризує фінансовий стан і повністю відповідає вимогам нормативних

документів щодо вартості чистих активів організації. Крім того, для визначення поточного стану показників слід зазначити, що за аналізований період чисті активи зросли на 9,8%. Враховуючи перевищення чистих активів над юридичним капіталом та його збільшення за цей період, можна говорити про хороший фінансовий стан організації за цією ознакою.

Оскільки обидва коефіцієнти були нижчими за норму, то як третій показник було розраховано коефіцієнт відновлення платоспроможності. Далі в таблиці 2.3 наведено визначення незадовільної структури балансу.

Таблиця 2.3 – Визначення незадовільної структури балансу

Показник	Значення показника		Змінення (гр.3- гр.2)	Нормативне значення	Відповідність фактичного значення нормативному на кінець періоду
	2019	2020			
1. Коефіцієнт поточної ліквідності	1,13	1,14	0,01	не менше 2	не відповідає
2. Коефіцієнт забезпеченості власними коштами	0,09	0,1	0,01	не менше 0,1	не відповідає
3. Коефіцієнт відновлення	x	1,14	x	не менше 1	відповідає

Цей коефіцієнт використовується для оцінки шестимісячної перспективи повернення до нормальної структури балансу (платоспроможності) при збереженні ліквідності та збереження власних коштів протягом аналізованого періоду. Значення коефіцієнта відновлення платоспроможності вказує на реальну можливість повернення до нормальної платоспроможності найближчим часом.

Очевидні зміни вартості чистих активів показані на рис. 2.2.

Основні показники фінансової стійкості організації приведені в таблиці 2.4.

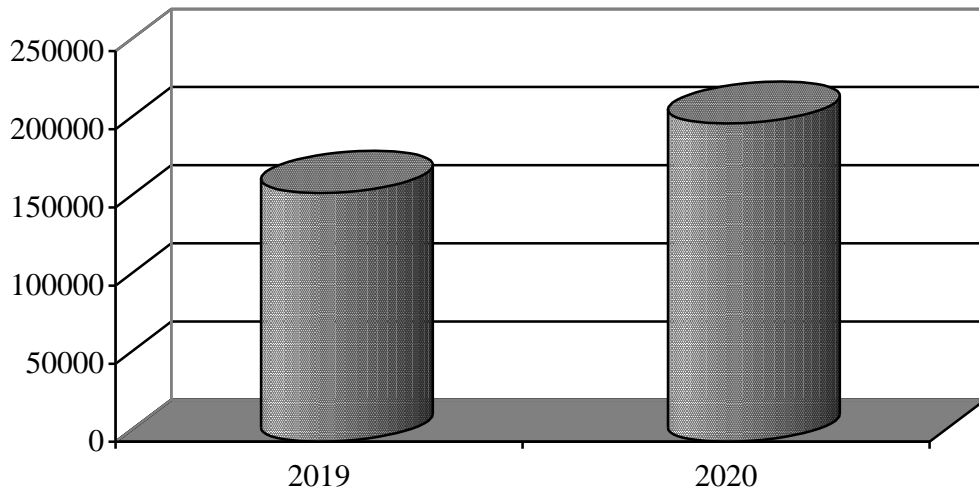


Рисунок 2.2 – Зміна вартості чистих активів над уставним капіталом, тис. грн

Таблиця 2.4 – Аналіз фінансової стійкості за величиною надлишку (нестачі) власних оборотних коштів

Показник власних оборотних засобів (ВОЗ)	2019		2020	
	Значення показника	Надлишок (брак)	Значення показника	Надлишок (брак)
ВОЗ ₁ (розрахований без урахування довгострокових і короткострокових пасивів)	117953	-732586	151994	-753050
ВОЗ ₂ (розрахований з урахуванням довгострокових пасивів)	153223	-697316	190823	-714221
ВОЗ ₃ (розрахований з урахуванням і довгострокових, і короткострокових пасивів)	1362347	511808	1514819	609775

Оскільки тільки три варіанти розрахунку покриття запасів і витрат на оборотний капітал мають позитивне значення в останньому варіанті, фінансове становище організації можна охарактеризувати як нестабільне. Слід зазначити, що протягом аналізованого періоду два з трьох показників власних оборотних коштів та собівартості погіршилися. Інші показники, що відображають фінансову стійкість ТОВ «Каспер», наведені в таблиці 2.5.

Таблиця 2.5 – Аналіз інших показників фінансової стійкості організації

Показник	Значення показника		Змінення показника (3-2)	Опис показника і його нормативне значення
	2019	2020		
1. Коефіцієнт автономії	0,27	0,27	<0,01	Відношення власного капіталу до загальної суми капіталу. Рекомендоване значення: >0,5 (звичайно 0,6-0,7)
2. Коефіцієнт відношення позикових і власних коштів	2,75	2,74	-0,01	Відношення позикового капіталу до власного. Оптимальне значення: 1
3. Коефіцієнт покриття інвестицій	0,29	0,29	<0,01	Відношення власного капіталу і довгострокових зобов'язань до загальної суми капіталу. Нормальне значення у світовій практиці: ок. 0,9; критичне - <0,75.
4. Коефіцієнт маневреності власного капіталу	0,31	0,36	0,04	Відношення власних оборотних коштів до джерел власних і довгострокових позикових коштів. Ставлення має бути, як мінімум, позитивне
5. Коефіцієнт мобільності оборотних коштів	0,8	0,81	0,01	Відношення оборотних коштів до вартості всього майна
6. Коефіцієнт забезпеченості матеріальних запасів	0,18	0,21	0,03	Відношення власних оборотних коштів до величини матеріально-виробничих запасів
7. Коефіцієнт забезпеченості поточних активів	0,11	0,13	0,01	Відношення власних оборотних коштів до поточних активів. Нормативне значення: не нижче 0,1
8. Коефіцієнт короткострокової заборгованості	0,97	0,97	<0,01	Ставлення короткострокової заборгованості до суми загальної заборгованості.

Коефіцієнт автономії становив 0,27. Цей коефіцієнт характеризує, якою мірою організація спирається на позиковий капітал. Отримане тут значення свідчить про те, що частка власного капіталу в загальному капіталі ТОВ «Каспер» надзвичайно мала (27%).

Значення коефіцієнта покриття інвестицій на кінець періоду становило 0,29, що було значно нижче допустимого значення (власний капітал і довгострокові зобов'язання становили лише 29% загального капіталу).

Коефіцієнт працездатності власного капіталу показує, яка частина власних коштів організації перебуває в ліквідному стані, щоб цими коштами можна було користуватися відносно вільно. Значення коефіцієнта власного капіталу становило 0,36. Вважається, що характеристикою добре організованої фінансової стабільності є значення в межах 0,5-0,6. Однак на практиці стандарт для цього показника не визначено, оскільки він значною мірою залежить від сфери діяльності організації.

Кінцеве значення коефіцієнта запасів (0,21) свідчить про те, що запаси не мають достатньої кількості власних оборотних коштів організації для забезпечення.

Коефіцієнт короткострокової заборгованості показує, що вартість короткострокової кредиторської заборгованості значно перевищує вартість довгострокової заборгованості (97% і 3% відповідно).

З чотирьох коефіцієнтів, які характеризують коефіцієнти активів на основі ліквідності та боргів за датою погашення, два задовольняються. ТОВ «Каспер» не має достатньо коштів та короткострокових фінансових вкладень (високоліквідних активів) для погашення найактуальніших боргів (різниця становить 613927 грн.). Відповідно до принципу оптимізації структури активів на ліквідність, короткострокова дебіторська заборгованість повинна бути достатньою для покриття середньострокових зобов'язань. У цьому випадку цей коефіцієнт не виконується – короткострокова дебіторська заборгованість становить лише 71% середньострокових зобов'язань організації. У таблиці 2.6 наведено аналіз коефіцієнта активів.

Коефіцієнт поточної, швидкої, абсолютної ліквідності, розраховані у таблиці 2.7, таких у цій таблиці відображено змінення цих показників.

Коефіцієнт поточної (загальної) ліквідності не відповідав специфікації (1,14 проти 2,0 і вище). Слід зазначити, що спостерігається позитивна динаміка – за період аналізу коефіцієнт збільшився на 0,02.

Таблиця 2.6 – Аналіз співвідношення активів за ступенем ліквідності і зобов'язань за строком погашення

Активи за ступенем ліквідності	На кінець звітного періоду, грн.	Приріст з поч. року, %	Норм. співвідношення	Пасиви за строком погашення	На кінець звітного періоду, грн.	Приріст з поч. року, %	Надлишок/недолік платіж. коштів грн., (гр.6 - гр.3)
A1. Високоліквідні активи (грош кошти короткострокові фін. вкладення)	54776	-25,3	>=	П1. Найбільш термінові зобов'язання (залучені кошти) (поточн.кред. заборг.)	668703	13	-613927
A2. Швидко реалізованих активи (короткострокова дебіторська заборгованість)	465507	29,7	>=	П2. Середньострокові зобов'язання (короткостр. кредити і позики)	655293	6,1	-189786
A3. Повільно реалізованих активів (довгострокових. деб. заборг. Інші оборот. Активи - РБП - ПДВ)	897238	6,1	>=	П3. Довгострокові зобов'язання	38829	10,1	858409
A4. Важкореалізовані активи (необоротні активи)	346647	3,1	<=	П4. Постійні пасиви (власний капітал-РБП - ПДВ до заліку)	401343	8,6	-54696

Таблиця 2.7 – Розрахунок коефіцієнтів ліквідності

Показник	Значення показника		зміна показника (гр.3 - гр.2)	Розрахунок, рекомендоване значення
	2019	2020		
1. Коефіцієнт поточної (загальної) ліквідності	1,13	1,14	0,02	Відношення поточних активів до короткострокових зобов'язань. Рекомендоване значення: > 2,0
2. Коефіцієнт швидкої (проміжної) ліквідності	0,36	0,39	0,04	Відношення ліквідних активів до короткострокових зобов'язань. Рекомендоване значення: > 1,0
3. Коефіцієнт абсолютної ліквідності	0,06	0,04	-0,02	Відношення високоліквідних активів до короткострокових зобов'язань. Рекомендоване значення: > 0,2

Для швидкого співвідношення нормативне значення вище 1,0. У цьому випадку його значення дорівнює 0,39. Це свідчить про те, що ТОВ «Каспер» не має ліквідних активів для погашення найбільш термінових боргів.

Коли коефіцієнт дорівнює 0,2 або вище, значення коефіцієнта абсолютної ліквідності дорівнює 0,04. Крім того, слід звернути увагу на негативну динаміку показника – за період аналізу коефіцієнт знизився на 0,02.

Згідно зі Звітом про фінансові результати за аналізований період організація отримала 122223 грн від реалізації, що еквівалентно 13% виручки. Порівняно з відповідним періодом минулого року прибуток зменшився на 28577 грн., або на 19%.

Порівняно з попереднім періодом дохід від продажів і щоденні витрати на діяльність зросли за цей період (зросли на 229041 грн. та 257618 грн. відповідно). Крім того, у відсотковому вираженні зміна витрат (45,8%) випереджає зміну доходу (32,1%)

Основні фінансові показники ТОВ «Каспер» за період аналізу наведено в таблиці 2.8.

Таблиця 2.8 – Основні фінансові результати

Показник	Значення показника, грн.		Зміна показника	
	2020	2019	грн. (гр.2 - гр.3)	± % (((2-3) : 3)
1. Виручка від реалізації продукції, робіт, послуг	942063	713022	229041	32,1
2. Прибуток (збиток) від реалізації	122223	150800	-28577	-19
3. Чистий прибуток (збиток) звітного періоду	44974	38774	6200	16

Аналіз зміни індексу чистого прибутку дозволив зробити висновок, що організація використала чистий прибуток у розмірі 500 тис. грн у 2020 році.

2.2 Аналіз показників рентабельності

Протягом періоду аналізу організація отримує прибуток від продажів та загальної фінансово-господарської діяльності, в результаті чого всі три показники прибутку, наведені в таблиці, є позитивними.

Результати розрахунку індексу прибутку наведені в таблиці 2.9.

Таблиця 2.9 – Показники рентабельності

Показник рентабельності	Значення показника (в копійках)		зміна, (гр.2 - гр.3)
	2020	2019	
1. Величина прибутку від продажів на кожну гривню, вкладену у виробництво і реалізацію продукції (робіт, послуг)	14,9	26,8	-11,9
2. Величина прибутку від продажів в кожній гривні виручки від реалізації (рентабельність продажів)	13	21,1	-8,1
3. Величина прибутку до оподаткування на рубль усіх витрат організації	3,8	5,7	-1,9

Рентабельність, розрахована як відношення прибутку до оподаткування до загальних витрат організації, становить 3,8%. Тобто з кожної гривні, витраченої на фінансово-господарську діяльність ТОВ «Каспер» за аналізований період, отримують 3,8 коп. прибуток. У цьому ж періоді також отримано прибуток, але він становив 1,9 коп.

Далі в таблиці 2.10 наведено три основні показники, які характеризують рентабельність капітальних вкладень у підприємницьку діяльність.

За аналізований період кожна гривня, вкладена в основні засоби та товарно-матеріальні цінності в ТОВ «Каспер», принесла прибуток від продажів у розмірі 0,11 грн.

Таблиця 2.10 – Рентабельність вкладеного у підприємницьку діяльність капіталу

Показник рентабельності	Значення показника у звітному періоді, %	Розрахунок показника
Рентабельність виробничих засобів	10,8	Відношення прибутку від продажів до середньорічної вартості основних засобів та матеріально-виробничих запасів
Рентабельність активів	2,5	Відношення чистого прибутку до середньорічної вартості активів
Рентабельність власного капіталу	9,5	Відношення чистого прибутку до середньорічної величини власного капіталу

Результатом позитивної характеристики організації є наступні показники – кінцевий прибуток складає велику частку (2,5%) від загальної вартості активів організації.

Фінансовий стан та показники діяльності організації з нормальними або близькими до нормальних величинами:

- коефіцієнт працездатності власного капіталу має задовільне значення (0,36);

- недотримання в повному обсязі нормального співвідношення активів, класифікованих за ступенем ліквідності, та зобов'язань, класифікованих за строками погашення;

- протягом звітного періоду отримано прибуток від реалізації (122223 грн.), але спостерігається негативна динаміка порівняно з попереднім періодом (-28 577 грн.).

Основними показниками фінансового стану організації є:

- висока залежність організації від позикових коштів (власний капітал становить лише 27%);

- коефіцієнт покриття інвестицій значно нижчий за нормальний (власний капітал та довгострокові зобов'язання становлять лише 29% загального капіталу ТОВ «Каспер», критичне значення – 75%);

– коефіцієнт швидкої (проміжної) ліквідності значно нижчий за нормальний;

– коефіцієнт абсолютної ліквідності значно нижчий за нормальний.

Фінансовий стан ТОВ «Каспер» був незадовільним. Враховуючи важливість ключових показників у діапазоні від -2 (критичне значення) до 2 (ідеальне значення), розрахована середня оцінка становить -0,86. Це означає, що в середньому значення показника стану організації не відповідає вимогам.

2.3 Організація діяльності фахівців з економічної безпеки

Система економічної безпеки підприємства, як і будь-яка система, – це сукупність взаємопов'язаних елементів, що забезпечують безпеку діяльності підприємства та реалізацію його бізнес-цілей (прибутку). Система економічної безпеки:

– розробка, трансформація та реалізація концепцій, стратегій і тактик у сфері безпеки шляхом скоординованої діяльності державних та недержавних інституцій;

– набір єдиних управлінських інститутів, сил і методів, призначених для вирішення завдань національної безпеки.

Слід розрізняти систему економічної безпеки підприємства та систему гарантій безпеки підприємства. Перша – функціональна система, що відображає процес взаємодії інтересів і загроз, друга – організаційна система інститутів, сил (суб'єктів безпеки), інструментів та різноманітних організацій, призначених для вирішення проблем організаційної безпеки.

Методологія забезпечення економічної безпеки підприємства визначається системою функціональної безпеки, її не слід плутати з

системою безпеки – організаційною системою. Ці системи мають різні цільові функції. Система безпеки – це теоретичний метод і практичний метод дії, який найбільш повно може захистити життєво важливі інтереси соціальної системи від внутрішніх і зовнішніх загроз. Система безпеки формується теоріями, методами, інструментами та механізмами, що реалізують функції безпеки в соціальній системі, і спрямована на захист її інтересів від загроз цих інтересів. Чи зможе система безпеки захищати інтереси самої соціальної системи, а також здатність захищати інтереси, права і волю людей як членів суспільства, залежить від установки та змісту складових елементів системи безпеки.

Система безпеки – це перш за все функціональна система. Він відображає процес взаємодії інтересів і загроз. Ядром системи є категорія цінних паперів і відсотків. З такого розуміння функціональної системи закономірно випливає розуміння сутності економічної безпеки підприємства, тобто захисту його життєво важливих інтересів. Особливістю функціональної системи є методологія теоретичного методу вирішення проблеми безпеки об'єкта, останнього - розуміння сутності системи безпеки. Іншими словами, яка методологія і методи того, що вважається об'єктом охорони, і як розуміти сам захист. У теорії економічної безпеки суб'єктів господарювання визнано, що виділяють основні характеристики методу, функції та принципи системи забезпечення економічної безпеки підприємства.

Основними методологічними характеристиками системи безпеки підприємства є: унікальність, незалежність та відокремленість від подібних систем інших виробничих підрозділів. Система економічної безпеки суб'єкта господарювання повинна виконувати основні функції: прогнозувати, виявляти, запобігати, пом'якшувати ризики та загрози, забезпечувати безпеку організації та її працівників, охороняти майно, створювати сприятливе конкурентне середовище, усувати наслідки та шкоду тощо.

Основними принципами побудови організаційної системи безпеки є: комплексність або системність, безперервність, легітимність, планування,

ощадливість, інтерактивність, поєднання відкритості та конфіденційності та спроможності. Можна бути впевненим, що забезпечення економічної безпеки суб'єктів господарювання є безперервним процесом, який визначається зовнішніми та внутрішніми умовами та наявністю ворожих чи нейтрально-ворожих факторів середовища, пов'язаних із ризиками, загрози та небезпеки здійснюються від моменту прийняття рішення про створення компанії до ліквідації, з метою створення найкращих умов для функціонування та розвитку компанії через її систему безпеки. Організація та функціонування системи гарантування економічної безпеки підприємства ґрунтуються на ефективній роботі офіційного гарантійного підрозділу, який є основним органом підприємства, що гарантує безпеку підприємства. Метою організації та діяльності відділу безпеки є захист економічних інтересів підприємства та його власників шляхом виявлення, діагностики, мінімізації, зменшення та запобігання загрозам і небезпечним проявам.

Вітчизняними вченими визначено основні функції та завдання, які вирішує відділ корпоративної безпеки для забезпечення своєї безпеки. Ці функції показані на рис. 2.3.

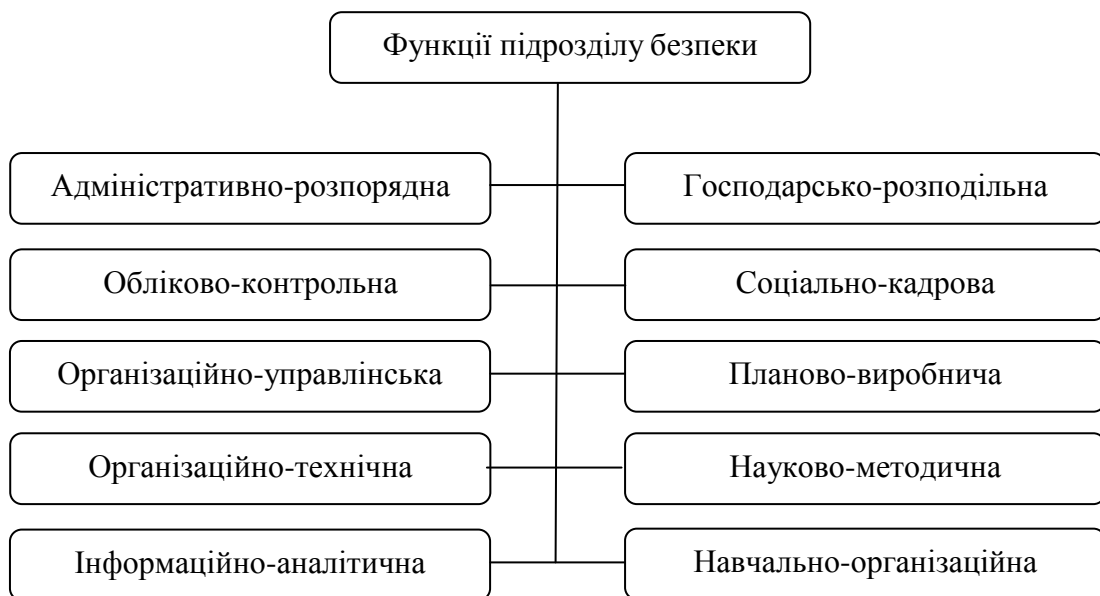


Рисунок 2.3 – Основні функції підрозділу безпеки підприємства

До основних завдань відділу безпеки слід віднести: захист економічних інтересів засновників товариства; сприяння керівництву товариства у забезпеченні контролю якості основних видів господарської діяльності, сприяння у забезпеченні дотримання вимог ліцензійні вимоги (якщо підприємство здійснює ліцензійні види діяльності); здійснювати профілактику правопорушень серед персоналу; забезпечувати особисту безпеку керівників та засновників підприємства; своєю діяльністю сприяти сталому розвитку компанії (через безпеку); забезпечувати особисту безпеку корпоративного майна, активів та особистих речей працівників; виявляти порушення законів; забезпечити безпеку співробітників і відвідувачів під час їх перебування на підприємстві; проводити навчання та консультації працівників з питань безпеки, встановлювати та контролювати відповідність системи безпеки; організовувати та контролювати дотримання комерційної таємниці та охорони інтелектуальної власності; збирати інформацію та надавати своїм засновникам та керівництву представлення про негативні тенденції та факти серед працівників; з'ясувати факти та організовувати контратаки проти проявів недобросовісної конкуренції; виявлення та боротьба з корупцією серед персоналу та неетичних державних службовців; взяти участь в аналізі фінансової стійкості підприємства та з'ясувати факт порушення відповідним персоналом підприємства фінансової дисципліни; сформулювати та контролювати систему входу працівників та іншого персоналу на підприємство; участь в оцінці надійності партнерів і підрядників; моніторинг реальних і потенційних загроз і небезпек для компанії; оцінювати стан економічної безпеки підприємства та вносити пропозиції щодо його покращення; технічний захист інформації підприємства; брати участь у службових розслідуваннях, пов'язаних з діяльністю корпоративного персоналу; контролювати стан пожежної безпеки підприємства; взаємодія з національною правоохоронною системою, забезпечуючи корпоративну безпеку.

Основним завданням забезпечення економічної безпеки підприємства є впровадження на підприємстві найкращої моделі безпеки; навчання керівників підрозділів підприємства методам відомчого забезпечення безпеки; контроль за дотриманням вимог безпеки; своєчасне звітування перед керівники підприємства та його відділу звітують про потенційні та реальні загрози господарській діяльності, контролюють систему безпеки підприємства, організовують роботу щодо зниження внутрішніх ризиків, пов'язаних з діяльністю персоналу підприємства; впроваджувати всі види інформації, аналізу інформації та бухгалтерського аналізу для підтримки економічної безпеки компанії; організовувати заходи щодо визначення надійності партнерів, підрядників та корпоративних споживачів; організовувати та впроваджувати заходи протидії недобросовісним конкурентам, а також відстежувати загрози існування компанії та небезпеки на ринку; організація захисту інформації, інформації, що становить комерційну таємницю або обмеженого доступу; організовувати перевірку персоналу та прийняття інформації про комерційну таємницю; організовувати та контролювати збереження конфіденційних документів.

Проаналізувавши завдання, які виконують експерти з безпеки для забезпечення економічної безпеки підприємства, можна визначити основні напрямки діяльності відділу безпеки щодо забезпечення економічної безпеки підприємства (рис. 2.4). Організовувати та контролювати збереження конфіденційних документів.

У сучасних словниках суб'єкт трактується як особа (фізична чи юридична особа), яка має певні права та обов'язки або носій дій, особа, яка знає, мислить і діє. Іншими словами, суб'єктом безпеки підприємства може бути особа (фізична чи юридична особа), яка має певні права та обов'язки щодо здійснення охоронних заходів на підприємстві.

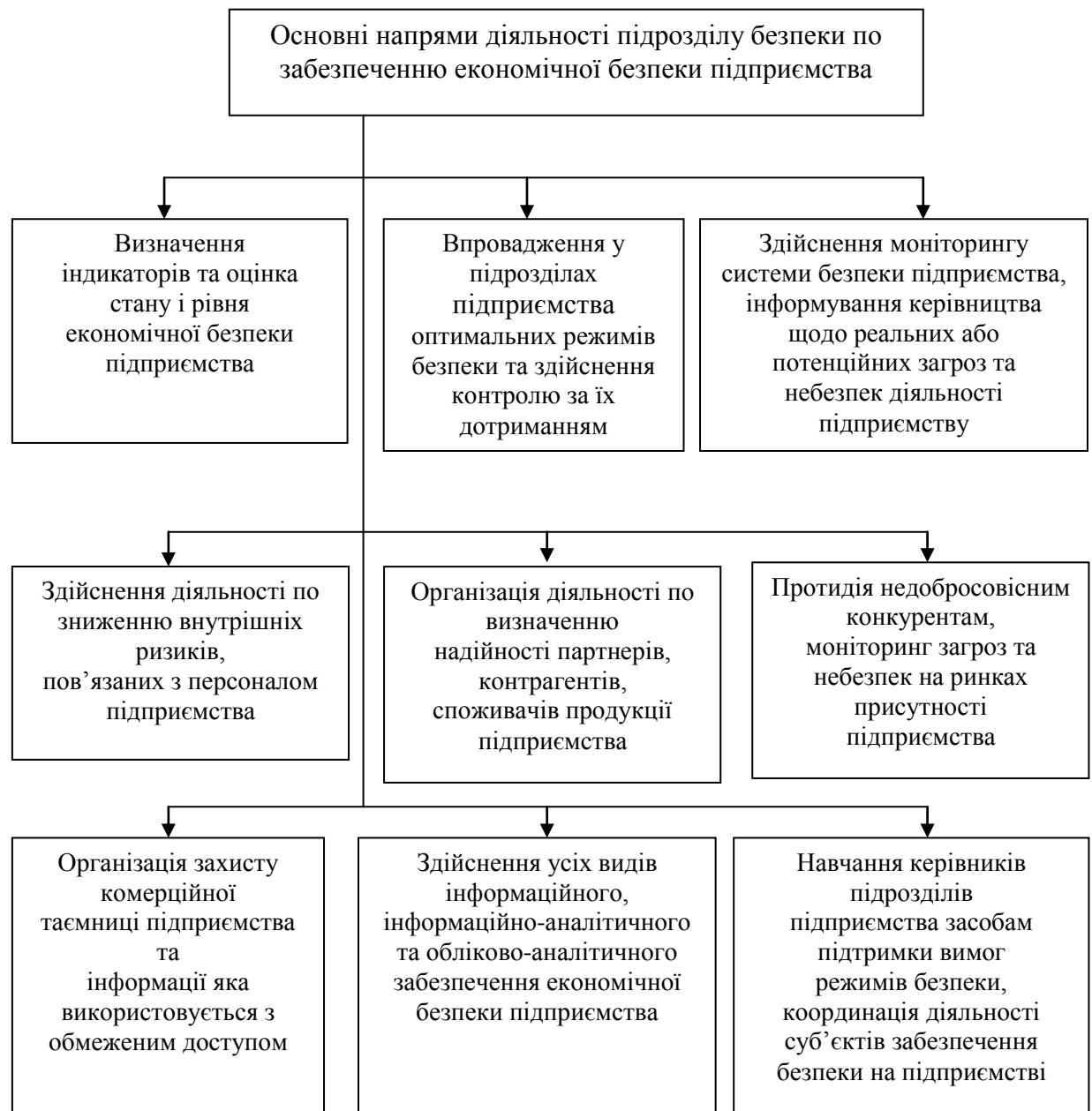


Рисунок 2.4 – Основні напрями діяльності фахівців підрозділу безпеки по забезпеченню економічної безпеки підприємства

До суб'єкта економічної безпеки підприємства слід віднести штатних або сумісників відділу охорони, які відповідають таким вимогам: мають відповідну академічну кваліфікацію (освіта: бакалавр, молодший коледж або магістр) та професійні здібності (знання, навички), можуть забезпечити безпеку підприємства, мати кваліфікаційні характеристики (завдання та

обов'язки) щодо здійснення відповідних заходів із забезпечення безпеки; зазначати у посадовій інструкції персоналу підприємства пов'язані з безпекою права та проводити відповідний інструктаж з техніки безпеки та як її забезпечити на підприємстві; наявність встановлених мотивів для забезпечення безпеки та відданості справі.

Таким чином, аналіз функцій і завдань підрозділу безпеки дає змогу визначити зміст роботи експертів з економічної безпеки щодо забезпечення економічної безпеки підприємства, що має бути відображено як один із напрямів діяльності підрозділу.

3 УДОСКОНАЛЕННЯ НАПРЯМІВ ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1 Формування механізму забезпечення економічної безпеки підприємства

У вигляді дворівневої системи захисту інформації забезпечується економічна безпека підприємства. Перший рівень передбачає конфіденційну роботу відділу безпеки організації, а другий рівень – формування психологічної атмосфери організації «пильності та відповідальності» за допомогою так званого координатора, а також призначення та володіння повноваженнями серед співробітників. від середнього керівництва. Визнаючи, що збереження інформації є одним із важливих аспектів корпоративної економічної безпеки, слід зазначити, що спрощення питань корпоративної економічної безпеки до захисту комерційної таємниці є дуже спрощеним вирішенням цієї проблеми. Очевидно, що таке вузьке розуміння економічної безпеки зумовлене надмірною «економністю», яка не враховує весь спектр екологічних впливів і розглядає його як основне джерело ризиків підприємства.

На економічну безпеку підприємства впливає зовнішнє середовище У ринковій економіці зовнішнє середовище постійно змінюється і ніколи не залишиться стабільним, незмінним або незмінним. Саме з точки зору зовнішнього впливу на навколишнє середовище, щоб захистити підприємства від їх негативного впливу, розглянути зміст економічної безпеки підприємств, у тому числі в кількох публікаціях вітчизняних економістів.

Найважливішими факторами, що впливають на економічну безпеку підприємств, є повнота законодавчої бази, рівень оподаткування, вихід на світовий ринок, інвестиційна привабливість регіонів і країн. Насамперед, економічна безпека підприємства залежить від економічної безпеки країни та

регіону, оскільки вона базується на його капіталі, сировині, виробничому потенціалі та перспективах розвитку. Наявність багаторівневої концепції економічної безпеки на всіх рівнях суб'єктів господарювання дає змогу забезпечити передбачуваність зовнішніх загроз для підприємства.

Особливу увагу слід приділити вивченню ділових партнерів, їх платоспроможності та ділової репутації. Досвід показує, що в умовах ринкової економіки та встановлення ділових відносин з неетичними контрагентами підприємство може зазнати значних економічних збитків у разі порушення договірних зобов'язань.

Слід звернути увагу на конкурентів, оскільки, застосовуючи методи недобросовісної конкуренції, вони можуть становити серйозні небезпеки та загрози для підприємства та призвести до серйозних економічних наслідків. Нині в науковій літературі, навіть якщо вона спеціально спрямована на це питання, дуже мало розкриттів сутності теорії корпоративної економічної безпеки, її складових та показників, а суть не завжди є чіткою та однозначною в визначення, що з'являються. Іноді неповна.

Взагалі кажучи, існує кілька способів визначення економічної безпеки підприємства:

– як запобіжний захід від економічних злочинів. У багатьох випадках економічна безпека підприємства зводиться до протистояння та захисту від різних економічних злочинів (крадіжки, шахрайства, підробки, промислового шпигунства тощо). Безсумнівно, що ці загрози є дуже важливими і їх необхідно постійно аналізувати та розглядати, але економічна безпека підприємства не може бути зведена лише до цього рівня. Це поняття все ширше і ширше.

– як стан захисту від внутрішніх і зовнішніх загроз. Підприємства є насамперед об'єктом економічних відносин. Власники бізнесу вважають, що результатом підприємницької діяльності є, насамперед, реалізація поставлених бізнесом цілей, яка зазвичай має економічний характер.

Боротьба із загрозами, як правило, не є метою створення та володіння бізнесом чи здійснення економічної діяльності. Однак власника можуть зацікавити міркування про економічну доцільність боротьби з загрозами, оскільки це безпосередньо зачіпає його матеріальні інтереси та через вартість ведення такої боротьби.

Тому рівень економічної безпеки підприємства в основному залежить від уміння керівництва прогнозувати та запобігати можливим загрозам та швидко вирішувати проблеми, що виникають. Відповідальний за компанію несе відповідальність за забезпечення контролю всіх бізнес-процесів, у тому числі за їх захист від очевидних і потенційних загроз. А кількість і види загроз збільшуються зі збільшенням чисельності працівників та зростанням виробництва та збуту підприємства.

До основних функціональних цілей економічної безпеки належать:

- забезпечити високу фінансову ефективність, фінансову стійкість та незалежність підприємства;
- забезпечити технологічну незалежність та реалізувати високу конкурентоспроможність технологічного потенціалу суб'єкта господарювання;
- реалізація високої ефективності управління, оптимізації та ефективної організаційної структури управління підприємством;
- досягнення високого рівня кваліфікації співробітників та їх інтелектуального потенціалу;
- юридична гарантія якості в усіх аспектах діяльності підприємства;
- забезпечити захист інформаційного поля та комерційної таємниці, а також досягнення рівня інформаційного забезпечення, необхідного для різних відділів та організаційних підрозділів підприємства;
- ефективно організувати безпеку корпоративного персоналу, капіталу та майна, інтересів бізнесу.

Рівень економічної безпеки підприємства залежить від добре організованої системи безпеки. Алгоритмом забезпечення економічної безпеки підприємства має бути: опис проблемної ситуації, визначення цільової установки; побудова системи економічної безпеки підприємства; розробка методів та інструментів оцінки економічної безпеки підприємства; розрахунок сил та засоби, необхідні для забезпечення економічної безпеки, формулювання заходів щодо реалізації економіки підприємства Основні положення концепції безпеки.

Вітчизняний та зарубіжний досвід свідчить, що головну роль у захисті комерційної таємниці відіграє саме підприємство, а не державний орган.

Серед суб'єктів, які захищають економічну безпеку підприємств, найважливіше значення мають власні служби економічної безпеки (як правило, за наявності відповідних суб'єктів підприємства та коштів).

Забезпечення економічної безпеки підприємства полягає у запобіганні можливим збиткам, досягненню найбільшого ступеня економічної безпеки зараз і в майбутньому, реалізації процесу функціональних складових економічної безпеки.

Спосіб забезпечення економічної безпеки підприємства - комплекс заходів та організаційна система для реалізації та контролю дозволяє досягти найвищого значення економічної безпеки підприємства. Створення сервісу з власною економічною безпекою є найбільшою складністю на практиці, адже кожен суб'єкт господарювання за своєю специфічною діяльністю є чистою особистістю. Однак при створенні служб економічної безпеки підприємцям рекомендується багато кроків:

– рішення про необхідність створення економічної безпеки. Проблема створення служби безпеки повинна виникнути при прийнятті рішення про організацію підприємства, що залежить від обраних видів діяльності, кількості продукції, що випускається, розміру річного обороту та прибутку, використання секретів виробництва, кількості працівників. Засновник

повинен передбачити потребу в охоронних послугах. Після державної реєстрації приймається остаточне рішення про створення організації служби економічної безпеки. Якщо рішення буде позитивним, визначити відповідальну особу, яка братиме безпосередню участь в організації служби економічної безпеки.

- визначити загальні завдання сектору економічної безпеки.

- розробити положення про служби економічної безпеки, визначити штатний склад та погодження. Наявність належної законодавчої бази дозволяє створювати служби юридичної безпеки.

- набір кадрів на роботу. Співробітники можуть бути ключовим персоналом, що займається цією діяльністю спеціально або протягом тривалого періоду часу, або вони можуть бути експертами.

При підборі штатних працівників найважливішим є професійна підготовка [42]. Система економічної безпеки потребує постійного контролю, вдосконалення та управління в таких аспектах:

- зміни в чинному державному законодавстві;

- розвиток компанії та вибір нових напрямків її економічної діяльності;

- збільшення чисельності працівників та зміни персоналу компанії;

- змінити перелік інформації, що становить комерційну таємницю компанії та конфіденційну інформацію;

- потреба в удосконаленні телефонної та комп'ютерної мережі компанії;

- винаходи промислового шпигунства та оманливі вороги нових технологій;

- поява на ринку недобросовісних конкурентів та зміна форм і методів;

- поява на ринку недобросовісних конкурентів та зміна форм і методів їх протиправної діяльності;

- криміногенна ситуація в районі тощо.

Підприємство має сформулювати стратегію корпоративної економічної безпеки, що включає: визначення стандартів і параметрів (кількісних і якісних порогів), що корпоративна економічна система відповідає її вимогам економічної безпеки; формулювання механізмів і заходів щодо виявлення ризиків економічної безпеки підприємства та його носіїв. та характеристики зони її виконання (зона розташування ризику); Визначити основні об'єкти ризику, механізм його дії та стандарти його економічної поведінки, у тому числі фінансові та корпоративні системи, розробити методи прогнозування та планування, методи виявлення та запобігання факторам, що призводять до ризиків економічної безпеки, та провести дослідження для визначення розвитку такі ризики Тенденції та можливості; створення ефективної системи економічної безпеки підприємства, формування механізмів та заходів фінансово-економічної політики щодо нейтралізації або зменшення впливу негативних факторів, визначення об'єктів, об'єктів та параметрів контролю для забезпечення економічної безпеки підприємств.

За допомогою механізму управління економічною безпекою підприємства здійснено ряд заходів щодо захисту його господарської діяльності від внутрішніх та зовнішніх негативних економічних ризиків. Ступінь цього захисту залежить від управлінських можливостей компанії на належному рівні:

- забезпечити стійкий економічний розвиток підприємства та досягнення цільових параметрів основної діяльності при збереженні ліквідності та незалежності його фінансової системи;

- забезпечити усунення негативних наслідків економічної кризи, свідомих дій конкурентів та інших «недружніх» структур.

- сформувати систему обліку потоків капіталу та посилити ефективність роботи системи контролю;

- залучайте та використовуйте позикові кошти з найкращою ціною та контролюйте прийнятні рівні боргового навантаження.

– запобігання працівникам недбалості, шахрайства та навмисних дій, пов'язаних з контрагентами, та інших фінансових порушень, у тому числі ситуацій, пов'язаних з використанням коштів державного бюджету;

– розробити та впровадити систему постійного моніторингу результатів фінансово-господарської діяльності підприємства з метою якнайшвидшої діагностики відхилень від встановлених параметрів;

– забезпечити заходи щодо захисту конфіденційності інформації, що становить комерційну таємницю.

Механізм управління економічною безпекою підприємства включає такі елементи: організаційну структуру; організацію, управління, перевірку та виконання функції створення, удосконалення та розвитку ефективних форм і методів системи економічної безпеки; забезпечення методів; засоби та важелі; показники та стандарти оцінки. нагляд та право та інформаційне забезпечення (рис. 3.1).

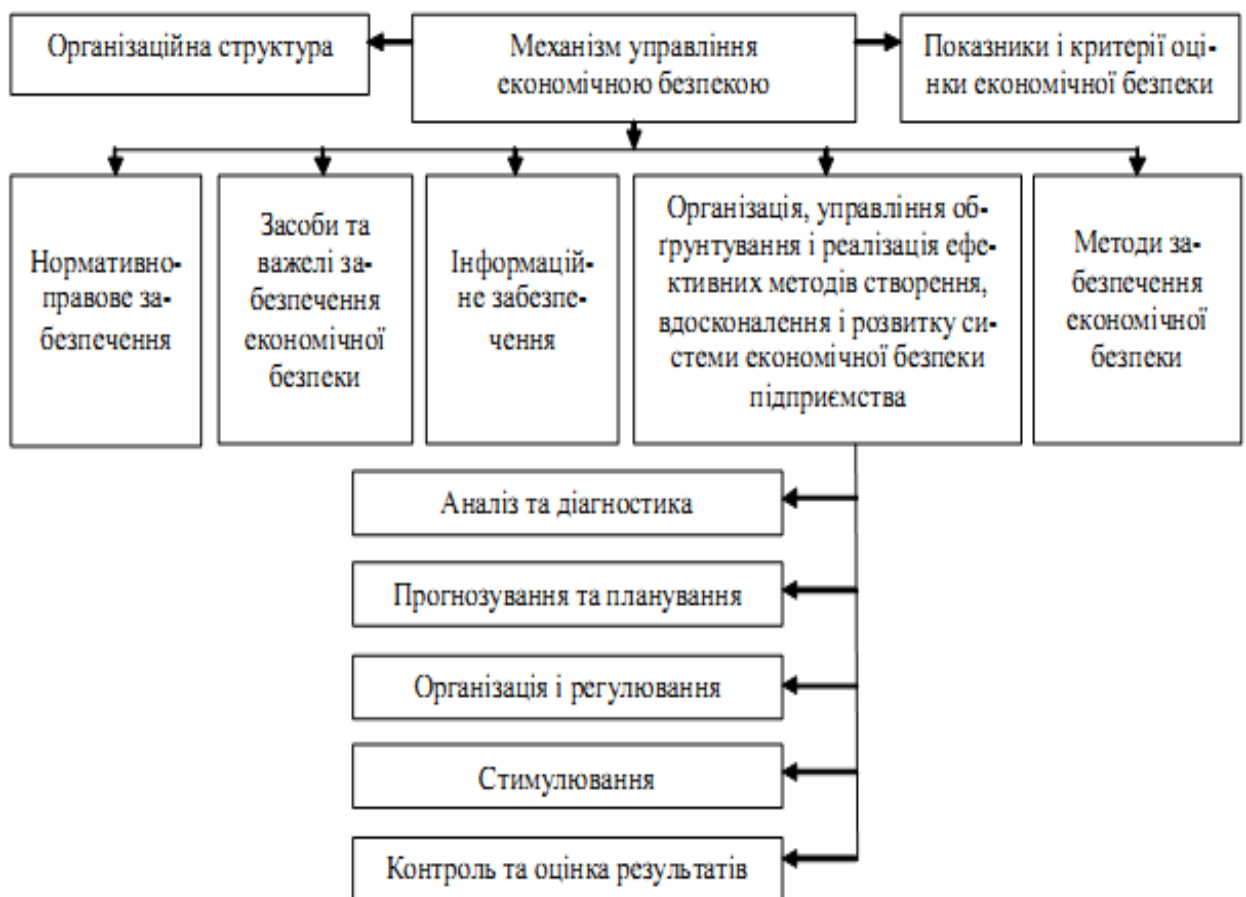


Рисунок 3.1 – Механізм управління економічною безпекою підприємства

Організаційна діяльність підприємства передбачає створення структури управління економічною безпекою підприємства та формулювання заходів щодо її забезпечення. Діяльність цього структурного поділу праці залежить від особливостей корпоративної діяльності. Однак управління господарською діяльністю може здійснюватися підрозділами, які беруть участь на контрактній основі.

До діяльності з економічної безпеки підприємства належать: забезпечення економічної безпеки підприємства, безперервний системний контроль та управління, демонстрація та впровадження ефективних форм і методів створення, підвищення та розвитку економічної безпеки підприємства, комплексне та ефективне використання всіх елементів захисту всіх засобів, а також постійне прогнозування можливостей Рівень професійної підготовки персоналу підприємства відповідає вимогам.

Основні цілі та функціональні цілі визначають формування необхідних структурних елементів і загального плану організації, управління, демонстрації та впровадження для створення, удосконалення та розвитку ефективних форм і методів системи економічної безпеки підприємства. Загальний план процесу економічної безпеки організації підприємства включає наступні дії послідовно або одночасно:

- аналіз економічної безпеки та економічна діагностика;
- сформувані необхідні фінансові ресурси;
- прогнозувати економічну безпеку на основі ідентифікації ризиків;
- планувати фінансово-господарську діяльність підприємства;
- операція та управління фінансово-господарською діяльністю підприємства;
- контролювати склад обліку, аналізу та аудиту;
- заходи стимулювання;
- загальна оцінка досягнутого підприємством рівня економічної безпеки тощо.

Хоча проблем у сфері корпоративної економічної безпеки багато, основними проблемами є недостатня увага до контролю ризиків, повільне реагування на кризові ситуації, що виникають, недостатній досвід управління корпоративною економічною безпекою.

У межах реалізації цих функцій рекомендується передбачити таку програму для організації оперативного аналізу економічної безпеки (рис. 3.2). Крім того, створення механізму забезпечення економічної безпеки підприємств потребує чітких показників та нормативів. Однак досі в економічній літературі не відбулося всебічного розвитку теорій з цього питання. Тому за основу формування показників і нормативів системи економічної безпеки можна прийняти показники, які є основою для визначення результатів фінансово-господарської діяльності. Вони дозволяють:

- урахування стратегічних цілей і завдань компанії;
- визначити функціональні складові економічної безпеки підприємства.

Ці складові можуть мати різну пріоритетність за видами діяльності суб'єкта господарювання;

- урахування потенційного рівня компанії;
- врахувати економічні втрати та збитки.

Для того, щоб механізм гарантування економічної безпеки підприємства функціонував, його показники оцінки повинні знаходитися в певному прийнятному діапазоні, в межах якого підприємство можливе для здійснення діяльності. На підприємстві до основних функціональних завдань економічної безпеки належать: забезпечення достатнього рівня фінансової ефективності, підтримання фінансової стійкості та незалежності підприємства, підтримання належного рівня підприємницької діяльності та підприємницьких інтересів.

формулювання необхідних заходів для адаптації до компанії та уникнення ризиків, з якими стикаються підприємства галузі.

Ризик зниження фінансової стійкості підприємств є актуальним, оскільки дисбаланс фінансово-економічного розвитку призведе до зниження економічної безпеки підприємств. Це може проявлятися як надмірне використання позикових коштів, що спричиняє дисбаланс корпоративних грошових потоків. Природу цього ризику та його прояв можна розглядати в процесі фінансового левериджу. У складі економічних ризиків такі ризики відіграють важливу роль. Ризик банкрутства підприємства обумовлений зниженням рівня ліквідності оборотних активів, що призводить до дисбалансу грошових потоків у часі. За своїми фінансовими наслідками цей ризик також є найнебезпечнішим.

3.2 Напрями удосконалення організації системи економічної безпеки ТОВ «Каспер»

За результатами попереднього аналізу було визначено, що економічна безпека підприємства (ЕБП) – це захист підприємства від зовнішніх і внутрішніх загроз, щоб матеріальні, фінансові та людські ресурси могли бути ефективно захищені та використані.

Забезпечення економічної безпеки ТОВ «Каспер» – це діяльність керівників і співробітників підприємства з метою запобігання негативному впливу зовнішніх і внутрішніх ресурсів на їхні корпоративні ресурси, що призведе до порушення стабільності роботи та економічного розвитку. загроза.

Аналізуючи стан економічної безпеки компанії, можна визначити, що ТОВ «Каспер» використовує наступні методи, стратегії, методи та завдання.

Необхідно розглянути організацію та методи, передбачені ЕБП. Забезпечити комплекс заходів планування та реалізації, які об'єднані на основі функцій в інтегрованій системі ЕБП. Відправною точкою для створення такої системи є бізнес-філософія, яка відображає уявлення засновників компанії про цінності бізнесу та кодекси поведінки.

Передумовою створення комплексної системи ЕБП є централізоване управління, яке забезпечує:

- координацію дій відповідальної особи ТОВ «Каспер» щодо надання ЕБП в межах своїх повноважень;

- концентрування корпоративних ресурсів для вирішення основного завдання забезпечення ЕБП;

- співпрацю з державними відомствами та органами місцевого самоврядування та підрядниками для формування надійної гарантії верховенства права;

- контроль повноти та своєчасності адміністративних дій, організованих генеральним директором підприємства, є частиною регламенту ЕБП.

ЕБП підтримує побудову комплексної системи на основі таких принципів: відповідність потенційним загрозам безпеки, адаптація до змін, цілісність і системність, а також розумна адекватність.

Стратегія управління ЕБП визначає основні напрями діяльності ТОВ «Каспер» для досягнення обраної мети. Стратегія була розроблена керівництвом компанії на основі усного аналізу потенційних джерел загроз безпеці, які можуть негативно вплинути на ресурси ТОВ «Каспер». При необхідності правові та інформаційні допоміжні матеріали, що стосуються господарської діяльності в прогнозних умовах.

Основні завдання щодо надання ЕБП:

- захищати законні права засновників, керівників та працівників;

- моніторинг навколишнього середовища ТОВ «Каспер» на основі довідкових матеріалів, статистичних та інших даних;

- використовувати індикатори ймовірності витрат для виявлення потенційних загроз безпеки та оцінки ризиків їх реалізації;

- захищати персонал та майно товариства, а також матеріали та засоби масової інформації, що містять захищену інформацію про товариства з обмеженою відповідальністю;

- запобігання та припинення протиправної діяльності, яку можуть здійснювати особи, що загрожують безпеці підприємства.

Стан усіх ресурсів підприємства (капітал, робоча сила, інформація, технології, технології, право) та підприємницькі навички. У такому стані вони можуть бути найбільш ефективно використані для стабільної роботи та динамічного науково-технічного та соціального розвитку, а превентивні можливості дозволяють швидко усувати різні внутрішні та зовнішні загрози; сукупність організацій і законів, системи та безпеки, технології, технології, економіка і фінанси, аналіз інформації та інші методи, призначені для усунення потенційних загроз та створення умов для ефективної діяльності суб'єктів господарювання відповідно до цілей і завдань, стан системи соціальних технологій компанії дозволяє використовувати наявні ресурси, підприємницькі здібності керівників, а також структурована організація та управління відносинами для уникнення зовнішніх загроз і боротьби з внутрішніми хаотичними факторами.

Основною метою управління економічною безпекою є забезпечення найбільш ефективної та ефективної роботи операційної системи та економного використання ресурсів, забезпечення певного рівня життя та якості бізнес-процесів, а також постійне стимулювання розвитку можливостей та їх стабільний розвиток.

Основні функціональні цілі економічної безпеки для ТОВ «Каспер» наведені в таблиці 3.1.

Таблиця 3.1 – Основні функціональні цілі економічної безпеки підприємства для ТОВ «Каспер»

№	Функціональні цілі економічної безпеки
1	Забезпечення високої ефективності роботи, фінансової стійкості та незалежності підприємства
2	Забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу підприємства
3	Досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством
4	Досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу, налагодження ефективної роботи кадрового відділу (кадрової політики)
5	Мінімізація аварій та інших впливів на виробничо-господарський процес, шляхом своєчасного проведення ремонту обладнання тощо
6	Якісна правова захищеність усіх аспектів діяльності підприємства
7	Забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства та відділів організації
8	Ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів

Отже, безпека підприємства – це здатність підприємства протистояти зовнішнім і внутрішнім негативним факторам, які можуть завадити підприємству досягти найбільш ефективних результатів. Успішний керівник завжди намагається встановити безпеку підприємства, тому що від цього залежить успішне «існування» організації на ринку. Щоб побудувати ефективну систему корпоративної безпеки, менеджери повинні розуміти джерела загроз, які можуть завдати шкоди підприємству. Джерело загрози показано на рис. 3.3.

Система захисту об'єктів ТОВ «Каспер» повинна включати як мінімум такі підсистеми, як охоронно-пожежна сигналізація, контроль та управління доступом, захист інформації, телевізійний моніторинг на окремих ділянках території. При виборі конфігурації підсистеми інформаційної безпеки компанії, що захищається, слід враховувати наступні моменти. Підприємство має велику кількість віддалених персональних місць. З метою забезпечення ефективного захисту та зниження експлуатаційних витрат рекомендується використовувати автоматизовану (мережеву) систему безпеки.

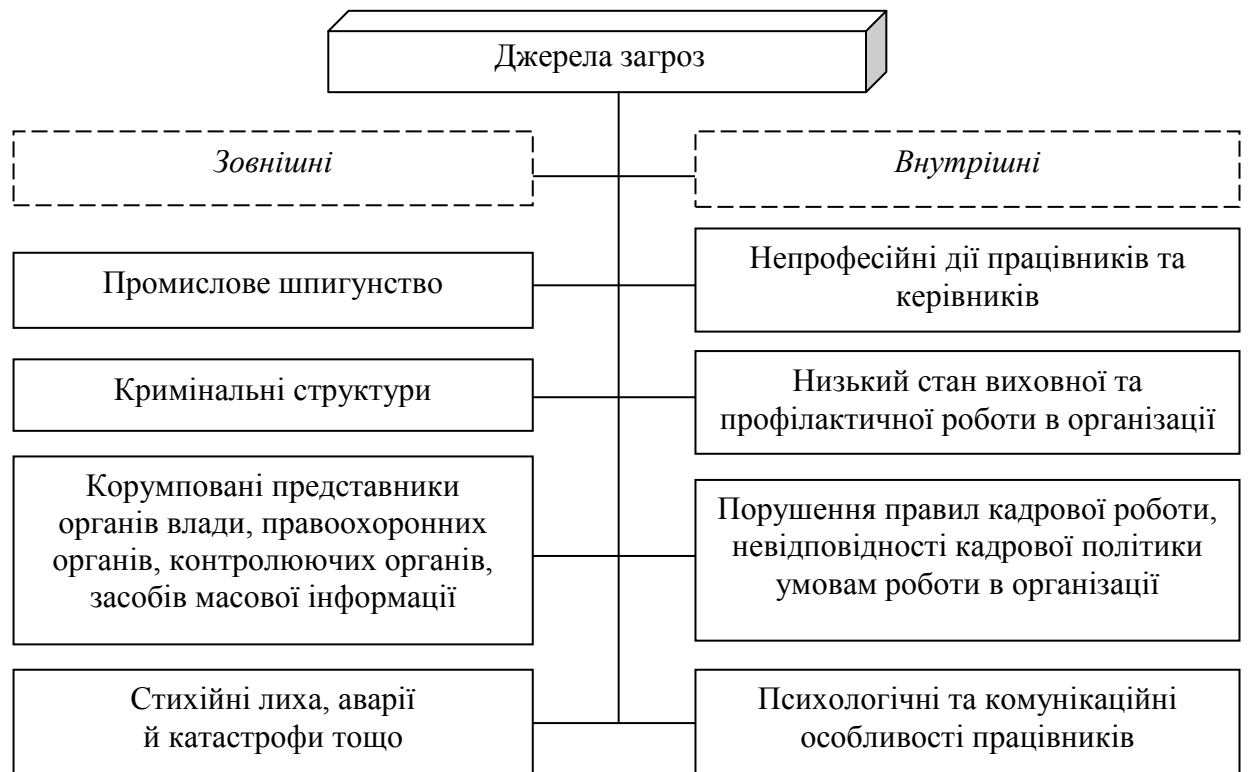


Рисунок 3.3 – Джерела загроз діяльності ТОВ «Каспер»

Однак поки що це може обмежитися локальною автономною системою, яка захищає інформацію. Система захищена в окремому, особливо офісному або кімнатному. Організаційні характеристики даного типу системи: Встановіть пароль для приміщення для запобігання несанкціонованому доступу співробітників і відвідувачів підприємства, використовуйте домашнє пошукове обладнання, щоб тимчасово перевірити, чи немає в приміщенні приладу моніторингу, використовувати віброакустичне обладнання, створюйте перешкоди на елементах будівельної конструкції, допомагайте захистити будинок від лазерних мікрофонів і стетоскопів, використовуйте спеціальні технічні засоби для дистанційного блокування будинку, щоб захистити будинок від несанкціонованого використання мобільних телефонів; обладнати встановлені в кімнаті телефони користувачів, сумісне голосове повідомлення технологічні засоби захисту, ці засоби використовуються для передачі голосових сигналів і факсів через телефонну мережу загального користування, шифрування; спеціальна перевірка

комп'ютерного обладнання на місці установки для запобігання несанкціонованого видалення інформації через непряме електромагнітне випромінювання та створених нею інструкцій.

Заходи щодо зменшення внутрішніх загроз включають: організаційні заходи щодо захисту інформації (обмеження доступу до інформації тощо); контрольно-правові заходи (контроль за виконанням відповідних інструкцій, наказів, наказів та положень щодо вимог до працівників); інженерно-технічні заходи (стабілізувати роботу, знизити (підготовчі роботи та обладнання для ризику аварії та ін.); профілактичні заходи (системні вимоги, правила роботи тощо, формування відповідного морально-етичного статусу в колективі), співпраця з працівниками (підбір працівників, консультування, навчання інформаційній безпеці, інформованість та навчання працівників). Їхня кваліфікація); організація персоналу та організація майнової охорони (встановлення камер спостереження тощо).

Отже, економічна безпека підприємства – це здатність захищати свою діяльність від негативного впливу зовнішнього середовища, а також здатність швидко усувати різноманітні загрози чи пристосовуватися до існуючих умов, які не впливають негативно на його діяльність. Внутрішні та зовнішні загрози безпеці компанії є постійними і не залежать від ролі, місця розташування та важливості організації. Тому керівництво компанії має надавати велике значення питанням безпеки, що забезпечить ефективну роботу підприємства, адже воно має всі необхідні інструменти, в тому числі технологічні та організаційні.

Тому, дотримуючись загальних рекомендацій, ТОВ «Каспер» зможе значно підвищити свою економічну безпеку. Крім того, у цьому розділі представлені розширені методи.

З метою підвищення ефективності економічної безпеки ТОВ «Каспер» потребує певної реорганізації.

Забезпечення економічної безпеки підприємств може бути пов'язано переважно із запобіганням шахрайству, недобросовісній конкуренції,

промислового шпигунства та іншим економічним злочинам, але це не повністю розкриває це поняття. Економічна безпека підприємства визначається багатьма факторами, які відображають незалежність, стабільність, можливості зростання та економічні вигоди. Проте економічну безпеку підприємства можна розділити на кілька складових за аспектами, які надає підприємство: фінанси, інформація, персонал, технології, ресурси, ринок тощо. Тому економічну безпеку підприємства можна виразити як стан ресурсів підприємства, який може забезпечити найбільш ефективне використання ресурсів у постійно мінливому середовищі загроз та сприяти сталому розвитку підприємства.

Оскільки економічна безпека підприємств значною мірою зумовлена необхідністю протистояти негативному впливу зовнішнього та внутрішнього середовища, що постійно змінюється, необхідно розробити достатні заходи, щоб такі показники не могли точніше відображати ці категорії. Однак господарська діяльність за чинними законами ринкової економіки означає, що підприємства самостійно визначають напрямки економічної політики, організовують і планують виробництво і реалізацію продукції, контролюють достатність оборотних коштів, порівнюють з умовами кредиторів і дебіторів.

Все це свідчить про те, що економічна безпека підприємства має забезпечуватися відповідно до особливостей і потреб кожного підприємства. Ключовим є те, що система економічної безпеки не може бути застосована однаково для всіх підприємств, це залежить від конкретних умов підприємства, зокрема від особливостей масштабів, структури капіталу, технологій виробництва, сфери функціонування, сфери бізнесу, національний економічний сектор (приватний, державний, національний), зовнішнє середовище, включаючи постачальників, споживачів, конкурентів тощо.

Слід зазначити, що загроза економічній безпеці підприємств походить від зовнішнього середовища, не тільки промислового шпигунства, недобросовісної конкуренції, шахрайства, а й нападів на підприємства та несприятливих ринкових коливань, що призводять до глибоких криз на

підприємстві. При цьому гарантування економічної безпеки підприємств має базуватися на трансформаційних заходах, особливо на заходах реструктуризації. При цьому під реструктуризацією розуміють комплекс заходів, спрямованих на відновлення стійкої економічної, фінансової та технологічної життєздатності підприємства для забезпечення ефективної діяльності підприємства в конкурентному середовищі та відновлення його конкурентоспроможності на довгостроковій основі. . Такий спосіб зміни компаній для реагування на екологічні загрози повністю відповідає інтересам економічної безпеки компанії.

Заходи реструктуризації здійснюються на різних рівнях компанії, оскільки нові бізнес-стратегії (оренда, оренда, франшиза) та внутрішня реорганізація (у вигляді злиття, поглинання, виділення, поділу та перетворення) використовуються для захисту її фінансів, майна, виробництво тощо.

Розглядаючи реорганізацію, слід зазначити, що термін «структура» вживається в економічному контексті, маючи на увазі специфічний і стійкий зв'язок між основними елементами конкретної функції чи процесу. Як структурна зміна, реорганізація характеризується цілеспрямованим процесом зміни організаційної структури. Така ж структура визначає обмеження компаній, які працюють у своїй повсякденній роботі та прагнуть до кращих економічних показників. Тому реорганізацію можна також розуміти як спробу змінити організаційну структуру, щоб зменшити деякі або всі короткострокові обмеження (загрози для навколишнього середовища), і вона повинна відповідати довгостроковій стратегії. Крім того, корпоративна реструктуризація також визначається як низка заходів, що вживаються для підвищення конкурентоспроможності підприємства та підвищення корпоративної вартості.

Підсумовуючи, головною метою реструктуризації підприємства є перетворення на підприємство з економічною безпекою, стабільністю ринку та високою вартістю володіння. При цьому підвищення економічної безпеки

підприємства забезпечується також на основі управління фінансовою та майновою безпекою підприємства, що є фактором, який формує вартість підприємства.

Крім того, реструктуризація може включати різні заходи, зокрема продаж активів неефективних компаній, злиття, поглинання, виділення тощо. Ці заходи зміцнили економічну безпеку фінансів компанії, зробили розвиток компанії більш динамічним, а також вчасно відреагували на придбання компаній.

З огляду на різноманітність форм реорганізації, обсягу реалізації та відповідних аспектів корпоративної економічної безпеки її можна поділити на три категорії: реорганізація портфеля активів, фінансова реорганізація та організаційна реорганізація.

Реорганізація портфеля активів передбачає значні зміни загальної суми активів, що належать компанії, або діяльності, в якій вона бере участь, включаючи ліквідацію, продаж активів, продаж активів та поділ підприємств. Заходи щодо реорганізації групи можуть підвищити фінансову безпеку компанії. Якщо існує загроза недружнього придбання, або зацікавлені сторони бажають придбати вторинні відділи, пов'язані з основним бізнесом, або сподіваються збільшити капітал за рахунок продажу в розстрочку, керівництво може прийняти цей метод реструктуризації.

При цьому компанія може реалізувати активний торговий портфель акцій, покращити структуру інвестиційного портфеля, підвищити захищеність коштів.

Порівняно з інвестиційними портфелями фінансова реструктуризація характеризується прямими значними змінами в структурі капіталу підприємства, включаючи зміни у погашенні боргового фінансування, структурі капіталу, частці власних і позикових коштів у боргу. У цьому випадку фінансова реорганізація передбачає розподіл грошових потоків підприємств або кредитних ресурсів, вирішення проблем з аспектів стратегії чи правил договору, коригування грошового потоку та визначення

додаткової вартості. Тому фінансова реорганізація може зміцнити фінансову безпеку підприємства, підвищити фінансову стійкість, підвищити вартість підприємства.

Організаційна реструктуризація полягає у зміні організаційної структури підприємства, посиленні менеджменту, підвищення ефективності прийняття управлінських рішень. Вона включає скорочення відомчих меж, уніфікацію рівнів, призначення контрольних інтервалів, зменшення диверсифікації продукції, перегляд заробітної плати, спрощення технічних процесів та реформ управління, а також спільне підвищення інформаційної складової економічної безпеки.

Тому рівень економічної безпеки підприємства залежить від здатності керівництва уникати можливих загроз та запобігати чи усувати негативні наслідки зовнішнього та внутрішнього середовища. Своєчасне впровадження заходів реструктуризації, спрямованих на відновлення фінансів та підвищення ефективності підприємства, може підвищити його економічну безпеку та забезпечити довгострокове зростання та розвиток.

Оскільки існує багато способів реорганізації, а єдиного стандарту виконання не існує, не існує єдиного методу оцінки ефективності реорганізації. Проте можна виділити деякі загальні методи оцінки ефективності або окреслити ряд типових проблем, які необхідно вирішити для успіху проекту реструктуризації.

По-перше, визначити вжиті заходи в процесі реорганізації та оцінити їх можливі наслідки, по-друге, вибрати критерії (один або системний) для оцінки запланованих заходів, по-третє, окреслити деякі показники оцінки ефективності. Це може бути конкретний показник; продажі зросли в 10 разів, а робочі місця збільшилися вдвічі; зниження собівартості продукції тощо, або комплексні показники чи набір показників: підвищення конкурентоспроможності продукції та підприємств, раціональне використання ресурсів, збільшення ринку частка I вихід у нові сектори, підвищення інвестиційної привабливості тощо.

Однак наслідки реорганізації можуть не піддаватися кількісному виміру, тобто їх результати неможливо обчислити, додати, відняти чи розділити, оскільки вони не розкривають форму матеріалізації. У цьому випадку зверніть увагу на якісні параметри наслідків реорганізації, які не очевидні на перший погляд. Оскільки зміни в процесі реорганізації охоплюють весь життєвий цикл підприємства, це неминуче торкнеться основного органу підприємства, тобто людських ресурсів.

Зазвичай найбільш цінні та глибокі зміни пов'язані з людьми. Після аналізу діяльності компанії були визначені основні загрози. Харківська філія ТОВ «Каспер» не має великих конкурентів, компанія працює у сфері ІТ-технологій, тому користується певним податковим «комфортом». Економічна ситуація в країні не погіршить економічну ситуацію компанії, адже ТОВ «Каспер» закріпило позиції замовлення не тільки в центрі країни, а й за кордоном. Тому загроза для підприємства є не стільки зовнішнім, скільки внутрішнім фактором, а полягає в недосконалості кадрової політики. Як відомо, 80% загроз компанії – це інсайдерські загрози. Співробітники можуть несвідомо розголошувати інформацію, яка може становити комерційну таємницю, своїм колегам через свою зарозумілість і сподівання підвищити свій соціальний статус. Незадоволені співробітники можуть зв'язатися з конкурентами і розкрити їм цінну інформацію, що також є загрозою для компанії. Такі працівники завдадуть великої шкоди підприємству.

Тому необхідно змінювати методи та принципи управління, змінювати стереотипи мислення та моделі поведінки керівників і співробітників, тобто характер соціального управління стає неминучим у заходах реструктуризації, і воно є ринковим. Це вже не форма, а суть, що виражається в переході до процесно-орієнтованої системи. Ці зміни будуть поширюватися з часом, вони будуть повільнішими, але ефект набагато очевидніший – вони завжди покращують якість менеджменту та самого менеджменту, таким чином починають розвивати бізнес у новому напрямку.

Необхідно обирати показники оцінки реструктуризації, пов'язані з категорією часу та ризиком. З огляду на це, можна говорити про короткостроковий, довгостроковий і стратегічний вплив (категорія часу пов'язана з часом виконання результату і тривалістю дії). Очікування очікуваного результату відбувається за невизначених умов, а його конкретним проявом є ризик, тому необхідно враховувати як ймовірність успіху, так і ймовірність невдачі;

Ефективність передбачає порівняння витрат і результатів. Компанії, як правило, орієнтуються лише на результат, не приділяючи належної уваги витратам. Тому важливо враховувати витрати на корпоративну реструктуризацію, особливо тому, що це відбувається за рахунок внутрішніх ресурсів. Тому необхідно оцінити вартість реструктуризації.

До ефективних категорій належать ті системні зміни, тобто всі елементи виробничої системи так чи інакше мають бути змінені. Реструктуризація має охопити всі об'єкти: структуру, фінанси, бізнес-план, маркетинг, логістику, економіку підприємства.

Якщо змінюється сфера маркетингу, складові цього процесу (просування товару на ринку, відносини з клієнтами тощо) неминуче повинні забезпечувати відповідну інформаційну систему, яка в свою чергу потребує відповідної системи обліку. Система обліку повинна мати можливість надавати адекватні послуги для процесу створення продукції, партій або замовлень. Це єдиний спосіб створити гнучкість для виробників і постачальників, дизайнерів і техніків, які працюють одночасно. Тому ці заходи щодо оптимізації процесів і функцій можна вважати ефективними.

Поняття системи слід розглядати в сукупності з послідовністю, що означає постановку цілей і узгодженість цілей. При недотриманні цього правила реорганізація може закінчитися сама по собі («сама річ») і не спричинить жодних змін у фінансово-господарській діяльності підприємства.

Підсумовуючи, реорганізація була ефективною та успішною, і мета, поставлена на першому етапі реорганізації, тобто концептуальна мета, була досягнута. Розглядаючи конкретну компанію ТОВ «Каспер», можна сказати, що найкраща для нього реорганізація компанії покращить показники економічної безпеки.

ВИСНОВКИ

У першому розділі роботи розглянуто теоретичні засади організації та управління системою економічної безпеки підприємства.

Розглянуто сутність та функціональні складові системи економічної безпеки підприємства.

Під економічною безпекою найчастіше розуміють стан використання матеріальних та нематеріальних ресурсів, динаміку їх впливу на результати діяльності та здатність забезпечити реалізацію економічних інтересів.

Економічна безпека підприємства розглядається як такий стан використання ресурсів, який забезпечує захищеність його економічних інтересів від внутрішніх і зовнішніх загроз та створює необхідні передумови для стійкого розвитку в поточному та довгостроковому періодах на основі використання фінансового потенціалу.

Наведено основні підходи до визначення сутності категорії «економічна безпека підприємства».

Графічно представлено взаємозв'язок між структурними елементами економічної безпеки підприємства.

Проаналізовано підходи різних авторів до визначення економічної безпеки підприємства.

Розглянуто теоретичні аспекти організації роботи з персоналом як складової системи економічної безпеки підприємства. В межах чого наведено послідовність формування системи роботи з персоналом та взаємозв'язок стратегії організації та стратегії управління персоналом.

Також у роботі розкрито особливості організації інформаційної безпеки підприємства.

У другому розділі роботи проаналізовано діяльність та напрями організації економічної безпеки ТОВ «Каспер».

ТОВ «Каспер» була заснована в 1991 році. Основні напрями діяльності ТОВ «Каспер»: поставка програмного забезпечення; автоматизація господарської діяльності підприємств; супровід і підтримка; навчання й сертифікація; надання консалтингових послуг.

Наведена організаційна структура підприємства.

Проведено аналіз показників, що характеризують результати фінансово-господарської діяльності підприємства.

У результаті проведених досліджень можна зробити такі висновки:

– недотримання в повному обсязі нормального співвідношення активів, класифікованих за ступенем ліквідності, та зобов'язань, класифікованих за строками погашення;

– протягом звітного періоду отримано прибуток від реалізації (122223 грн.), але спостерігається негативна динаміка порівняно з попереднім періодом (-28 577 грн.).

Основними показниками фінансового стану організації є:

– висока залежність організації від позикових коштів (власний капітал становить лише 27%);

– коефіцієнт покриття інвестицій значно нижчий за нормальний (власний капітал та довгострокові зобов'язання становлять лише 29% загального капіталу ТОВ «Каспер», критичне значення – 75%);

– коефіцієнт швидкої (проміжної) ліквідності значно нижчий за нормальний;

– коефіцієнт абсолютної ліквідності значно нижчий за нормальний.

Також проаналізовано напрями організації економічної безпеки на досліджуваному підприємстві.

Наведено основні функції підрозділу безпеки та основні напрями діяльності фахівців підрозділу безпеки по забезпеченню економічної безпеки підприємства.

Сукупність конкретних завдань, що стоять перед службою безпеки підприємства, зумовлює певний набір виконуваних нею функцій. Загальні функції, що покладаються на службу безпеки підприємства полягають в такому:

- захист законних прав та інтересів суб'єктів підприємницької діяльності та їх співробітників;
- збирання даних, їх аналіз, оцінювання і прогнозування оперативної обстановки та різноманітних ризиків на підприємстві, в організації, установі;
- вивчення та перевірка партнерів, клієнтів і конкурентів;
- своєчасне виявлення можливих посягань на об'єкт чи його співробітників з боку джерел зовнішніх загроз безпеці;
- недопущення проникнення на об'єкт структур промислового шпіонажу, злочинних формувань чи осіб із протиправними намірами;
- протидія технічному проникненню на об'єкт чи його комунікаційні системи;
- захист співробітників об'єкта від насильницьких посягань;
- виявлення, запобігання можливій протиправній чи іншій негативній діяльності співробітників суб'єкта підприємництва на шкоду його безпеці;
- збереження матеріальних цінностей, відомостей з обмеженим доступом;
- пошук та здобування необхідної інформації для прийняття оптимальних управлінських рішень з питань стратегії тактики подальшої підприємницької діяльності;
- фізичну і технічну охорону будівель, споруд, територій, транспортних засобів та інше.

У третьому розділі роботи запропоновано рекомендації щодо формування механізму управління економічною безпекою підприємства. Створення механізму забезпечення економічної безпеки підприємств потребує чітких показників та нормативів.

Розроблено напрями удосконалення організації системи економічної безпеки ТОВ «Каспер».

У межах цього запропоновано додаткові напрями організації експрес-аналізу економічної безпеки підприємства.

Визначено основні функціональні цілі економічної безпеки та джерела загроз діяльності ТОВ «Каспер».

Основні результати досліджень опубліковані в роботах [68, 69].

Копії опублікованих праць наведено в додатку А.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Єфдокимов В. В., Олійник О. В., Грицишен Д. О., Грищенко О. О. Концепція управління економічною безпекою суб'єктів господарювання в контексті теорії сталого розвитку: монографія.; Житомир. держ. технол. ун-т. Житомир, 2013. 251 с.
2. Майстро Р.Г., Полозова Т.В. Напрями вдосконалення державного регулювання економічної безпеки України. *Приазовський економічний вісник*. 2019. Випуск 1(12). С. 46-50.
3. Шмалій Л. В., Ількевич М. В. Управління економічною безпекою підприємства. *Економіка. Менеджмент. Бізнес*. 2020. № 4. С. 68-73.
4. Меліхова Т. О. Вдосконалення функцій та завдань забезпечення економічної безпеки підприємств. *Інвестиції: практика та досвід*. 2018. № 3. С. 70-73.
5. Новик І. В. Проблеми та перспективи забезпечення економічної безпеки підприємства в Україні. *Інфраструктура ринку*. 2020. Вип. 43. С. 229-233.
6. Жадько К. С., Самойленко Д. М. Економічна безпека підприємств в умовах цифрових технологій і пандемії. *Центральноукраїнський науковий вісник . Економічні науки*. 2020. Вип. 5. С. 170-176.
7. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету. Економічні науки*. 2020. № 4(1). С. 32-35.
8. Ольшанський О. В., Крамчанінова М. Д. Вплив пандемії COVID-19 на проблеми забезпечення економічної безпеки малих та середніх підприємств. *Економічний вісник Донбасу*. 2021. № 2. С. 78-82.

9. Штангрет А. М., Караїм М. М., Штангрет І. А. Інтенсифікація управління економічною поведінкою підприємства: безпекові засади. *Ефективна економіка*. 2020. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2020_5_8.

10. Христофоров В. О., Андрющенко Є. Г. Формування механізмів забезпечення економічної безпеки підприємств. *Вісник ХНАУ. Серія: Економічні науки*. 2019. № 1. С. 328-336.

11. Економіка підприємства: підручник / За ред. С.Ф. Покропивного. Київ: КНЕУ, 2001. 528 с.

12. Федоренко Р. М. Система управління ресурсами як основа забезпечення економічної безпеки. Недержавна система безпеки підприємництва як суб'єкт національної безпеки України: [зб. матер. наук.-практ. конф.]. Київ: Вид-во Європ. ун-ту, 2003. С. 224-229.

13. Козаченко А. В., Пономарев В. П., Ляшенко А. Н. Экономическая безопасность предприятия: сущность и механизм обеспечения: монография. Київ: Либра, 2003. 280 с.

14. Ареф'єва О. В., Кузенко Т. Б. Планування економічної безпеки підприємств. Київ: Вид-во Європ. ун-ту, 2005. 170 с.

15. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: навчальний посібник. Київ: Атіка, 2005. 432 с.

16. Економічна та майнова безпека підприємства і підприємництва. Антирейдерство / [за наук. ред. Б. М. Андрушківа]. Тернопіль: Терно-граф, 2008. 424 с.

17. Пухальська Г. В., Христич Г. О. Економічна безпека підприємства: сутність та її складові. *Вісник Хмельницького національного університету. Економічні науки*. 2008. № 6. Т.1. С. 197-200.

18. Поснова Т. В. Механізм функціонування соціальної складової економічної безпеки: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 08.00.01. К., 2008. 19 с.

19. Кошембар Л. О. Механізм удосконалення системи економічної безпеки суб'єктів господарювання на основі оптимізації оподаткування: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 21.04.02; Вищий навчальний заклад «Університет економіки та права «Крок». Київ, 2009. 21 с.

20. Економічна безпека підприємств, організацій та установ: навч. пос. [для студ. вищ. навч. закл.] / [Ортинський В. Л., Керницький І. С., Живко З. Б. та ін.]. Київ: Правова єдність, 2009. 544 с.

21. Зацеркляний М. М., Мельников О. Ф. Основи економічної безпеки: навчальний посібник. Київ: КНТ, 2009. 337 с.

22. Іванюта Т. М., Заїчковський А. О. Економічна безпека підприємства: навч. посіб. [для студ. вищ. навч. закл.]. Київ: Центр учбової літератури, 2009. 256 с.

23. Шемаєва Л. Г. Економічна безпека підприємств у стратегічній взаємодії з суб'єктами зовнішнього середовища : автореф. дис. на здобуття наук. ступеня д-ра екон. наук: спец. 21.04.02; Вищий навчальний заклад «Університет економіки та права «Крок». Київ, 2010. 40 с.

24. Соколенко Т. М. Економічна безпека підприємства в умовах транзитивної економіки. *Сучасна наука XXI століття: сьома міжнародна наук.-практ. інтернет-конф.* URL: <http://intkonf.org/kand-ped-n-sokolenko-tm-ekonomichna-bezpeka-pidприємства-v-umovah-tranzitivnoyi-ekonomiki>.

25. Мішин О. Ю., Мішина С. В. Сутність поняття «економічна безпека підприємства». *Вісник економіки транспорту і промисловості.* 2012. № 38. С. 86-92.

26. Комплексне забезпечення фінансово-економічної безпеки: навч. посіб. для студентів ВНЗ / ред. Г. Є. Павлова та ін. Дніпро: Акцент, 2018. 559 с.

27. Управління фінансовою безпекою економічних суб'єктів: навч. посіб. для студентів ВНЗ екон. і юрид. спец. усіх форм навчання / ДВНЗ «Укр. акад. банк. справи Нац. банку України», Каф. фінансів; за заг. ред. д-ра екон. наук, проф. С. М. Фролова; [уклад.: С. М. Фролов та ін.]. Суми: ДВНЗ «УАБС НБУ», 2015. 331 с.

28. Єпіфанов А. О., Пластун О. Л., Домбровський В.С., Болгар Т. М., Ващенко О. М. Фінансова безпека підприємств і банківських установ: монографія; Ред.: А. О Єпіфанов. Суми: ДВНЗ «УАБС НБУ», 2009. 295 с.

29. Фінансово-економічна безпека: стратегічна аналітика та аудиторський супровід: монографія / ред.: Т. В. Момот; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків: ХНУМГ ім. О. М. Бекетова, 2015. 340 с.

30. Мандзіновська Х. О. Управління фінансово-економічної безпекою: підручник / ред.Онищенко В. О. та ін. Полтава: ПолтНТУ, 2018. 530 с.

31. Козаченко Г. В., Рамазанов С. К., Ляшенко О. М., Погорелов Ю. С., Пшик Б. І. Система економічної безпеки: держава, регіон, підприємство: монографія [у 3 т.]. Т. 3. Луганськ: Промдрук, 2014. 336 с.

32. Живко З. Б. Управління системою економічної безпеки підприємства: навч. посіб.; Львів. держ. ун-т внутр. справ. Львів, 2016. 211 с.

33. Онищенко С. В., Пугач О. А. Загрози економічній безпеці України: сутність, оцінювання та механізм упередження: монографія. Полтава: ПолтНТУ, 2015. 337 с.

34. Франчук В. І. Економічна безпека суб'єктів господарської діяльності: підручник; Львів. держ. ун-т внутр. справ. Львів, 2015. 235 с.

35. Мазаракі А. А., Корольчук О. П., Мельник Т. М. Економічна безпека України в умовах глобалізаційних викликів: монографія; Ред.: А. А. Мазаракі; Київ. нац. торг.-екон. ун-т. К., 2010. 717 с.

36. Новик І. В. Проблеми та перспективи забезпечення економічної безпеки підприємства в Україні. *Інфраструктура ринку*. 2020. Вип. 43. С. 229-233.

37. Концептуальні засади формування фінансово-економічної безпеки: колект. монографія / [Абакуменко О. І. та ін.]; за заг. ред. д-ра екон. наук, проф. Шкарлета Сергія Миколайовича; Черніг. нац. технол. ун-т. Ніжин: Лук'яненко В.В.: Орхідея, 2015. 440 с.

38. Шмалій Л. В., Ількевич М. В. Управління економічною безпекою підприємства. *Економіка. Менеджмент. Бізнес*. 2020. № 4. С. 68-73.

39. Лук'янова В. В., Шутяк Ю. В. Діагностика економічної безпеки підприємства: монографія. Хмельницький: ХНУ, 2014. 165 с.

40. Герасименко Т. О., Мазуренко О. М. Аналіз господарської діяльності: навч. посіб.; Львів. комерц. акад. Львів, 2014. 319 с.

41. Божидарнік Т. В., Кривов'язюк І. В. Обґрунтування господарських рішень і діагностика промислового підприємства: сучасний формат: монографія; Луц. нац. техн. ун-т. Луцьк, 2014. 160 с.

42. Міщук Г. Ю., Джигар Т. М., Шишкіна О. О. Економічний аналіз: навч. посіб.; Нац. ун-т вод. госп-ва та природокористування. Рівне: НУВГП, 2017. 155 с.

43. Могилевська О. Ю., Уфимцева Т. М., Слободяник А. М. Економіка підприємства. Теорія і практика : навч. посіб.; Київ. міжнар. ун-т. Київ, 2017. 295 с.

44. Ковальчук І. В. Економіка підприємства: навч. посібник. Київ: Знання, 2014. 679 с.

45. Основи економічного аналізу: навч.-метод. посіб. для студентів екон. спец., магістрів, аспірантів, викл. / В. М. Микитюк та ін.; ред. В. М. Микитюк; Житомир. нац. агрокол. ун-т. Житомир: Рута, 2018. 439 с.

46. Шарко М. В., Мешкова-Кравченко Н. В., Радкевич О. М. Економіка підприємства: навч. посіб. для студ. ВНЗ. Ч. 1; Херсон. нац. техн. ун-т. Херсон, 2014. 434 с.

47. Череп А. В., Ярмош В. В. Економіка підприємства: підручник; ДВНЗ «Запоріж. нац. ун-т». Запоріжжя: ЗНУ, 2014. 335 с.

48. Семенда Д. К., Бурляй О. Л., Коротєєв М. А., Семенда О. В. Економіка підприємства: підруч. для студентів ВНЗ; ред.: Д. К. Семенда; Уман. нац. ун-т садівництва. Умань: Сочінський, 2014. 477 с.

49. Стратегія та механізми забезпечення фінансово-економічної безпеки: колект. монографія / Чернігів. нац. технол. ун-т ; за заг. ред. д-ра екон. наук, проф. Ільчука Валерія Петровича. Чернігів: ЧНТУ, 2017. 349 с.

50. Ольшанський О. В., Крамчанінова М. Д. Вплив пандемії COVID-19 на проблеми забезпечення економічної безпеки малих та середніх підприємств. *Економічний вісник Донбасу*. 2021. № 2. С. 78-82.

51. Череп А. В., Худолей Л. В. Використання інструментів забезпечення фінансово-економічної безпеки промислових підприємств: монографія; Запоріж. нац. ун-т. Запоріжжя: Запоріж. нац. ун-т, 2018. 221 с.

52. Polozova T., Musiienko V., Storozhenko O., Peresada O., Geseleva N. Modeling of energy-saving processes in the context of energy safety and security. *Journal of security and sustainability issues*. 2019. № 8 (3). С. 387-397.

53. Polozova T.V., Nicola Jennifer John Elia. Enterprise economic security system: theoretical aspects of formation. Економічні та безпекові виклики сучасного бізнес-середовища: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2020. С. 355-362.

54. Мусієнко В. О., Іванова В. Б. Математичні методи діагностики ймовірності банкрутства як інструментарій забезпечення фінансово-економічної безпеки підприємства. Економічні та безпекові виклики сучасного бізнес-середовища: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ФОП Андреев К.В., 2020. С. 397-408.

55. Мусієнко В. О., Мандзіна В. І. Організаційні аспекти забезпечення економічної безпеки підприємства. *Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта*. Матеріали II Міжнародної науково-практичної конференції (м. Харків, 2 листопада 2021 р.) / За заг. ред. Т. В. Полозової [та ін.]. Харків. ХНУРЕ. 2021. С. 117-118.

56. Мусієнко В. О., Клименко Д. О., Мандзіна В. І. Теоретичні аспекти забезпечення економічної безпеки підприємства. Сучасні економічні стратегії: інновації, безпека та сталий розвиток: колективна монографія / За заг. ред. д.е.н., проф. Т.В. Полозової, д.е.н., проф. І.В. Колупаєвої, к.е.н., доц. О.В. Мурзабулатової Харків: ХНУРЕ, 2021. С. 260-265.