Східноєвропейський національний університет імені Лесі Українки
Факультет економіки та управління
Кафедра економіки, безпеки та інноваційної діяльності підприємства

Олена Скорук

ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА ВИРОБНИЧОГО ПІДПРИЄМСТВА

Конспект лекцій

Луцьк
2017

УДК 334:336(075)
ББК 65.291-983я73-2
С 44

Рекомендовано до друку науково-методичною радою Східноєвропейського національного університету імені Лесі Українки (протокол №__ від _____ 2017 р.)

Рецензенти:

Ліпич Л. Г., д.е.н., професор, декан факультету економіки та управління Східноєвропейського національного університету імені Лесі Українки

Савош Л. В., к.е.н., доцент, зав. кафедри економічної теорії та міжнародної економіки Луцького національного технічного університету

Скорук О. В.
С-44 Фінансово-економічна безпека виробничого підприємства: конспект лекцій / Олена Володимирівна Скорук. – Луцьк : ПП «Поліграфія», 2017. – 148 с.

У навчальному виданні узагальнено теоретичні та методичні засади забезпечення фінансово-економічної безпеки виробничого підприємства за різними функціональними складовими, визначено загрози фінансово-економічній безпеці виробничих підприємств, формування та реалізація стратегії фінансово-економічної безпеки виробничого підприємства як складової його загальної стратегії розвитку.

Рекомендовано студентам 5 курсу спеціальності 073 «Менеджмент» освітньої програми «Управління фінансово-економічною безпекою».

УДК 334:336(075)
ББК 65.291-983я73-2

ЗМІСТ

Передмова

Менеджери, професіонали та фахівці з управління фінансово-економічною безпекою повинні знати закони, принципи та технології ринкової економіки. Вітчизняні підприємства функціонують в умовах існування великої кількості ризиків, небезпек та загроз. Гарантування фінансово-економічної безпеки підприємств має свої особливості. Тому тільки системний підхід до управління підприємством та його фінансово-економічної безпеки може стати запорукою його успіху. Для цього менеджери, професіонали та фахівці повинні ретельно засвоїти та ефективно застосовувати основні способи управління організацією, персоналом і системою фінансово-економічної безпеки. Насамперед необхідно засвоїти основи знань про безпеку підприємництва з огляду на прояв загроз, небезпек та ризиків.

Основними завданнями навчальної дисципліни «Фінансово-економічна безпека виробничого підприємства" є: є ознайомлення управлінців з фінансово-економічної безпеки із особливостями розробки та управління системами безпеки підприємств, особливостями розробки систем безпеки відповідно до вимог міжнародних стандартів; організації та управління захистом майна на підприємстві, організації забезпечення кадрової безпеки на підприємстві, характеристики методів забезпечення надійності персоналу, організації профілактичної роботи серед персоналу по недопущенню правопорушень.

Після засвоєння курсу студент повинен **знати**: механізм управління системою фінансово-економічною безпеки виробничого підприємства; функції і процес управління системою забезпечення фінансово-економічної безпеки виробничого підприємства; завдання та функції служби фінансово-економічної безпеки підприємства; нормативно-методичні механізми формування положення про службу фінансово-економічної безпеки підприємства; нормативно-методичні механізми формування інструкції, що регламентують усі види діяльності підрозділу фінансово-економічної безпеки підприємства та їх персоналу при виконанні службових обов'язків; порядок розроблення посадових інструкцій персоналу підрозділу фінансово-економічної безпеки підприємства; порядок формування та реалізації стратегії фінансово-економічної безпеки підприємства; методи управління системою безпеки підприємства.

Після засвоєння курсу студент повинен **вміти**: вільно й грамотно оперувати термінологічним апаратом організації та управління системою фінансово-економічної безпеки виробничого підприємства; володіти методами розробки перспективних та поточних планів забезпечення фінансово-економічної безпеки підприємств; розробляти положення про службу фінансово-економічної безпеки підприємств; визначати розподіл повноважень і відповідальності між структурними складовими служби фінансово-економічної безпеки підприємства; розробляти штатний розпис підрозділу фінансово-економічної безпеки підприємства.

Структура навчальної дисципліни

Таблиця 1

Назва змістових модулів і тем	Кількість годин				
	Усього	у тому числі			
		Лек.	Практ. (Семі)	Конс.	Сам роб.
1	2	3	4	5	6
Змістовий модуль 1. Теоретичні основи управління фінансово-економічною безпекою виробничого підприємства					
Тема 1. Теоретико-методичні основи фінансово-економічної безпеки виробничого підприємства	13	4	2	1	6
Тема 2. Система фінансово-економічної безпеки виробничого підприємства	11	2	2		7
Тема 3. Організація процесу управління фінансово-економічною безпекою виробничого підприємства	12	2	2	1	7
Тема 4. Організація діяльності служби фінансово-економічної безпеки виробничого підприємства	11	2	2	1	6
Тема 5. Формування стратегії фінансово-економічної безпеки виробничого підприємства як складової його загальної стратегії розвитку	12	2	2	1	7
Тема 6. Реалізація стратегії фінансово-економічної безпеки виробничого підприємства	12	2	2	1	7
Разом за змістовим модулем 1	71	14	12	5	40
Змістовий модуль 2. Забезпечення фінансово-економічної безпеки виробничого підприємства за функціональними напрямами					
Тема 7. Особливості забезпечення фінансової безпеки в системі фінансово-економічної безпеки виробничого підприємства	11	2	2	1	6
Тема 8. Забезпечення інтелектуально-кадрової безпеки виробничого підприємства	12	2	2	1	7
Тема 9. Забезпечення інформаційної безпеки виробничого підприємства	12	2	2	1	7

Продовження табл. 1

1	2	3	4	5	6
Тема 10. Комерційна таємниця та особливості її дотримання на підприємстві	10	2	2		6
Тема 11. Особливості забезпечення силової безпеки виробничого підприємства	11	2	2	1	6
Тема 12. Особливості забезпечення техніко-технологічної та ринкової безпеки виробничого підприємства	11	2	2		7
Тема 13. Ризики в системі фінансово-економічної безпеки виробничого підприємства	12	2	2	1	7
Разом за змістовим модулем 2	79	14	14	5	46
Усього годин	150	28	26	10	86

ЗМІСТОВИЙ МОДУЛЬ І
ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

ТЕМА 1
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

1.1. Сутність фінансово-економічної безпеки виробничого підприємства
1.2. Складові фінансово-економічної безпеки виробничого підприємства, їх характеристика
1.3. Задоволення інтересів як основа забезпечення фінансово-економічної безпеки виробничого підприємства
1.4. Негативні чинники впливу на фінансово-економічну безпеку виробничого підприємства
1.5.Принципи забезпечення фінансово-економічної безпеки виробничого підприємства
1.6. Методичні підходи до оцінки безпеки підприємства

1.1. Сутність фінансово-економічної безпеки підприємства

Термін «безпека» сьогодні розглядається як одна з найвагоміших проблем окремої людини, підприємства, регіону, держави та світової спільноти загалом. Категорія «безпека» безупинно розвивається, а її зміст поступово змінюється й ускладнюється.

Поняття «безпека» (за тлумачним словником В.Даля) – це відсутність загрози, збереженість, надійність, тобто відсутність будь-яких загроз особі, суспільству і державі (об’єктам безпеки).

Безпека – стан захищеності життєво важливих інтересів особи, суспільства, організації від потенційно і реально існуючих загроз або відсутність таких загроз.

В країнах Західної Європи термін «безпека» став уживатися наприкінці XII століття, однак не набув широкого розповсюдження. У XVII–XVIII століттях практично в усіх країнах переважала думка, що головне завдання держави – досягнення загального добробуту та безпеки, а сам термін «безпека» визначався як стан відсутності чи нейтралізації загроз, небезпек, а також створення умов та соціальних інститутів, що його забезпечують.

За часів Російської імперії термін «безпека» почали використовувати для позначення охорони громадського порядку, зумовленого посиленням революційної боротьби. У серпні 1881 року з’явилося «Положення про заходи щодо охорони державного порядку та громадського спокою», в якому вперше визначено поняття «громадська безпека».

У законодавстві Радянського Союзу в 1934 році вперше з’явилося поняття «державна безпека», а в 1977 році в Конституції СРСР (стаття 32) зазначено, що держава виступає гарантом державної безпеки та обороноздатності країни.

Починаючи з 80-х років XX століття велася широкомасштабна наукова розробка поняття «безпека» установами провідних країн світу, найбільш відомі з них Лондонський міжнародний інститут стратегічних досліджень і Стокгольмський міжнародний інститут досліджень миру.

Безпека – це такий стан того чи іншого об'єкта, який дозволяє запобігти зовнішнім і внутрішнім загрозам та сприяє їх нейтралізації для забезпечення ефективного існування цього об'єкта та його стабільного розвитку.

Безпека є складним та багатоаспектним поняттям, яке розглядають на різних рівнях (глобальному, міжнародному, національному, регіональному, локальному та індивідуальному). Розглянемо детальніше окремі рівні безпеки і визначимо зв'язок між ними.

На *міжнародному рівні* безпеки створюються умови для гарантування безпеки окремих держав та їх господарюючих суб'єктів. Розширення інтеграційних зв'язків супроводжується тісним вплітанням економік окремих країн у світову економіку і не лише здійснює на неї вплив залежно від рівня розвитку окремої країни, але й з її боку відчуває сильний вплив, примушуючи кожну країну узгоджувати свою економічну політику з загальними світовими тенденціями та інтересами інших країн-партнерів і сприяти взаємовигідній співпраці між ними.

Безпека на *національному рівні* розглядається як такий стан економіки та інститутів влади, при якому забезпечується гарантований захист національних інтересів, гармонійний, соціально спрямований розвиток країни загалом і достатній її економічний потенціал. Забезпечення безпеки на національному рівні можливе лише за умови ефективної участі кожної країни у міжнародному поділі праці, гармонізації економічних політик окремих країн, сталого соціально-економічного розвитку кожної країни і світової економіки загалом.

Головний документ, який визначає основні засади державної політики, спрямованої на гарантування безпеки держави, – Закон України «Про основи національної безпеки», прийнятий у червні 2003 року. Основний координаційний орган з питань національної безпеки – Рада національної безпеки і оборони України.

Вперше термін «економічна безпека» було використано майже вісімдесят років тому Ф. Рузвельтом. Офіційно він зафіксований у 1985 році, коли на 40-й сесії Генеральної Асамблеї ООН було прийнято резолюцію «Міжнародна економічна безпека».

У структурі національної безпеки економічна безпека посідає особливе місце. Це обумовлено тим, що всі види безпеки так чи інакше не можуть бути достатньою мірою реалізовані без економічного забезпечення. З багаторічного досвіду відомо, що лише надійна та ефективна система забезпечення економічної безпеки є необхідною умовою для стабільного та стійкого соціально-економічного розвитку держави і захисту її незалежності. Тобто, економічна безпека – це фундамент для функціонування всієї системи національної безпеки.

В економічній науці та практиці наведено достатню кількість підходів до визначення поняття «економічна безпека держави». Проте більшість авторів,

визначаючи економічну безпеку держави, виокремлюють лише інтереси людини, суспільства та держави загалом, при цьому інтересам підприємства, які є основною ланкою економіки держави, не приділяють належної уваги.

Під економічною безпекою регіону З. Герасимчук та Н. Вавдіюк розуміють такий стан економічного розвитку регіону, який характеризується найбільш повним та раціональним використанням його економічного потенціалу, здатністю до самовідтворення, захищеністю від дій дестабілізуючих чинників, міцністю взаємозв'язків між елементами регіональної системи, що сприяє задоволенню економічних і соціальних інтересів населення регіону в руслі загальнодержавних інтересів.

Особливе місце в ієрархії рівнів безпеки належить рівню безпеки підприємства, оскільки підприємство – важливий об'єкт економічного життя особистості, регіону, на території якого воно розташоване, і, звісно, держави.

Стабільний розвиток, ефективне функціонування та конкурентоспроможність підприємств перш за все залежать від безпеки їх господарської діяльності. Цей напрям діяльності підприємства охоплює його фінансову, інформаційну безпеку, охорону власного майна та посадових осіб підприємства, захист та права на інтелектуальну власність тощо.

Очевидним є той факт, що підприємницька діяльність є привабливою для таких антисуспільних явищ, як корупція, організована злочинність, шахрайство, рейдерство, недобросовісна конкуренція тощо.

Сучасні умови діяльності підприємств є доволі складними та небезпечними через наявність численних загроз. Джерела загроз дислокуються як у зовнішньому, так і у внутрішньому середовищі підприємств. За таких умов однією з головних цілей діяльності підприємств має бути забезпечення їх фінансово-економічної безпеки.

Сьогодні практично кожне підприємство в Україні має потребу в забезпеченні власної фінансово-економічної безпеки, а отже, – і у професіоналах в цій сфері.

Перші вітчизняні наукові дослідження, які стосуються проблем забезпечення безпеки підприємств, з'явилися з *середини 90-х років XX століття*. Значного поширення набуло поняття «економічна безпека підприємства», сутність якого першочергово визначалась як збереження комерційної таємниці та іншої інформації підприємства, що не підлягає розголошенню. Сьогодні це поняття набуло нових ознак і розглядається набагато ширше, охоплюючи не тільки захист інформаційних ресурсів, а й інші сфери діяльності підприємства.

В економічній літературі існують різні підходи до визначення сутності економічної безпеки підприємства:

– перший з них – «ресурсно-функціональний» – передбачає визначення економічної безпеки підприємства «*як стану найбільш ефективного використання корпоративних ресурсів (ресурсів капіталу, персоналу, інформації, технології, техніки, прав і підприємницьких можливостей) для запобігання загроз та забезпечення стабільного функціонування підприємства в теперішній час і в майбутньому»;* цей підхід отримав найбільший розвиток

на практиці, представником підходу є російський вчений Є. А. Олейніков. Подібний підхід до визначення суті економічної безпеки підприємства застосовано в працях С. Ф. Покропивного та Т. Б. Кузенко. Цей підхід має комплексний характер і фактично ототожнюється з ефективністю діяльності підприємства;

– другий підхід визначає економічну безпеку підприємства з позиції здатності підприємства ефективно функціонувати та захищеності від негативного впливу середовища діяльності підприємства. *«Економічна безпека підприємства – це захищеність його діяльності від негативних впливів зовнішнього середовища, а також здатність швидко усувати різноваріантні загрози або пристосуватися до існуючих умов, що не позначаються негативно на його діяльності"* (Ковальов Д. і Сухорукова Т.). Вважаємо, що недоліком цього визначення є певне обмеження щодо виявлення негативного впливу на діяльність підприємства, оскільки на підприємство та його економічну безпеку негативно впливають не тільки фактори зовнішнього, а й внутрішнього середовища (кадровий потенціал, техніко-технологічне оснащення, фінансове забезпечення тощо). Крім цього, не завжди можна виявити умови та їх здатність впливати (позитивно чи негативно) на діяльність підприємства.

Прихильниками цього підходу ще є О. М. Бандурка, В. Є. Духов, К. П. Петрова та І. М. Червяков, С. Б. Довбня та Н. Ю. Гічова;

– третій підхід визначає економічну безпеку підприємства з позиції захисту його економічних інтересів, а саме як *«міру гармонізації й інтеграції в часі і просторі інтересів підприємства з інтересами суб'єктів зовнішнього середовища, що взаємодіють з ними* (В. Козаченко, О. М. Ляшенко та В. П. Пономарьов).

Цей підхід значно ускладнює дослідження економічної безпеки підприємства, оскільки врахувати та визначити ступінь гармонізації інтересів підприємства з інтересами суб'єктів зовнішнього середовища проблемно через значну кількість інтересів усіх суб'єктів середовища. Існують суб'єкти зовнішнього середовища, що не взаємодіють безпосередньо з підприємством, проте опосередковано впливають на його діяльність.

Соснін А. С. та Пригунов П. Я. визначають економічну безпеку підприємства як стан захищеності його життєво важливих та законних інтересів від зовнішніх і внутрішніх загроз у різних протиправних формах, що гарантує його стабільний розвиток відповідно до задекларованих цілей.

– четвертий підхід визначає економічну безпеку підприємства з позицій стану діяльності підприємства та його господарських відносин: *економічна безпеки підприємства – стан юридичних та виробничих відносин, матеріальних та інтелектуальних ресурсів, який забезпечує ефективне функціонування, фінансово-комерційне процвітання, а також науково-технічний та соціальний розвиток підприємства (*О. Ф. Долженков, Ж. О. Жуковська, О. М. Головченко). Прихильниками цього підходу ще є О. А. Грунін та С. О. Грунін;

– окремі автори підходять до трактування сутності поняття «економічна безпека підприємства» *з позиції сукупності методів, засобів та чинників, які*

забезпечують умови для функціонування підприємства. Прихильниками підходу є О. Раздіна, О. Мітрофанов, Н. Капустін.

У запропонованих для розгляду визначеннях дослідники переважно зосереджують увагу на таких аспектах, як стан найбільш ефективного використання ресурсів підприємства, його ринкових можливостей, захист інтересів підприємства, здатність протистояти загрозам та небезпекам, стан юридичних та виробничих відносин підприємства, здатність підприємства до ефективного функціонування та успішного розвитку тощо. І лише окремі науковці (О. В. Ареф'єва та Р. М. Федоренко) розглядають економічну безпеку як сукупний динамічний стан підприємства, який дозволяє формувати та здійснювати власну стратегію розвитку. Цей підхід не знайшов значної кількості прихильників і не зазнав широкого використання в науковій літературі. Проте саме він вказує на те, що економічна безпека дозволяє підприємству швидко адаптуватися до змін зовнішнього та внутрішнього середовищ, забезпечуючи йому стратегічний розвиток.

Отже, економічна безпека підприємства передбачає створення умов для досягнення цілей діяльності підприємства незалежно від негативного впливу зовнішніх та внутрішніх чинників.

Сьогодні широко використовують поняття «фінансово-економічна безпека», проте єдиного підходу до визначення його сутності нема.

Окремі науковці ототожнюють це поняття із фінансовою складовою.

Як відомо, між економічною і фінансовою діяльністю господарюючих суб'єктів, існує тісний взаємозв'язок: деякі категорії , з одного боку, є економічними за своєю суттю, а з іншого – фінансовими. Так прибуток є прямим результатом економічної діяльності підприємства, і водночас – він є фінансовим результатом, фінансовим ресурсом підприємства, який підприємство може свідомо витрачати на свій розвиток, на розвиток та мотивацію персоналу, на створення комфортних умов для праці та відпочинку, на розширення бізнесу та його диверсифікацію. Тому, до наукового обігу ввійшло поняття фінансово-економічної безпеки підприємства, що очевидно підкреслює взаємозалежність економічної та фінансової діяльності підприємства та визначальну роль фінансів у економічній сфері будь-якого суб'єкта господарювання.

Н. Ю. Подольчак, В. Я. Карковська під **фінансово-економічною безпекою підприємства** необхідно розуміти захищеність потенціалу підприємства у різних сферах діяльності від негативної дії зовнішніх і внутрішніх чинників, прямих або непрямих загроз, а також здатність суб'єкта до відтворення. Ці ж автори пишуть, що фінансово-економічна безпека – це стан і здатність фінансово-економічної системи протистояти небезпеці руйнування її оргструктури і статусу, а також перешкодам у досягненні цілей розвитку.

Столбов В.Ф. та Шаповал Г.М. вважають, що під **фінансово-економічною безпекою підприємства** слід розуміти стан захищеності його ресурсів та інтелектуального потенціалувід наявних та потенційних загроз зовнішнього і внутрішнього середовища його функціонування, який

характеризується високими фінансовими показниками діяльності та перспективою економічного розвитку в майбутньому.

Як вважають О. Л. Трухан та М. О. Кокнаєва, **фінансово-економічна безпека підприємства** трактується одночасно з двох позицій – статичної (як результат діяльності підприємства на певну дату) та динамічної (розвиток підприємства в умовах фінансово-економічної безпеки у короткостроковій та довгостроковій перспективі.

І. П. Мойсеєнко та О. М. Марченко поняття **фінансово-економічної безпеки підприємства** визначають як такий його фінансово-економічний стан, який забезпечує захищеність його фінансово-економічних інтересів від внутрішніх і зовнішніх загроз та створює необхідні фінансово-економічні передумови для стійкого розвитку в поточному та довгостроковому періодах.

Фінансово-економічна безпека підприємства є складною системою, яка включає певний набір внутрішніх характеристик, спрямованих на забезпечення ефективності використання корпоративних ресурсів за кожним напрямом діяльності. Таким чином безпеку варто розглядати через призму її функціональних складових, що дозволяє: здійснювати моніторинг чинників, які впливають на стан як функціональних складових, так і фінансово-економічної безпеки загалом; досліджувати процеси, які здійснюють вплив на забезпечення фінансово-економічної безпеки; проводити аналіз розподілу і використання ресурсів підприємства; вивчати економічні індикатори, що відображають рівень забезпечення функціональних складових; розробляти заходи, які сприятимуть досягненню високого рівня складових, що призведе до посилення фінансово-економічної безпеки підприємства загалом.

Фінансово-економічна безпека підприємства розглядає діяльність підприємства в динамічному та статичному аспектах, що дозволяє реалізовувати його потенціал за визначеними складовими, запобігати виникненню або нейтралізувати негативні чинники і забезпечувати цілеспрямований розвиток.

Фінансово-економічна безпека підприємства – стан захищеності життєво важливих інтересів підприємства від різноманітних внутрішніх та зовнішніх негативних чинників, що гарантує найбільш ефективне використання корпоративних ресурсів підприємства для забезпечення стабільного функціонування та динамічного розвитку.

Особливості фінансово-економічної безпеки підприємства:

– фінансово-економічна безпека підприємства – одна з найважливіших умов його ефективної та результативної діяльності;

– фінансово-економічна безпека підприємства – комплексне поняття, вона пов’язана з усіма напрямами його виробничо-господарської, фінансової та комерційної діяльності;

– рівень економічної безпеки змінюється під впливом низки зовнішніх та внутрішніх чинників (методи управління та організації виробництва, ефективні бізнес-процеси, рівень оподаткування, зв’язки з постачальниками і споживачами тощо);

– фінансово-економічна безпека підприємства – необхідна умова розвитку підприємства незалежно від його виду економічної діяльності та рівня розвитку.

Фінансово-економічна безпека підприємства є, з одного боку, вагомою компонентою конкурентоспроможності підприємства, з іншого боку, компонентою безпеки держави.

Існує багато наукових поглядів на сутність поняття «фінансово-економічна безпека», але його варто досліджувати з метою формування оптимальної системи та механізму управління фінансово-економічною безпекою.

Фінансово-економічна безпека підприємства є однією з найважливіших умов нормального функціонування і розвитку сфери підприємництва в економіці будь-якої країни. Це пов'язано, насамперед, з конкуренцією на ринку, як на внутрішньому, так і на зовнішньому. Фінансово-економічна безпека підприємства є основою його стабільного розвитку, рушійною силою для досягнення поставлених цілей, а також тих цілей, що намічені у перспективі.

1.2. Складові фінансово-економічної безпеки підприємства, їх характеристика

В економічних наукових джерелах вітчизняних та зарубіжних науковців знаходимо різні підходи до виділення складових економічної безпеки підприємства. Так, представники ресурсно-функціонального підходу виділяють сім функціональних складових економічної безпеки підприємства, а саме: фінансову, інтелектуальну й кадрову, техніко-технологічну, політико-правову, інформаційну, екологічну, силову.

Д. Ковальов та Т. Сухорукова пропонують чотири складові – технологічну, ресурсну, фінансову та соціальну.

На думку С. М. Ілляшенка, поняття економічної безпеки підприємства охоплює фінансову, інтелектуальну, кадрову, технологічну, правову, екологічну, інформаційну, силову, ринкову та інтерфейсну складові.

Кравчук О. Я. та Кравчук П. Я. запропонували свою декомпозицію безпеки підприємства як складної системи, взявши за основу структуризацію безпеки представників ресурсно-функціонального підходу. Так, на їхню думку, сутність корпоративної безпеки реалізується у таких складових (підсистемах другого порядку): фінансово-економічної, інтелектуально-кадрової, техніко-технологічної, інституційно-правової, інформаційної та силової.

На думку І. О. Бородіна, система корпоративної безпеки містить економічну, інформаційну та соціальну підсистеми, кожна з яких має зворотний зв'язок, який допомагає коригувати її ефективність за рахунок використання внутрішніх ресурсів у випадку зниження реального рівня безпеки порівняно з бажаним рівнем.

Окремі науковці вважають, що досягнення економічної безпеки підприємства здійснюється за такими складовими: ринкова, ресурсна, фінансова, кадрова, техніко-технологічна, інформаційна, безпека якості продукції.

Функціональні складові фінансово-економічної безпеки підприємства – це сукупність основних напрямів його фінансово-економічної безпеки, кожна з яких характеризується власним змістом, набором функціональних критеріїв і способом забезпечення.

Доцільно виділяти такі **функціональні складові фінансово-економічної безпеки:**

– *фінансова* (вважається провідною та вирішальною, оскільки за ринкових умов господарювання фінанси є «двигуном» будь-якої економічної системи). Сутність фінансової безпеки підприємства полягає у досягненні та утриманні його фінансової стійкості, ліквідності, платоспроможності, забезпеченні оборотності активів та прибутковості, тобто характеризує фінансову забезпеченість діяльності підприємства. Ця складова також проявляється у максимізації обсягів реалізації продукції за рахунок оптимізації асортименту, ритмічності реалізації продукції та загальної ефективності збутової діяльності.

Центральне місце у системі фінансово-економічної безпеки підприємства належить фінансовій безпеці, яка відображає мету та узагальнює результати його господарської діяльності.

Це пояснюється тим, що рівень фінансової безпеки будь-якого підприємства визначає його можливості забезпечувати інші складові його фінансово-економічної безпеки. І навпаки, зміни в будь-якій сфері підприємства в кінцевому результаті відображаються у його фінансовій безпеці;

– *інтелектуально-кадрова* (належний рівень економічної безпеки підприємства залежить від професіоналізму працюючих на підприємстві кадрів, складу кадрів). Вона виявляється у забезпеченні підприємства персоналом, його високої професійної підготовки, мотивації і стимулюванні працівників та належного рівня їх соціального забезпечення, а також налаштуванні такої взаємодії між окремими елементами управлінської системи, яка забезпечить необхідний рівень економічної безпеки підприємства та ефективність його діяльності;

– *техніко-технологічна* (економічна безпеки залежить від ступеня відповідності застосовуваних на підприємстві техніки та технологій найкращим світовим аналогам). Техніко-технологічна безпека підприємства характеризує наявність виробничо-технічної структури основних засобів, рівень технологічного розвитку підприємства, технологічний потенціал підприємства;

– *політико-правова* (полягає у всебічному правовому забезпеченні діяльності підприємства, дотриманні чинного законодавства);

– *інформаційна* (полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства). Сутність інформаційної безпеки полягає у збиранні, систематизації і зберіганні інформації, аналізу вірогідності інформації, захисту інформації від несанкціонованого доступу;

– *екологічна* (полягає у дотриманні діючих екологічних норм, мінімізації втрат від забруднення навколишнього середовища);

– *силова* (полягає в забезпеченні фізичної безпеки працівників підприємства (в першу чергу керівників) та збереженні його майна;

– *ринкова* (відображає конкурентоспроможність підприємства, його конкурентну позицію і здатність протидіяти конкурентному тиску, адаптаційні можливості до змін ситуації на ринку, можливості та перспективи реалізації продукції підприємства);

– *інтерфейсна безпека* характеризує надійність взаємодії підприємства з контрагентами (постачальниками, торговими та збутовими посередниками, інвесторами, споживачами та ін.). Ця складова економічної безпеки підприємства пов'язана з особливостями відносин, які сформувалися між підприємством і постачальниками сировини та матеріалів. Умовами забезпечення цієї складової економічної безпеки підприємства є: тривалість та надійність відносин із постачальниками; оптимальний рівень цін на сировину, наявність достатньої кількості якісної сировини, відсутність значної залежності підприємства від постачальника.

Всі ці складові економічної пов'язані між собою.

Наприклад, зменшення рівня техніко-технологічної безпеки через використання застарілого обладнання спричиняє збільшення собівартості продукції і, відповідно, зниження її конкурентоспроможності. Це, в свою чергу, означає втрату підприємством певної частки ринку, виручки від реалізації, прибутку, що очевидно, зменшує можливості підприємства до самофінансування, розширеного відтворення.

Використання недостатньо кваліфікованої робочої сили може мати наслідком брак продукції, а це прямі збитки, і, відповідно, зниження прибутку та рівня фінансової безпеки підприємства.

Фінансово-економічна безпека підприємства – комплексне поняття. Кожна її складова розглядається і як самостійна система, і як елемент складної системи: економіко-виробничої системи підприємства (за горизонтальною структурою) або складовим елементом економічної безпеки держави (за вертикальною структурою). Тому теоретичною основою дослідження фінансово-економічної безпеки підприємства є системний підхід.

Виокремлення функціональних складових дозволяє приймати ефективні управлінські рішення щодо кожної з них та для забезпечення безпеки підприємства загалом.

1.3. Принципи забезпечення фінансово-економічної безпеки виробничого підприємства

Основою забезпечення фінансово-економічної безпеки є принципи, у відповідності до яких відбувається процес забезпечення фінансово-економічної безпеки. **Основні принципи забезпечення безпеки підприємств:**

1. Принцип системності – керівництву підприємства слід підходити до процесу забезпечення безпеки комплексно, не применшуючи значення окремих складових.

2. Принцип обґрунтованості та економічної доцільності – обмеженість ресурсів вимагає техніко-економічного обґрунтування рішень із забезпечення безпеки, співставлення можливих збитків і витрат на забезпечення безпеки.

3. Законності, тобто верховенства законів України в процесі забезпечення безпеки.

4. Наукової обґрунтованості, що передбачає організацію служби безпеки та процесу забезпечення безпеки підприємства на основі об'єктивних економічних законів і закономірностей, сучасних наукових досліджень, вітчизняного та зарубіжного передового досвіду в сфері безпеки, новітніх досягнень науково-технічного прогресу.

5. Збалансованості інтересів власників підприємства та трудового колективу, постачальників сировини та споживачів продукції, держави та фінансово-кредитних установ.

6. Своєчасності реагування на внутрішні та зовнішні негативні впливи на основі аналізу і прогнозування ситуації, можливих негативних чинників.

7. Гнучкості, тобто здатності системи безпеки швидко змінювати моделі та інструменти захисту відповідно до змін внутрішнього та зовнішнього середовищ діяльності підприємства.

8. Безперервності, що передбачає постійний моніторинг ситуації та придатність системи захисту не лише у момент виявлення негативних чинників, а постійно.

9. Адекватності та достатності, що полягає у виборі інструментів і засобів захисту відповідно до масштабів та наслідків впливу негативних чинників.

10. Централізації управління, що передбачає чітку організацію роботи підрозділу (служби) економічної безпеки підприємства, взаємоузгодженість та координацію діяльності всіх структурних структурних підрозділів.

Належний рівень забезпечення фінансово-економічної безпеки можливий за умови дотримання всіх зазначених принципів.

1.4. Задоволення інтересів як основа забезпечення фінансово-економічної безпеки виробничого підприємства

Інтереси підприємства – усвідомлені, матеріалізовані та конкретизовані керівництвом потреби підприємства (збільшення обсягу продажу продукції, завоювання ринкової ніші, покращення іміджу підприємства тощо).

Різноманіття інтересів підприємства зумовлює необхідність їх систематизації за рядом ознак, що дасть змогу їх чітко формулювати, виділяти з них пріоритетні, визначати заходи щодо їх реалізації та захисту, контролювати ступінь їх досягнення.

Класифікація інтересів виробничого підприємства.

1. За сутністю інтереси поділяються:

– *економічні інтереси* полягають у найефективнішому використанні економічних ресурсів підприємства;

– *фінансові інтереси* проявляються в забезпеченні оптимальної структури капіталу, фінансової стійкості та ліквідності, високої оборотності активів;

– *соціальні інтереси* полягають у належному соціальному забезпеченні та захисті працівників, що є запорукою високої продуктивності праці,

сприятливого соціально-психологічного клімату у колективі, позитивного соціального іміджу підприємства);

– *ринкові інтереси* характеризуються мірою задоволення потреб споживачів продукції, ефективністю просування та стимулювання збуту продукції, зростання частки ринку підприємства;

– *технологічні інтереси* полягають у забезпеченні високого технологічного рівня оснащеності підприємства, прогресивності технологій, що використовуються, високого рівня механізації та автоматизації виробництва та технічної оснащеності праці, а також у наявності сучасних власних науково-технічних розробок;

– *виробничі інтереси* полягають підвищенні продуктивності праці, покращенні інноваційно-інвестиційного забезпечення виробництва, пошук резервів зниження собівартості продукції);

– *інформаційні інтереси* полягають в отриманні вчасної та достовірної інформації для прийняття ефективних управлінських рішень.

2. За масштабом інтереси поділяються на:

– *глобальні інтереси*, які охоплюють усі сфери на напрями діяльності підприємства;

– *локальні інтереси*, які проявляються щодо окремих сфер чи видів діяльності підприємства.

3. За суб'єктами виділяють:

– *інтереси власників* полягають у стабільному функціонуванні та розвитку підприємства, отриманні максимальної віддачі на вкладений капітал;

– *інтереси керівництва* полягають у забезпеченні стабільного та ефективного функціонування підприємства та в отриманні належного рівня оплати і умов праці, що визначаються контрактом;

– *інтереси трудового колективу* полягають у створенні належних умов праці та відпочинку, дотриманні норм охорони праці та техніки безпеки, отриманні високого рівня матеріальної винагороди за виконану роботу, гарантуванні соціального захисту та допомоги працівникам.

4. За вагомістю інтереси поділяють на:

– *першочергові (дуже важливі);*

– *другорядні (важливі);*

– *опосередковані (неважливі).*

Вагомість тих чи інших інтересів підприємства визначається поточною економічною кон'юнктурою в країні, фінансовим станом підприємства, галузевими особливостями, прогнозами розвитку підприємства, економіки країни.

5. За ймовірністю реалізації інтереси поділяють на:

– *реальні;*

– *потенційні;*

– *майже недосяжні (малоймовірні).*

Можливість реалізації інтересів визначається насамперед наявністю ресурсів, обґрунтованістю цілей діяльності, станом та перспективами розвитку вітчизняної та світової економік.

6. За рівнем реалізації інтереси поділяють на:

– *міжнародні* полягають у наявності інтересів підприємства на міжнародних ринках товарів, технологій, капіталів, праці;

– *національні;*

– *регіональні*.

7. Залежно від часу реалізації виділяють інтереси:

– *довгострокові*, термін реалізації яких становить 5-10 років і більше;

– *середньострокові*, передбачають реалізацію протягом 3-5 років;

– *короткострокові*, які є досяжними у найближчій перспективі.

8. За сферою виникнення інтереси поділяються на:

– *інтереси у сфері виробництва;*

– *інтереси у сфері торгівлі;*

– *сільськогосподарські інтереси;*

– *інтереси у сфері інтелектуальної діяльності.*

9. За правовим статусом виокремлюють інтереси :

– *законні інтереси* – реалізація яких передбачає використання законних методів, інструментів і шляхів досягнення;

– *незаконні інтереси*, втілення яких обумовлює необхідність порушення чинних правових норм та законодавчих актів.

Складним питанням є встановлення показників, які будуть визначати інтереси підприємства.

1.5. Негативні чинники впливу на фінансово-економічну безпеку виробничого підприємства

Поряд з поняттям «безпека» необхідно розглядати споріднені між собою поняття – «ризик», «загроза», «небезпека».

Ризик, загроза та небезпеки є негативними чинниками впливу на фінансово-економічну безпеку підприємства, які мають різну інтенсивність.

Підприємству необхідно реагувати на ризики та загрози, оскільки їх подолати значно легше, ніж небезпеки.

Економічний ризик підприємства – можливість настання негативних подій, явищ, процесів чи несприятливих умов зовнішнього та внутрішнього середовищ, що можуть призвести до непередбачуваних негативних наслідків у процесі діяльності підприємства, до зниження фінансово-економічної безпеки.

Економічна загроза підприємства – реальна негативна дія чинників зовнішнього та внутрішнього середовищ, за якої відбуваються небажані зміни стану фінансово-економічної безпеки.

Економічна небезпека підприємства – деструктивний вплив негативних чинників на діяльність підприємства, що може призвести до його занепаду чи банкрутства.

Для того, щоб забезпечити фінансово-економічну безпеку підприємства, необхідно сформувати чіткий механізм виявлення та ідентифікації негативних чинників впливу на фінансово- економічну безпеку.

Аналізуючи господарську діяльність підприємства, потрібно враховувати всі негативні чинники, з якими воно стикається. Ефективність організації

виявлення та нейтралізації негативних чинників багато в чому визначається їхньою класифікацією.

Класифікація негативних чинників впливу на фінансово-економічну безпеку підприємства – це їх розподіл на окремі групи за певними ознаками для досягнення конкретної мети. Науково обґрунтована класифікація негативних чинників дозволить чітко визначити місце кожної з них у загальній системі і створить можливості для ефективного розроблення та використання відповідних методів і прийомів нейтралізації ризиків, загроз та небезпек.

Класифікація негативних чинників впливу на фінансово-економічну безпеку підприємства за різними ознаками:

1) джерело виникнення:

– внутрішні – ті, що виникають у внутрішньому середовищі підприємства (низький рівень менеджменту, низький рівень кваліфікації персоналу, нестійкий фінансовий стан тощо);

– зовнішні – ті, що виникають у макро- та мікросередовищі діяльності підприємства (зниження купівельної спроможності споживачів, істотний рівень інфляції, нестабільність господарського і податкового законодавства, посилення конкуренції в галузі порушення постачань матеріалів, сировини та інші);

2) можливість уникнення дії негативного впливу:

– нівельовані – ті, які вдалося вчасно виявити та нейтралізувати, які не встигли заподіяти шкоди;

– неминучі – ті, яких уникнути неможливо в силу певних обставин, а можливо лише пом’якшити їх вплив;

3) сфера охоплення:

– системні – ті, що впливають на діяльність підприємства як системи. За своїм характером є найбільш руйнівними і призводять до повного порушення цілісності системи (до них можна віднести тероризм);

– елементні – ті, що впливають лише на окремі елементи структури системи, мають постійний характер і можуть бути небезпечними при умові невідстеження їх розвитку;

4) суб’єктивна зумовленість:

– об’єктивні – ті, що виникають не з волі конкретного підприємства або його окремих працівників;

– суб’єктивні – ті, що виникають внаслідок неефективної роботи підприємства загалом або окремих його працівників;

5) наслідки впливу (обсяги втрат або збитків):

– беззбиткові – ті, в результаті дії яких підприємство не несе збитків та будь-яких матеріальних, фінансових чи інших втрат;

– збиткові – ті, в результаті дії яких підприємство несе незначні збитки та невеликі матеріальні, фінансові чи інші втрати;

– руйнівні (катастрофічні) – ті, в результаті дії яких підприємство несе значні збитки та суттєві матеріальні, фінансові чи інші втрати, що загрожують його подальшій діяльності;

6) ймовірність реалізації:

– реальні – ті, що негативно впливають на діяльність підприємства і їхній шкідливий вплив можна виміряти;

– потенційні – ті, негативний вплив яких може проявитися в майбутньому за певних обставин;

7) етап життєвого циклу підприємства:

– негативні чинники на етапі створення та початкової організації діяльності підприємства;

– негативні чинники на етапі становлення і розвитку підприємства;

– негативні чинники на етапі санації та відродження підприємства;

– негативні чинники на етапі банкрутства (ліквідації) підприємства;

8) об'єкти впливу:

– персоналу – ті, негативний вплив яких проявляється щодо персоналу підприємства;

– фінансовим ресурсам – ті, негативний вплив яких проявляється у втраті фінансових активів, зменшенні власного капіталу, погіршенні загального фінансового стану підприємства;

– матеріальним активам – ті, негативний вплив яких проявляється у втраті підприємством кількості та якості виробничих засобів підприємства;

– інтелектуальним ресурсам (нематеріальним активам) – ті, негативний вплив яких проявляється у незаконному доступі до науково-технічних розробок, винаходів, розголошенні конфіденційних секретів;

9) суб'єкти впливу:

– обумовлені діями з боку персоналу підприємства;

– обумовлені діями з боку учасників зовнішнього ринкового середовища (конкурентів, посередників, постачальників, покупців тощо);

– обумовлені діями з боку злочинних угрупувань;

10) тривалість впливу:

– довгострокові, термін дії наслідків яких триває від 5 до 10 років і більше;

– середньострокові, термін дії наслідків яких триває від 1 до 5 років;

– короткострокові, негативні наслідки яких проявляються протягом поточної діяльності підприємства до 1 року;

11) функціональна спрямованість (складові фінансоо-економічної безпеки):

– негативні чинники впливу на стан техніко-технологічної безпеки;

– негативні чинники впливу на стан інформаційної безпеки тощо;

12) характер впливу:

– перманентні – постійно існуючі ризики, загрози та небезпеки фінансово-економічній безпеці підприємства;

– дискретні – ті, що характеризуються переривчастістю;

– епізодичні – поодинокі ризики, загрози та небезпеки, які проявляються час від часу.

Класифікація негативних чинників дозволить вчасно їх виявляти та розробляти ефективні методи нейтралізації. Виявлення та ідентифікація негативних чинників впливу – одне з найважливіших завдань гарантування фінансово-економічної безпеки підприємства.

1.6. Методичні підходи до оцінки безпеки підприємства

Існують такі найбільш поширені методи оцінки рівня безпеки підприємства: **індикаторний, тримірний, ресурсно-функціональний, прибутково-інвестиційний** тощо. Одні з них більш придатні для застосування в сучасних умовах господарювання підприємства, інші викликають певні труднощі на етапі їх практичного використання.

1. Індикаторний метод передбачає визначення рівня безпеки за допомогою індикаторів, недотримання рівня яких призводить до погіршення стану безпеки.

Індикатори представляють собою кількісні та якісні величини, які характеризують граничні значення різних функціональних показників. Методика оцінки безпеки підприємства полягає у порівнянні фактичних показників діяльності підприємства з встановленими індикаторами.

Оцінка рівня безпеки підприємства на основі цього методичного підходу передбачає визначення груп індикаторів, що характеризують основні напрями діяльності підприємства.

На основі порівняння фактичних показників діяльності підприємства з граничними значеннями-індикаторами формується висновок про рівень безпеки. На нашу думку, основною проблемою використання індикаторного методу, з якою часто стикаються науковці, є розробка системи індикаторів і впровадження її на практиці. І полягає вона у встановленні рівня індикатора, який необхідно зіставити з фактичними показниками діяльності суб'єкта господарювання. Ця проблема зумовлена відсутністю чіткої методичної бази щодо визначення показників-індикаторів, які враховували б особливості діяльності кожного суб'єкта господарювання відповідно до його виду економічної діяльності.

2. Найбільш визнаний та широковживаний **ресурсно-функціональний метод** оцінки рівня економічної безпеки підприємства, який базується на оцінці ступеня використання корпоративних ресурсів підприємства, необхідних для досягнення цілей бізнесу, за кожною функціональною складовою безпеки підприємства. Рівень безпеки підприємства оцінюють шляхом визначення сукупного критерію, який, у свою чергу, розраховується на основі значень часткових функціональних критеріїв безпеки підприємства та їх питомої ваги значимості.

Часткові функціональні критерії розраховуються як відношення сукупної відверненої шкоди за окремою функціональною складовою до суми витрат на реалізацію заходів з нейтралізації негативних впливів і загальної заподіяної шкоди щодо цієї складової.

3. Критерієм економічної безпеки підприємства, **за прибутково-інвестиційним методом**, є отриманий в результаті взаємодії з суб'єктами зовнішнього середовища прибуток, яким підприємство може розпоряджатися, тобто чистий прибуток.

Саме наявність у підприємства чистого прибутку свідчить про досягнення певного рівня економічної безпеки. Для кількісної оцінки рівня безпеки підприємства здійснюють порівняння обсягу інвестицій підприємства,

здійснених переважно за рахунок реінвестованого прибутку, з обсягом коштів, необхідних для забезпечення безпеки підприємства. Цей метод передбачає визначення суми прибутку, що необхідний для розширеного відтворення капіталу, оскільки вона залежить від конкретної динаміки процесу відтворення, притаманному кожному підприємству.

На основі кількісної оцінки рівня безпеки підприємства дослідник виділяє такі рівні безпеки підприємства, як підтримуючий, мінімальний, дуже низький, низький, середній, високий та дуже високий, залежно від інтенсивності конкуренції в галузі, в межах якої підприємство здійснює свою діяльність.

Запропонований підхід, хоч і має важливе практичне значення, проте у ньому є суттєвий недолік: він не дозволяє оцінити рівень безпеки збиткових підприємств, частка яких у загальній кількості підприємств у 2010 році складала 41,0 %.

4. Тримірний метод до визначення рівня безпеки підприємства передбачає виділення таких її основних форм, як поточної, тактичної і стратегічної безпеки. Особливість цього методу полягає у визначенні рівня безпеки залежно від певного проміжку часу, відповідно до якого вона оцінюється. Загальний рівень економічної безпеки визначається на підставі оцінки всіх трьох складових.

Для оцінки рівня поточної безпеки використовують ряд фінансово-економічних показників, які характеризують рівень фінансової незалежності підприємства, стан ліквідності його активів і можливості своєчасного виконання поточних фінансових зобов'язань, фінансово-економічні результати діяльності підприємства.

З метою визначення рівня тактичної безпеки, яка відображає здатність підприємства до відтворювання у процесі реалізації ним господарської діяльності, що досягається при певному рівні ефективності використання ресурсів підприємства (основних засобів, матеріальних і трудових ресурсів), оцінюють такі її основні складові: виробничо-технічну, інтелектуально-кадрову, комерційну.

Стратегічна безпека характеризує рівень економічного потенціалу, що обумовлює здатність підприємства до подальшого успішного функціонування та водночас є підтвердженням правильності обраного напряму розвитку, відповідності результатів роботи підприємства основним макроекономічним тенденціям. До основних складових стратегічної безпеки дослідники відносять: ринкову, соціальну, інноваційно-технологічну, сировинну й енергетичну, екологічну

5. Метод, який передбачає визначення **узагальненого показника рівня безпеки підприємства.**

Оцінку рівня безпеки підприємства важливо здійснюють за всіма її складовими. Для оцінки рівня безпеки кожної складової безпеки визначають систему аналітичних показників з урахуванням галузевих і ринкових особливостей діяльності підприємства та негативних чинників впливу на безпеку, які зводять до одного комплексного показника кожної складової, що буде об'єктивно відображати стан безпеки за кожним напрямом. Комплексні

показники окремих складових безпеки визначають значення узагальненого показника економічної безпеки, який і буде характеризувати досягнутий рівень безпеки підприємства.

Основні переваги узагальненого показника безпеки підприємства полягають у тому, що він синтезує у собі вплив обраних для дослідження показників і коефіцієнтів та зводить оцінку рівня безпеки до одного кількісного значення, що значно полегшує економічну інтерпретацію отриманих результатів.

6. Для оцінки рівня безпеки підприємства використовують методи, які **засновані на прогнозуванні фінансової неспроможності підприємств**, тобто прогнозуванні банкрутства. Серед них можна виділити кількісні факторні моделі, розроблені науковцями в США: 5-факторна модель Альтмана, шкала Бівера, формула Du Pont, а також маловідомі моделі Ліса, Тишоу, Таффлера, Фулмера, Спрінгейта, узагальнена модель, побудована на основі дискримінантної функції.

Фінансовий стан підприємств із рейтинговим числом R менше від 1 визначається як незадовільний. Чим більше значення R, тим менша ймовірність банкрутства і відповідно вищий рівень безпеки підприємства.

Метод В. В. Ковальова, метод Аргенті, метод Скоуна, методика компанії ERNST&WHINNEY – якісні методи прогнозування банкрутства, які мало застосовуються на практиці українськими підприємствами, оскільки допускають широке використання експертизи і не враховують реальних умов господарювання підприємств.

ТЕМА 2
СИСТЕМА ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

2.1. Сутність, мета та завдання системи фінансово-економічної безпеки виробничого підприємства

2.2. Порядок формування системи фінансово-економічної безпеки виробничого підприємства

2.3. Основні елементи системи фінансово-економічної безпеки виробничого підпримства

2.1. Сутність, мета та завдання системи фінансово-економічної безпеки підприємства

Відомо, що економічна система держави, як матеріальна основа національної безпеки, складається із сотень тисяч господарюючих суб'єктів. Успішне та ефективне вирішення завдань, що стоять перед економікою держави, значною мірою залежить від результативної діяльності підприємств усіх форм власності. Якщо національна економіка спирається на потужну виробничу базу, на міцні, високорозвинені виробничі структури, які спроможні успішно добиватися поставлених ринкових цілей, то і вся сукупність економічних потреб суспільства буде задовольнятися своєчасно та в повному обсязі.

В умовах формування нової економічної системи в Україні, підприємства, що функціонують у різних організаційно-правових формах, організують свою діяльність в умовах невизначеності, непередбаченості дій партнерів і держави. Глибока економічна криза породила велику кількість небезпек і загроз молодому українському бізнесу.

Крім того, на умови розвитку підприємництва суттєво впливають і такі чинники, як нестабільна політична і соціально-економічна ситуація в країні, недосконаліть і часта зміна комерційного законодавства, криміналізація суспільства, корупція тощо. Все це та інше різко актуалізувало проблему забезпечення безпеки підприємства.

В Україні розробка теорії економічної безпеки господарюючих суб'єктів перебуває лише на початковому етапі. У сучасній науковій літературі, яка приділяє професійну увагу теорії безпеки, розкриття сутності теорії економічної безпеки підприємництва, її структури, основних категорій, індикаторів зустрічається досить рідко і не на достатньому науковому рівні.

Переважно забезпечення економічної безпеки підприємництва зводиться до захисту від різного роду економічних правопорушень (крадіжки, рекет, фальсифікація документів, недобросовісна конкуренція, хакерство тощо). Цілком зрозуміло, що ці загрози є важливими і постійно повинні аналізуватися та враховуватися.

В умовах соціалістичної планової економіки держава жорсткими централізованими мірами в основному регулювало економічні відносини. Такі явища, як недобросовісна конкуренція, організована економічна злочинність,

корупція, тіньова економіка існували в незначних обсягах. Для боротьби з ними використовувалася державна система правоохоронних органів. Підприємствам не було потреби приділяти увагу забезпеченню власної економічної безпеки. Слід пам'ятати і те, що збиткові підприємства на чолі з непрофесійними керівниками штучно підтримувалися державою за рахунок перерозподілу створеного національного доходу, надання пільг, дотацій, субсидій тощо.

Така економічна політика держави породжувала появу великої «армії» нерентабельних підприємств. Їх керівники не боялися попасти в «боргову яму», збанкрутувати, їм не потрібно було ризикувати, адже за їх «спинами» стояв власник – держава, яка простить борги, нав'яже споживачу неякісну продукцію, надасть субсидію за рахунок рентабельних підприємств або експорту сировини.

В умовах ринкових відносин підприємства є економічно самостійними. Вони повинні визначати свою економічну політику, формувати портфель замовлень, організовувати як виробництво, так і збут продукції (послуг) і повністю відповідати за результати господарської діяльності. Усе це, безумовно, актуалізує проблему створення власної системи фінансово-економічної безпеки.

Надійний захист фінансово-економічної безпеки підприємства можливий лише за комплексного або системного підходу до її організації. Тому існує таке поняття як **система фінансово-економічної безпеки підприємства.**

Системний підхід базується на принципі цілісності об'єкта дослідження, тобто дослідження його властивостей як єдиного цілого, оскільки ціле (система) володіє такими якостями, якими не володіє жоден його складник. Наявність таких властивостей зумовлена результатом виникнення між елементами синергетичного зв'язку. В кібернетиці та загальній теорії систем під синергетичним зв'язком розуміють такий зв'язок, який за спільної дії окремих елементів системи забезпечує загальний ефект, більший, ніж сума ефектів цих елементів, які б діяли незалежно.

Під час формування системи як єдиного цілого її складники зазнають якісних змін. Створення системи здійснюється за рахунок перетворення структури взаємозв'язків між складниками, а також завдяки розвитку цих складників.

В умовах ринку система фінансово-економічної безпеки необхідна всім суб'єктам господарювання.

Система фінансово-економічної безпеки кожного підприємства є індивідуальною. Дієвість таких систем залежить від чинної в державі законодавчої бази, від обсягу матеріально-технічних і фінансових ресурсів, виділених на її фукціонування, від розуміння кожним працівником важливості гарантування безпеки, а також від досвіду роботи керівників служб безпеки підприємств (підрозділів фінансово-економічної безпеки).

Система фінансово-економічної безпеки підприємства (СФЕБ) – це організована сукупність засобів, методів, організаційно-управлінських, режимних, технічних, профілактичних та інших заходів, спрямованих на реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх негативних чинників і досягнення цілей діяльності.

Виділяють такі характеристики системи фінансово-економічної безпеки підприємства:

1. Система фінансово-економічної безпеки не може бути типовою, вона є *унікальною* на кожному підприємстві, оскільки залежить від особливостей кожного підприємства (рівня розвитку, структури, розміру, виробничого потенціалу та ефективності його використання, напряму діяльності, кваліфікації кадрів, виробничої дисципліни, конкурентного середовища, місця розташування, наявності секретних матеріалів та ступеня їх секретності тощо).

2. Система фінансово-економічної безпеки підприємства є *відносно відокремленою*, оскільки вона функціонує як окремий структурний елемент. Відносна відокремленість пояснюється тим, що багато завдань, які постають перед системою фінансово-економічної безпеки підприємства, не можуть бути виконані самостійно, без необхідних рішень, що приймаються на більш високому рівні, передусім на державному.

Підрозділ фінансово-економічної безпеки (служба безпеки) конкретного підприємства залежить також від активності протидії служб безпеки конкурентів та, в першу чергу, від їх розвідувальних підрозділів, Вона створюється та функціонує на основі прийнятих законодавчих актів в країні, наявності та можливості придбати засоби захисту, рівня підготовки та кваліфікації кадрів тощо.

3. Система фінансово-економічної безпеки підприємства є *комплексною.* Вона повинна забезпечити безпеку кадрову, екологічну, інформаційну та ін. Тому до її складу повинні входити відповідні засоби, заходи, ресурси тощо. Лише комплексність системи фінансово-економічної безпеки може забезпечити відповідну надійність безпеки підприємства.

4. Основним положенням є *дієвість та ефективність* фінансово-економічної безпеки, оскільки унікальність, самостійність та комплексність системи ФЕБ не дає жодної гарантії, що ця система буде діяти, окрім того, діяти ефективно.

Мета системи фінансово-економічної безпеки виробничого підприємства – передбачення, прогнозування, своєчасне виявлення та протидія як внутрішнім, так і зовнішнім негативним чинникам, досягнення та збереження стабільного функціонування і забезпечення динамічного розвитку підприємства.

Така здатність підприємства надасть можливість, навіть в умовах світової кризи, стійко функціонувати та прогресивно розвиватися.

До основних завдань системи фінансово-економічної безпеки виробничого підприємства належать:

– захист законних інтересів підприємства та його працівників;

– прогнозування можливих негативних чинників фінансово-економічній безпеці;

– організація діяльності із запобігання негативним чинникам (розробка превентивних заходів);

– виявлення, аналіз та оцінювання впливу негативних чинників фінансово-економічній безпеці;

– ухвалення рішень і організація діяльності з обмеження впливу негативних чинників фінансово-економічній безпеці;

– відшкодування матеріального і морального збитку, нанесеного деструктивним впливом негативних чинників;

– формування позитивного іміджу підприємства з метою ефективної реалізації планів його діяльності та статутних цілей;

– постійне удосконалення системи фінансово-економічної безпеки;

– контроль за ефективністю функціонування системи фінансово-економічної безпеки підприємства;

– організація взаємодії з правоохоронними органами з метою захисту законних інтересів підприємства;

– формування власної служби безпеки (підрозділу фінансово-економічної безпеки), адекватної небезпекам і загрозам.

З урахуванням перерахованих завдань, конкурентного середовища, специфіки діяльності підприємства будується його система фінансово-економічної безпеки.

У кожного начальника служби безпеки свій підхід до вирішення проблеми формування системи фінансово-економічної безпеки.

2.2. Порядок формування системи фінансово-економічної безпеки виробничого підприємства

Алгоритм формування системи фінансово-економічної безпеки повинен вміщувати такі етапи:

Етап 1. Вивчення специфіки діяльності підприємства, визначення його місця на ринку, штатного розпису, знайомство з персоналом підприємства.

Етап 2. Аналіз зовнішніх та внутрішніх негативних чинників. Ознайомлення із кризовими ситуація на підприємстві, їх причини і результати вирішення.

Етап 3. Проведення аудиту наявних на підприємстві заходів щодо забезпечення фінансово-економічної езпеки та аналіз їх відповідності виявленим негативним чинникам.

Етап 4. Моделювання нової системи фінансово-економічної безпеки підприємства:

– розробка плану усунення виявлених під час аудиту зауважень;

– розробка пропозицій щодо удосконалення системи фінансово-економічної безпеки,

– розробка плану використання додаткових ресурсів;

– планування щомісячних витрат (бюджет) на забезпечення функціонування системи фінансово-економічної безпеки.

Етап 5. Затвердження керівником підприємства моделі нової системи фінансово-економічної безпеки і бюджету на її функціонування.

Етап 6. Безпосереднє формування системи фінансово-економічної безпеки.

Етап 7. Експертна оцінка дієвості сформованої системи фінансово-економічної безпеки та її удосконалення (при потребі).

Разом з тим, якщо на підприємстві розроблена система фінансово-економічної безпеки, не варто на цьому зупинятися.

Система фінансово-економічної безпеки – це живий організм, який потребує постійного контролю та удосконалення управління ним у зв'язку з: змінами діючого законодавства в країні; розвитком підприємства та розширенням сфер його діяльності; збільшенням кількості персоналу та змінами в штатному розписі підприємства; змінами переліку відомостей, що становлять комерційну таємницю і конфіденційну інформацію підприємства; необхідністю удосконалення телефонної та комп'ютерної мережей підприємства; розробкою нових технологій промислового шпигунства; появою на ринку недобросовісних конкурентів та зміною форм і методів їх протиправної діяльності; станом криміногенної ситуації в регіоні тощо.

2.3. Основні елементи системи фінансово-економічної безпеки

Основними елементами системи фінансово-економічної безпеки підприємства є: об'єкти, суб'єкти, принципи, функції, цілі та завдання, стратегія, механізм забезпечення фінансово-економічної безпеки, режими функціонування.

Об'єктом системи фінансово-економічної безпеки є все те, на що спрямовані зусилля щодо забезпечення безпеки. До них слід віднести:

– фінансово-економічний стан підприємства в поточний і перспективний періоди;

– інтереси підприємства;

– види діяльності підприємства (виробничу, комерційну, управління, постачання, планування тощо);

– майно та ресурси підприємства (фінансові, матеріальні, інформаційні, кадрові);

– персонал підприємства, його керівники, акціонери, власники, різноманітні структурні підрозділи, служби, партнери та ін.

Суб'єкти системи фінансово-економічної безпеки – ті особи, підрозділи, служби, органи, установи, які безпосередньо займаються забезпеченням безпеки.

Виділяють дві групи суб'єктів, які забезпечують фінансово-економічну безпеку підприємства: зовнішні та внутрішні.

Перша група (внутрішні) – це суб'єкти, які займаються забезпеченням фінансово-економічної безпосередньо на підприємстві і підпорядковані його керівництву. Серед них виділяють такі підгрупи:

1) спеціальні суб'єкти, основним призначенням яких є постійна діяльність із забезпечення фінансово-економічної підприємства (служба безпеки чи охорони, рятувальна служба, підрозділ чи відділ тощо);

2) напіспеціальні суб'єкти, частина функцій у яких полягає в забезпеченні фінансово-економічної безпеки підприємства (юридичний відділ, планово-економічний відділ, відділ кадрів тощо);

3) персонал та окремі підрозділи підприємства, які в межах своїх посадових інструкцій та положень про підрозділи зобов'язані вживати заходів

щодо забезпечення фінансово-економічної безпеки підприємства.

Друга група (зовнішні) – зовнішні органи та організації, які функціонують самостійно і не підпорядковуються керівництву підприємства, але при цьому їх діяльність істотно впливає на фінансово-економічну безпеку підприємства. До цієї групи належать:

– законодавчі органи, які приймають закони, що створюють правову основу діяльності щодо забезпечення безпеки на рівні держави, регіону, підприємства;

– органи виконавчої влади, які проводять політику безпеки, деталізують механізм безпеки;

– суди – забезпечують дотримання законних прав підприємства та його працівників;

– правоохоронні органи – ведуть боротьбу з правопорушеннями та злочинами;

– науково-освітні заклади – реалізують завдання щодо наукового опрацювання проблем безпеки та підготовки кадрів.

Засоби забезпечення фінансово-економічної безпеки виробничого підприємства:

1. Технічні – охоронно-пожежні ситеми, відео-, радіоапаратура, засоби виявлення вибухових приладів тощо.

2. Організаційні – спеціалізовані організаційні структурні формування, що забезпечують фінансово-економічну безпеку.

3. Інформаційні – насамперед друкована і відеопродукція з питань збереження конфіденційної інформації. Крім того, важлива інформація для прийняття рішень з питань фінансово-економічної безпеки зберігається на комп'ютерах.

4. Фінансові – без достатніх грощових коштів неможливе функціонування системи фінансово-економічної безпеки підприємства, треба тільки використовувати їх цілеспрямовано і з високою віддачею.

5. Нормативно-правові – підприємство повинно у своїй діяльності не тільки керуватися законами та підзаконними актами, що видані вищими органами влади, а й розробляти власні (локальні) нормативно-правові акти з питань забезпечення фінансово-економічної безпеки.

6. Кадрові – підприємство повинно бути забезпечене кадрами, що займаються питаннями фінансово-економічної безпеки.

7. Інтелектуальні – кваліфіковані спеціалісти, наукові працівники, що дає змогу модернізувати систему фінансово-економічної безпеки підприємства.

Методи забезпечення фінансово-економічної безпеки:

– *технічні* – спостереження, контроль, ідентифікація;

– *інформаційні* – складання характеристик на працівників, аналітичні матеріали конфіденційного характеру тощо;

– *фінансові* – матеріальне стимулювання працівників, що мають досягнення у забезпеченні економічної безпеки підприємства;

– *нормативно-правові* – правовий захист законних інтересів, сприяння діям правоохоронних органів;

– *кадрові* – підбір, навчання кадрів, що забезпечують економічну безпеку підприємства;

– *інтелектуальні* – патентування, ноу-хау тощо.

Функції системи фінансово-економічної безпеки:

– прогнозування, виявлення, попередження, нівелювання, обмеження впливу небезпек і загроз;

– забезпечення захищеності умов функціонування підприємства та його персоналу;

– формування ефективного конкурентного середовища;

– формування безпечних інформаційних систем;

– збереження майна та комерційної таємниці;

– ліквідація наслідків деструктивного впливу загроз і небезпек.

Механізм забезпечення фінансово-економічної безпеки – це сукупність законодавчих актів, правових норм, рушійних мотивів та стимулів, методів, засобів та заходів для ефективного функціонування системи фінансово-економічної безпеки підприємства.

Система фінансово-економічної безпеки, залежно від ситуації та її розвитку, може функціонувати в трьох режимах: повсякденному, підвищеної готовності і надзвичайного стану.

Повсякденний режим – це звичайний робочий режим, коли всі суб'єкти системи фінансово-економічної безпеки, крім кризової групи, виконують свої функції, реалізують заходи запобігання виникненню негативних чинників, їх виявлення та розроблення відповідних типових планів дій на випадок реалізації тих чи інших загроз.

Режим підвищеної готовності – це функціонування системи фінансово-економічної безпеки у разі виявлення конкретних загроз та їх деструктивного впливу.

Режим надзвичайного (кризового) стану – це функціонування системи фінансово-економічної безпеки за наявності небезпек. У цьому разі:

– оперативне управління організацією переходить до кризової групи;

– рада з безпеки розпочинає працювати в постійному режимі;

– забезпечується повна готовність системи безпеки, особливо служби безпеки, функціональних і лінійних керівників та персоналу підприємства до безпосереднього припинення дії небезпек;

– залучаються зовнішні сили безпеки (державна служба охорони, органи внутрішніх справ) та сили підтримки (структури міністерства надзвичайних ситуацій тощо).

Під **стратегією безпеки** розуміють сукупність найбільш важливих рішень, направлених на забезпечення програмного рівня безпеки функціонування підприємства.

Стратегії безпеки за своїм змістом бувають таких видів:

1. Стратегія безпеки, орієнтована на збереження безпеки та попередження виникнення можливих негативних чинників економічним інтересам суб'єкта.

Перший вид стратегії передбачає реалізацію випереджальних дій із метою недопущення появи загроз або нейтралізації виявлених явищ, які можуть

призвести до появи небезпеки. Стратегічні рішення, прийняті в рамках визначеної стратегії, спрямовані на використання можливостей, які з'являються та які були виявлені при вивченні загроз та стану фінансово-економічної безпеки підприємства та проведенні випереджальних заходів. Така стратегія є ефективною, тому що виключає можливість появи кризової ситуації, і водночас найбільш дорогою, тому що потребує значних витрат ресурсів, що може негативно позначитися на діяльності підприємства.

2. Стратегія безпеки, що обмежує небажані дії на об'єкти безпеки.

Другий вид стратегій передбачає таку діяльність із забезпечення безпеки, у результаті якої створюється заслін негативному впливу загроз. Наприклад, обмежується доступ до інформації, розголошування якої може завдати певні збитки. Така стратегія припускає, що реагування на загрози починається в момент, коли загрози фінансово-економічної безпеки починають впливати на фінансово-економічну безпеку.

3. Стратегія безпеки, що передбачає відновлення безпеки та компенсацію збитку або упущеної вигоди, що завдається.

У третьому випадку збиток припускається (виникає), проте він компенсується діями (наприклад, через інноваційну й інвестиційну політику з оцінками ризику), що передбачені відповідною стратегією за рахунок заздалегідь створених резервів. Цілком очевидно, що стратегії третього типу можуть розроблятися і реалізовуватися стосовно до ситуацій, де збитки можуть бути відновлені, або тоді, коли немає можливості здійснити програму реалізації стратегій першого або другого типу.

Формування системи фінансово-економічної безпеки та створення її суб'єктів залежить від розмірів підприємства, його економічних, фінансових, виробничо-технічних, інформаційних, інтелектуальних та інших можливостей.

Як свідчить досвід, малі підприємства найчастіше користуються послугами зовнішніх спеціалізованих приватних організацій: консалтингових, охоронних, інформаційних. До них належать підприємства, які займаються підбором та атестацією кадрів, центри маркетингових досліджень, приватні охоронні організації тощо.

Середні підприємства можуть використовувати комбіновану систему безпеки: з одного боку, у випадку необхідності отримувати послуги від зовнішніх організацій, з іншого – активно спиратися на можливості власних служб та підрозділів (юридичний чи фінансовий відділ, відділ маркетингу, техніки безпеки, пропускного режиму, діловодства тощо). З метою підвищення ефективності діяльності служб та підрозділів, як займаються захистом економічних інтересів, на підприємстві повинен бути створений координуючий орган або призначений один з керівників відповідальним за фінансово-економічну безпеку.

Для великого підприємства доцільним буде створення власної служби безпеки (підрозділу фінансово-економічної безпеки). Як правило, всю діяльність щодо забезпечення безпеки координує один з керівників підприємства. Для вироблення пропозицій та виконання консультативних функцій може створюватись рада з безпеки. Служба безпеки може включати

відділи, групи, підрозділи (охорони, режиму, роботи з кадрами, спеціального документообігу з грифом КТ, розвідки та контррозвідки, інформаційно-аналітичної діяльності, оперативного реагування тощо).

ТЕМА 3
ОРГАНІЗАЦІЯ ПРОЦЕСУ УПРАВЛІННЯ СИСТЕМОЮ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ВИРОБНИЧОГО ПІДПРИЄМСТВА

3.1. Основи організації управління системою фінансово-економічної безпеки підприємства

3.2. Принципи організації управління системою фінансово-економічної безпеки підприємства

3.1. Основи організації управління системою фінансово-економічної безпеки підприємства

Організація управління системою фінансово-економічної безпеки підприємства – формування його організаційної структури (визначення складу суб'єктів управління та їхніх взаємозв'язків) та розподіл завдань, повноважень, відповідальності між окремими ланками управління.

Організаційну структуру управління системою фінансово-економічної безпеки підприємства визначають як склад, взаємозв'язки та субпідрядність організаційних одиниць (підрозділів) апарату управління, які виконують різні функції управління фінансово-економічною безпекою підприємства.

Організаційна структура управління системою фінансово-економічної безпеки підприємства становить єдність і взаємозв'язок його рівнів та ланок.

Ланка управління системою фінансово-економічної безпеки підприємства – це відокремлений органом (працівник), наділеним функціями управління, можливістю їхньої реалізації, а також відповідальністю.

Рівень управління системою фінансово-економічної безпеки підприємства відображає сукупність його ланок на певному щаблі ієрархії управління.

Організаційне забезпечення управління системою фінансово-економічної безпеки – це взаємопов'язана сукупність внутрішніх функціональних служб та підрозділів підприємства, які здійснюють розробку, прийняття і реалізацію управлінських рішень, що забезпечують захист його інтересів.

Головними чинниками, які визначають організаційну структуру управління системою фінансово-економічної безпеки на підприємстві, є:

– вид економічної діяльності підприємства;

– організаційно-правова форма підприємства;

– характеристики ринку, на якому діє підприємство (рівень та методи конкуренції, особливості попиту тощо) та його ринкова позиція (частка ринку, рівень конкурентоспроможності тощо);

– обсяг фінансово-економічної діяльності підприємства;

– головні види фінансово-економічної діяльності підприємства;

– досягнутий рівень фінансово-економічної безпеки;

– наявність та кількість регіональних відділень;

– кількість та професійно-кваліфікаційний рівень працівників;

– можливість фінансового забезпечення функціонування системи управління фінансово-економічною безпекою підприємства;

– стиль керівництва (менеджменту);

– погляди власників (керівників) на необхідність та принципи побудови системи управління фінансово-економічною безпекою тощо.

Практичне виконання організації управління системою фінансово-економічної безпеки підприємства серед багатьох інших завдань передбачає: регламентацію управлінських функцій, операцій і процедур; визначення складу підрозділу фінансово-економічної безпеки та кількості працівників для реалізації кожної управлінської функції; встановлення посадових прав і обов'язків, відображених у відповідних посадових інструкціях та положенні про службу (відділ, підрозділ) фінансово-економічної безпеки підприємства.

3.2. Принципи організації управління системою фінансово-економічної безпеки підприємства

Принципи організації управління системою фінансово-економічної безпеки:

– адаптивність (здатність пристосовуватися до змін у зовнішньому середовищі);

– гнучкість, динамізм (здатність швидко реагувати на зміни чинників зовнішнього середовища);

– адекватність (постійна відповідність організаційної структури параметрам керованої системи);

– спеціалізація (функціональна замкнутість структурних підрозділів, обмеження та конкретизація сфери діяльності кожної керуючої ланки);

– оптимальність (налагодження раціональних зв'язків між рівнями та ланками управління);

– оперативність (недопущення незворотніх змін у керованій системі за час прийняття рішення);

– надійність (гарантованість достовірності передавання інформації);

– економічність (відповідність витрат на утримання органів управління можливостям організації);

– простота (легкість розуміння та пристосування до даної форми управління та участі у реалізації мети організації).

Можна виділити два принципові підходи до організації управління системою фінансово-економічної безпеки підприємства:

– без створення спеціалізованого підрозділу (відділу, служби);

– зі створенням спеціалізованого підрозділу (відділу, служби).

На малих підприємствах реалізацію функції управління системою фінансово-економічної безпеки доцільно здійснювати шляхом створення тимчасових робочих груп із залученням персоналу з усіх його функціональних відділів (по одному виконавцю з кожного відділу) на чолі з адміністратором фінансово-економічної безпеки, якого обирає керівник підприємства Як свідчить досвід, створення таких робочих груп звільняє керівництво від значного обсягу додаткової роботи і стимулює діяльність усіх функціональних відділів.

Для середніх підприємств найбільш ефективна з погляду управління системою фінансово-економічної безпеки організаційна структура, яка

передбачає два напрями управління: вертикальний – відображає управління структурними підрозділами підприємства, які забезпечують фінансово-економічну безпеку, горизонтальний – управління стратегічно орієнтованими напрямами досягнення фінансово-економічної безпеки підприємства, для реалізації яких залучають працівників і ресурси різних підрозділів підприємства.

Впровадження такої організаційної структури, яка характеризується структурною гнучкістю для пристосування в нових умовах функціонування, дозволить зменшити завантаженість вищого керівництва, оскільки існує чіткий розподіл прав та обов'язків між менеджерами, які здійснюють управління окремими підрозділами, та менеджерами, що керують функціональними стратегічно-орієнтованими напрямами забезпечення фінансово-економічної безпеки підприємства. Перевагами цієї організаційної структури є й можливість залучення до вирішення стратегічних питань менеджерів середнього та нижнього рівнів управління і використання комплексного підходу до прийняття стратегічних рішень.

Використовуючи таку організаційну структуру управління, керівник окремого стратегічного напряму забезпечення фінансово-економічної безпеки працює з лінійними керівниками, визначаючи що і коли необхідно зробити по конкретному напряму досягнення фінансово-економічної безпеки, а вже лінійні керівники вирішують, хто і як буде виконувати ту чи іншу роботу.

На великих підприємствах процес формування організаційної структури підприємства, яка забезпечить ефективну роботу механізму забезпечення фінансово-економічної безпеки підприємства, необхідно розпочинати із створення нової структурної одиниці – служби (підрозділу) фінансово-економічної безпеки. Цілі, завдання і функції служби (підрозділу) визначатимуться Положенням про службу (підрозділ) фінансово-економічної безпеки, яке узгоджується з керівниками інших підрозділів підприємства і затверджується безпосередньо керівником підприємства.

ТЕМА 4
ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ СЛУЖБИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

4.1. Мета та порядок створення служби фінансово-економічної безпеки підприємства

4.2. Основні завдання та функції служби фінансово-економічної безпеки підприємства

4.3. Управління діяльністю служби фінансово-економічної безпеки підприємства

4.1. Мета та порядок створення служби фінансово-економічної безпеки підприємства

Для забезпечення фінансово-економічної безпеки підприємства застосовують два підходи:

– без створення спеціалізованого підрозділу (відділу, служби);

– зі створенням спеціалізованого підрозділу (відділу, служби).

Зростання кількості загроз, ризиків і небезпек у господарській діяльності зумовлюють необхідність створення служби фінансово-економічної безпеки підприємства.

Служба фінансово-економічної безпеки підприємства – це штатний структурний підрозділ підприємства, який підпорядковується безпосередньо його керівникові (власнику) і організовує у взаємодії з іншими структурними підрозділами (а також за необхідності, органами державної влади та управління, іншими зовнішніми суб'єктами) розроблення, реалізацію та контроль виконання заходів щодо захисту життєво важливих інтересів підприємства від зовнішніх і внутрішніх загроз.

Створення служби фінансово-економічної безпеки зіштовхується з певними труднощами, оскільки кожний суб'єкт підприємництва індивідуальний, адже індивідуальна його діяльність. Проте можна виділити декілька етапів, які рекомендуються підприємцям при створенні такої служби.

Етап 1. *Прийняття рішення про створення служби фінансово-економічної безпеки підприємства.* Питання про створення служби фінансово-економічної безпеки повинно виникати в момент ухвалення рішення про організацію підприємства в залежності від вибраного виду діяльності, обсягу передбачуваного виробництва продукції, кількості працівників тощо. Після державної реєстрації керівниками приймається остаточне рішення про створення СФЕБ. При цьому визначається відповідальна особа (група осіб), яка безпосередньо буде займатися організацією СФЕБ.

Етап 2. *Визначення загальних завдань служби фінансово-економічної безпеки* (попередження загроз, реагування на загрози, що виникли, і визначення конкретних об'єктів захисту (персонал, інформація тощо).

Етап 3. *Проектування організаційної структури служби фінансово-економічної безпеки.*

Етап 4. *Розробка внутрішніх нормативних документів*, які регулюють

діяльність усіх підрозділів і працівників СФЕБ. Такими нормативними документами є: положення про службу фінансово-економічної безпеки підприємства, положення про підрозділи, посадові інструкції працівників служби економічної безпеки тощо.

Етап 5. *Формування ресурсного забезпечення служби фінансово-економічної безпеки підприємства.*

Цей етап передбачає фінансове, матеріально-технічне та інформаційне забезпечення діяльності СФЕБ.

Етап 6. *Кадрове забезпечення діяльності служби фінансово-економічної безпеки підприємства.*

Етап 7. *Розміщення кадрів, розподіл прав, повноважень і міри відповідальності.* Це дозволяє забезпечити ефективну роботу окремих підрозділів служби фінансово-економічної безпеки. Важливим фактором підвищення ефективності діяльності вказаної служби є гнучка система стимулювання працівників в залежності від результатів роботи.

Етап 8. *Організація контролю та аналізу результатів діяльності служби фінансово-економічної безпеки.* Він передбачає підтримку високого рівня професіоналізму працівників служби, дисципліни всього персоналу і забезпечення ефективної роботи СФЕБ. Для цього використовуються:

– регулярні поточні звіти СФЕБ перед керівництвом підприємства;

– звіти про захист від конкретних загроз і вжитих заходів;

– аналіз звітів і висновок керівництва підприємства про ефективність роботи СФЕБ.

4.2. Основні завдання та функції служби фінансово-економічної безпеки підприємства

Головною метою діяльності служби фінансово-економічної безпеки підприємства є захист його життєво важливих інтересів та запобігання фінансовій, матеріальній та нематеріальній шкоді, яку може завдати реалізація зовнішніх і внутрішніх загроз.

Загальні функції служби фінансово-економічної безпеки підприємства:

– організація захисту його життєво важливих інтересів;

– моніторинг зовнішнього та внутрішнього середовища;

– прогнозування загроз зовнішнього та внутрішнього середовища;

– розроблення планів заходів з забезпечення фінансово-економічної безпеки підприємства;

– оцінка ризику альтернативних управлінських рішень;

– інформаційне забезпечення управління системою фінансово-економічної безпеки підприємства: організація спеціального діловодства; пошук необхідної інформації;

– оцінка рівня фінансово-економічної безпеки та захищеності життєво важливих інтересів підприємства;

– контроль за виконанням планових заходів із забезпечення фінансово-економічної безпеки підприємства;

– оцінка ефективності управлінських рішень у сфері фінансово-економічної безпеки.

Основні завдання служби фінансово-економічної безпеки підприємства:

– забезпечення збереження, ефективного використання та нарощування фінансових, матеріальних, інформаційних ресурсів, об'єктів інтелектуальної власності та персоналу;

– своєчасне виявлення, нейтралізація чи мінімізація реалізації загроз життєво важливим інтересам підприємства; причин і умов, що можуть завдати фінансового, матеріального і морального збитку підприємству, порушення його нормального функціонування і розвитку;

– аналіз і оцінка рівня фінансово-економічної стійкості, ступеня захищеності від внутрішніх і зовнішніх загроз;

– створення умов для максимально можливого відшкодування і локалізації збитків, нанесених реалізацією загроз;

– прогнозування стану чинників зовнішнього і внутрішнього середовища підприємства, що можуть порушити нормальний розвиток і функціонування підприємства;

– отримання необхідної інформації для вироблення оптимальних управлінських рішень у питаннях стратегії і тактики діяльності підприємства;

– забезпечення захисту відомостей, що вважаються комерційною таємницею підприємства: запобігання несанкціонованого доступу до них; виявлення і локалізація можливих каналів витоку конфіденційної інформації;

– забезпечення безпеки за здійснення всіх видів діяльності, включаючи зустрічі, переговори й наради у рамках ділового співробітництва підприємства з іншими партнерами;

– охорона приміщень, устаткування, іншого майна та матеріальних цінностей, необхідних для господарської діяльності;

– забезпечення особистої безпеки керівництва та провідних менеджерів і спеціалістів підприємства;

– аналіз і оцінка ефективності заходів, спрямованих на захист життєво важливих інтересів підприємства.

4.3. Управління діяльністю служби фінансово-економічної безпеки підприємства

Очолює службу фінансово-економічної безпеки начальник служби.

Начальник служби фінансово-економічної безпеки – безпосередній керівник персоналу служби фінансово-економічної безпеки. Він підпорядковується директорові підприємства або одному із його заступників. Начальник служби фінансово-економічної безпеки здійснює керівництво діяльністю СФЕБ, вирішує всі організаційні питання, пов'язані з діяльністю служби, крім тих, що стосуються виключно компетенції дирекції підприємства. Призначення на посаду начальника СФЕБ підприємства, а також його звільнення виконуються тільки керівником підприємства.

Начальник СФЕБ без додаткового доручення діє від імені служби у всій

своїй діяльності, визначає посадові оклади її працівників, вирішує питання щодо надання чи позбавлення премій, інших видів заохочення та мотивування тощо.

Начальник служби фінансово+економічної безпеки повинен мати такі особисті якості:

– *концептуальність*, тобто представляти діяльність служби фінансово-економічної безпеки в цілому і адаптувати її до мінливих умов зовнішнього середовища;

– *оперативність*, тобто мати кваліфікацію на рівні прийнятого рішення;

– *аналітичність*, тобто вміти ефективно застосовувати наукові методи аналізу;

– *здатність до адміністративних рішень*, тобто володіти навичками організаційних рішень і процедурних питань;

– *комунікативність*, тобто вміти передавати свої ідеї та розробки як в усній, так і в письмовій формі;

– *володіння певним рівнем спеціальних знань* з питань організації системи забезпечення фінансово-економічної безпеки підприємства;

– *комунікабельність*, тобто вміти будувати свої відносини в спілкуванні з керівниками, колегами, підлеглими.

Принципи управління службою фінансово-економічної безпеки:

1. Науковість. Основний зміст цього принципу полягає у вимозі, щоб всі управлінські дії здійснювалися на базі застосування наукових методів і підходів. Цей принцип вимагає від керівників служби фінансово-економічної безпеки і його підрозділів уважного вивчення управлінської та спеціальної літератури з проблем забезпечення безпеки підприємства.

2. Єдиноначальність і колегіальність. Сутність цього принципу полягає в тому, що на основі думок низових керівників і виконавців конкретних рішень, керівник вищого рівня користується правом одноосібного вирішення питань, що входять у його компетенцію.

3. Принцип системності та комплексності. Системність означає необхідність використання елементів теорії великих систем, системного аналізу в кожному управлінському рішенні. Комплексність в управлінні означає необхідність всебічного охоплення керованої системи, обліку всіх сторін, усіх напрямків, всіх властивостей. Цей принцип вимагає від керівника служби економічної безпеки вироблення у себе аналітико-синтетичного складу мислення.

4. Принцип оптимального поєднання централізації і децентралізації. Цей принцип полягає в оптимальному розподілі (делегуванні) повноважень при прийнятті управлінських рішень.

5. Принцип плановості. Сутність цього принципу полягає у встановленні основних напрямів і пропорцій служби фінансово-економічної безпеки в перспективі. Практична реалізація цього принципу означає, що всі працівники, підрозділи і служби безпеки в цілому повинні планувати свою діяльність у такій послідовності: служба фінансово-економічної безпеки – підрозділи – працівники.

6. Принцип поєднання прав, обов'язків і відповідальності. Цей принцип передбачає, що кожен працівник служби фінансово-економічної безпеки повинен виконувати покладені на нього обов'язки, при цьому він наділяється адекватними йому правами і несе відповідальність за якість їх виконання.

Методи управління службою фінансово-економічної безпеки: *економічні, організаційно-розпорядчі та соціально-психологічні.*

Керівники служби економічної безпеки повинні бездоганно володіти всіма методами управління в їх єдності. Для цього вони повинні знати особливості кожного з них.

На рівні працівника служби фінансово-економічної безпеки переважним впливом користується такий економічний стимул, як заробітна плата. Вміле використання цього стимулу з урахуванням рівня професіоналізму, стажу роботи, результатів діяльності працівника і т.д. дозволяє в значній мірі підвищити його трудову активність.

Організаційно-розпорядчі методи управління (накази, розпорядження, вказівки, інструкції тощо) поділяються на три групи: розпорядчі, організаційно-стабілізуючі та дисциплінуючі.

Соціально-психологічні методи засновані на використанні моральних стимулів до праці і впливають на особистість працівника служби фінансово-економічної безпеки за допомогою психологічних прийомів з метою перетворення завдання у внутрішню потребу людини. Це досягається за допомогою прийомів, які носять особистісний характер (особистий приклад, авторитет тощо).

ТЕМА 5
ФОРМУВАННЯ СТРАТЕГІЇ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

5.1. Сутність стратегії фінансово-економічної безпеки підприємства та її види

5.2. Послідовність формування стратегії фінансово-економічної безпеки підприємства

5.3. Набір стратегій фінансового-економічної безпеки підприємства

5.1. Сутність стратегії фінансово-економічної безпеки підприємства та її види

Стратегія фінансово-економічної безпеки підприємства – це обґрунтована система послідовних дій і заходів, орієнтованих на досягнення поставленої мети, спосіб досягнення встановлених цілей забезпечення фінансово-економічної безпеки з урахуванням тенденції зміни її рівня.

Мета формування та реалізації стратегії фінансово-економічної безпеки – досягнення такого рівня фінансово-економічної безпеки, який здатний забезпечити стійкий, стабільний та динамічний розвиток підприємства у перспективі.

Місце стратегії фінансово-економічної у системі стратегічного управління підприємством.

У вітчизняній та зарубіжній літературі існують різні підходи до класифікації стратегій підприємства. Залежно від організаційного рівня розроблення виділяють такі види стратегій підприємства:

– корпоративна стратегія – визначає загальний напрям функціонування багатопрофільної компанії і поширюється на всі сфери її діяльності;

– ділова стратегія (бізнес-стратегія) – фокусується на одному напрямку діяльності компанії, визначаючи способи досягнення конкурентних переваг у вибраному напрямку та завоювання довгострокових конкурентних позицій на ринку;

– функціональна стратегія – стратегія для окремого функціонального напрямку конкретної сфери діяльності (виробнича, маркетингова, фінансова, інноваційна та ін.). Функціональні стратегії підпорядковуються корпоративній та діловій стратегіям підприємства і їх конкретизують.

Стратегію фінансово-економічної безпеки підприємства необхідно формувати в межах корпоративної стратегії та на основі функціональних стратегій фінансово-економічної безпеки.

Заходи забезпечення фінансово-економічної безпеки підприємства повинні спрямовуватись, насамперед, на підтримку здатності підприємства реалізувати корпоративну стратегію.

Функціональні стратегії фінансово-економічної безпеки забезпечують стратегічно-орієнтовані напрями досягнення цілей фінансово-економічної безпеки підприємства:

– стратегія фінансової безпеки;

– стратегія інтелектуально-кадрової безпеки;
– стратегія техніко-технологічної безпеки;
– стратегія політико-правової безпеки;
– стратегія інформаційної безпеки;
– стратегія екологічної безпеки;
– стратегія силової безпеки;
– стратегія ринкової безпеки;
– стратегія інтерфейсної безпеки.

Формування стратегії фінансово-економічної безпеки підприємства – це складний процес, який охоплює чітку послідовність взаємозалежних та взаємопов'язаних етапів, що заснована на вимогах конкретної ситуації і враховує вплив багатьох зовнішніх та внутрішніх чинників.

Фактори, що впливають на формування стратегії фінансово-економічної безпеки підприємства:

– стан та перспективи розвитку конкретного виду економічної діяльності;
– рівень фінансово-економічної безпеки підприємства;
– наявні можливості підприємства стосовно забезпечення та підтримання необхідного рівня фінансово-економічної безпеки (виробничі, фінансові, ринкові, інтелектуально-кадрові, інноваційні тощо), які відповідають його потребам;
– висока кваліфікованість керівництва щодо формування стратегії та досягнення встановлених стратегічних цілей підприємства;
– активна участь персоналу у формуванні та реалізації стратегії.

Процес розроблення стратегії фінансово-економічної безпеки підприємства можна охарактеризувати як процес узгодження цілей підприємства стосовно забезпечення фінансово-економічної безпеки з можливостями підприємства.

Види стратегій фінансово-економічної безпеки:

1. Стратегія збереження фінансово-економічної безпеки та нівелювання негативних чинників. Ця стратегія покликана забезпечувати утримання високого рівня фінансово-економічної безпеки та створення нових передумов її зміцнення. Вона виключає можливість появи небезпечної ситуації. Цей вид стратегії доцільно застосовувати в тому випадку, коли рівень фінансово-економічної безпеки перебуває на високому рівні.

Стратегія збереження фінансово-економічної безпеки та нівелювання негативних чинників – найбільш ефективна, яка потребує достатнього часу для прийняття стратегічних управлінських рішень та високих можливостей підприємства для забезпечення фінансово-економічної безпеки. Ця стратегія дає можливість підприємству нівелювати негативні чинники ще до початку їхнього дестабілізуючого впливу.

2. Стратегія зміцнення фінансово-економічної безпеки та інтенсифікації зусиль на обмеження впливу негативних чинників. Ця стратегія, з одного боку, передбачає заходи підтримання позитивних тенденцій до посилення фінансово-економічної безпеки підприємства, а з іншого боку, вона повинна забезпечити недопущення послаблення фінансово-економічної безпеки. Цей вид стратегії доцільно застосовувати при середньому рівні фінансово-економічної безпеки.

Стратегія зміцнення фінансово-економічної безпеки та інтенсифікації зусиль на обмеження впливу негативних чинників передбачає наявність скороченого часового терміну для розробки необхідних заходів та середніх можливостей підприємства до забезпечення фінансово-економічної безпеки, які відповідають наявним потребам. Цей вид стратегії передбачає швидке реагування на вплив негативних чинників, що містить чітко продумані дії, які дозволять пристосуватися в максимально короткі строки.

3. Стратегія відновлення фінансово-економічної безпеки та ліквідації наслідків впливу негативних чинників. Ця стратегія повинна передбачати використання заходів подолання небезпек для діяльності підприємства, які стримуватимуть поширення негативних процесів та забезпечать виживання підприємства. Ця стратегія впроваджується при низькому рівні фінансово-економічної безпеки.

Стратегія відновлення фінансово-економічної безпеки та ліквідації наслідків впливу негативних чинників передбачає моментальне реагування на негативний вплив небезпек в умовах обмеження часу та низьких можливостей, що не завжди дозволяють повною мірою здійснювати заходи із забезпечення фінансово-економічної безпеки. В рамках цієї стратегії проявляється певна суперечливість. З одного боку, прийняті поспіхом рішення не завжди ефективні, а з іншого, зволікання у швидкому розробленні конкретних заходів може призвести до занепаду підприємства або його банкрутства.

5.2. Послідовність формування стратегії фінансово-економічної безпеки підприємства

Етапи процесу формування стратегії фінансово-економічної безпеки підприємства:

Етап 1. Визначення місії підприємства.

Місія підприємства (філософія, бачення підприємства) – короткий опис господарської одиниці, її основних цілей, призначення, сфери діяльності, норм поведінки та ролі у вирішенні соціальних проблем суспільства.

Ціль визначення місії – довести до відома всіх учасників розроблення стратегічних рішень основні правила, які підприємство встановлює для ведення всіх своїх справ.

Місія підприємства, як чітко виражена узагальнена довгострокова мета діяльності підприємства повинна відображати:

– основне призначення підприємства для тих ринків і покупців, які воно обслуговує;

– індивідуальність підприємства та майбутнє бачення того, яким воно хоче стати;

– основні принципи діяльності підприємства.

Основне запитання, на яке відповідає місія, – яку людську потребу задовільняє підприємство.

Етап 2. Формування цілей фінансово-економічної безпеки підприємства.

На основі місії розробляються цілі, які, на відміну від місії, визначають конкретні стани, яких підприємство хоче досягнути у майбутньому.

Сформовані цілі повинні бути чіткі, конкретні і кількісно вимірювані, реалістичні і досяжні, визначені в термінах їх досягнення, забезпечені ресурсами і підкріплені персональною відповідальністю менеджерів. Вони лежать в основі прийняття окремих бізнесових рішень та сприяють формуванню конкретних планових показників. Усі сформовані цілі повинні бути ієрархічно поєднані, тобто цілі більш низького рівня конкретизують та деталізують цілі більш високого рівня і є засобом для їх досягнення.

Етап 3. Аналіз зовнішнього середовища підприємства (макросередовища та мікросередовища).

Аналіз макросередовища підприємства передбачає вивчення впливу на його діяльність загального стану економіки та його державного регулювання, науково-технічного розвитку, природно-екологічної ситуації країни, соціально-культурної і демографічної складової суспільства. Найчастіше на цьому етапі обмежуються PEST-аналізом чотирьох компонентів макросередовища: політичного (political environment), економічного (economic environment), соціального (sociocultural environment) й технологічного (technological environment). PEST-аналіз спрямований на виявлення тих факторів макросередовища, які найбільше впливають на підприємство, та передбачення сприятливої чи несприятливої динаміки впливу цих факторів.

Аналіз цих факторів ведеться комплексно, з урахуванням взаємозв'язку, швидкості зміни та рівня впливу на підприємство. Результати аналізу дають змогу підприємству визначити, які з чинників макросередовища є потенційними носіями загроз або можливостей.

Аналіз мікросередовища здійснюють за допомогою моделі п'яти конкурентних сил М. Портера, яка передбачає визначення впливу на здатність підприємства реалізувати свою перевагу на ринку таких чинників, як-от: постачальників; покупців; наявних конкурентів; потенційних конкурентів, які можуть вийти на ринок; товарів-замінників. Взаємодія саме цих конкурентних сил визначає потенціал мікросередовища підприємства.

Зовнішнє середовище ніколи не буває стабільним, у ньому безперервно відбуваються динамічні зміни: з'являються нові можливості для підприємства та виникають додаткові непередбачувані труднощі. Тому важливим для підприємства є виявлення можливостей та загроз зовнішнього середовища, які будуть враховуватися при формуванні стратегії.

Етап 4. Аналіз внутрішнього середовища підприємства.

Аналіз внутрішнього середовища підприємства орієнтується на аналіз його корпоративного потенціалу за такими напрямами: виробництво, управлінська діяльність, економічна культура, маркетинг, фінанси, кадрове забезпечення, загальна ефективність підприємства. Під час стратегічного планування необхідно з'ясувати, які сильні та слабкі сторони має підприємство та як вони вплинуть на діяльність підприємства.

Аналіз зовнішнього та внутрішнього середовища – SWOT-аналіз – дозволяє встановити зв'язки між сильними та слабкими сторонами підприємства і можливостями та загрозами, які в подальшому будуть використовуватися для формування стратегії підприємства.

Етап 5. Оцінка рівня фінансово-економічної безпеки підприємства.

Без інформації про стан фінансово-економічної безпеки підприємства менеджери не зможуть розробити стратегію, яка дозволить підприємству ефективно розвиватися в майбутньому.

Оцінку рівня фінансово-економічної безпеки підприємства важливо здійснювати за всіма її складовими. Значення узагальненого показника фінансово-економічної безпеки, який і буде характеризувати досягнутий рівень фінансово-економічної безпеки підприємства.

Етап 6. Коригування цілей підприємства залежно від результатів аналізу та оцінки рівня фінансово-економічної безпеки.

Після аналізу зовнішнього середовища, внутрішнього середовища, оцінки рівня фінансово-економічної безпеки менеджери повинні уточнити місію та цілі підприємства, здійснити коригування на фактори, вплив яких не було враховано.

Етап 7. Формування набору альтернативних стратегій фінансово-економічної безпеки підприємства.

На основі проведеного аналізу та необхідних розрахунків формується набір альтернативних стратегій фінансово-економічної безпеки підприємства і приймається рішення щодо того, яким чином і за допомогою яких засобів підприємство досягне поставлених цілей.

Етап 8. Вибір стратегії фінансово-економічної безпеки підприємства.

Процес вибору оптимальної для підприємства стратегії фінансово-економічної безпеки повинен базуватися на дотриманні таких принципів:

– обґрунтованості – вибір стратегії фінансово-економічної безпеки повинен бути чітко обґрунтованим за допомогою оптимального поєднання різних методичних підходів;

– альтернативності – стратегія фінансово-економічної безпеки підприємства повинна обиратись серед декількох альтернативних видів стратегій;

– об’єктивності – стратегія фінансово-економічної безпеки повинна бути об’єктивно узгодженою для досягнення стратегічних цілей підприємства;

– доцільності – стратегія фінансово-економічної безпеки підприємства повинна забезпечувати можливий рівень фінансово-економічної безпеки;

– узгодженості – обрана стратегія фінансово-економічної безпеки повинна узгоджуватися з іншими стратегіями діяльності підприємства;

– оптимальності – обрана стратегія фінансово-економічної безпеки повинна бути оптимальною з точки зору поєднання результатів, витрат та ризику реалізації;

– цілісності – обрана стратегія фінансово-економічної безпеки повинна забезпечити розвиток підприємства як цілісної системи, а не тільки окремих його підрозділів, відділів чи напрямів діяльності.

Етап 9. Реалізація стратегії фінансово-економічної безпеки підприємства.

Обрана з альтернативного набору найбільш ефективна стратегія фінансово-економічної безпеки, яка максимально підвищить довгострокову ефективність

підприємства, потребує реалізації, що є наступним етапом процесу розробки стратегії.

Реалізація стратегії фінансово-економічної безпеки – сукупність управлінських дій, які пов'язані з послідовним виконанням усіх етапів стратегічного плану, розподілом обов'язків, відповідальності, створенням необхідного ресурсного, нормативно-правового, інформаційного та організаційного забезпечення, необхідною координацією зусиль усіх підрозділів підприємства. Саме на цьому етапі важливу роль відіграє залучення до цього процесу менеджерів усіх рівнів та персоналу підприємства.

Етап 10. Контроль за процесом реалізації стратегії фінансово-економічної безпеки підприємства

Реалізація стратегії потребує постійного контролю, що забезпечує зворотний зв'язок між досягненнями підприємства у процесі реалізації стратегії та поставленими цілями. Здійснюється причинно-наслідковий аналіз виявлених відхилень у процесі реалізації стратегії. При потребі коригуються цілі підприємства, власне процес реалізації стратегії чи сама стратегія.

5.3. Набір стратегій фінансового-економічної безпеки підприємства

В межах загальних стратегій фінансово-економічної безпеки, які є загальним планом управління, спрямованим на збереження, зміцнення чи відновлення фінансово-економічної безпеки та нівелювання чи обмеження впливу негативних чинників, необхідно формувати функціональні стратегії фінансово-економічної безпеки підприємства, які в сукупності створюють набір стратегій економічної безпеки.

Набір стратегій фінансово-економічної безпеки підприємства – це сукупність загальної та функціональних стратегій фінансово-економічної безпеки, які формуються для кожного підприємства з метою забезпечення його фінансово-економічної безпеки.

Модель набору стратегій фінансово-економічної безпеки має такий вигляд:

$$S_z : \{S_i^1; ...; S_i^n\}, n = \overline{1,9},$$

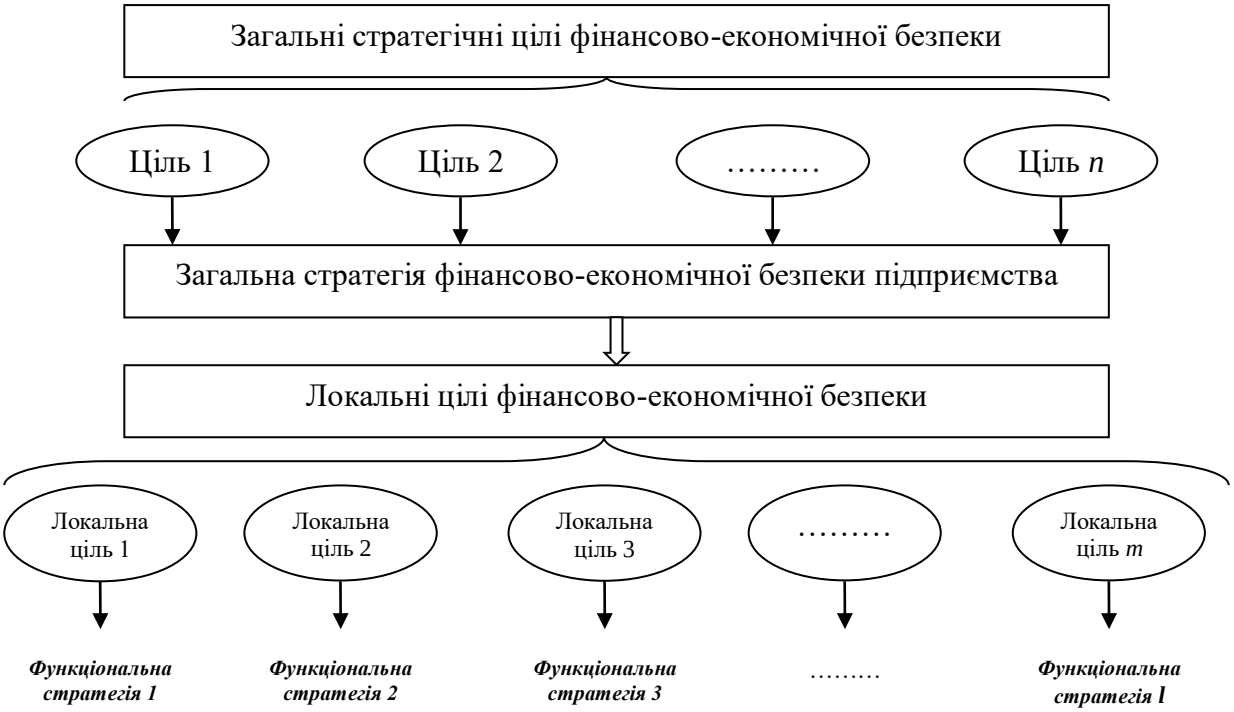
де S_z – загальна стратегія фінансово-економічної безпеки; $z = \overline{1,3}$; $S_i^1, ..., S_i^n$ – функціональні стратегії фінансово-економічної безпеки; $S_i^1 \in \{S_1^1; S_2^1; S_3^1\}$; $S_i^2 \in \{S_1^2; S_2^2; S_3^2\}; \ldots;\ S_i^n \in \{S_1^n; S_2^n; S_3^n\};\ i = \overline{1,3}$.

Функціональні стратегії фінансово-економічної безпеки охоплюють:

– перелік можливих заходів щодо збереження, підтримання та відновлення фінансово-економічної безпеки, запобігання негативних чинників впливу на складові фінансово-економічної безпеки;

– перелік чітких дій при виникненні непередбачуваної ситуації щодо забезпечення фінансово-економічної безпеки;

– перелік конкретних заходів з відновлення діяльності підприємства, налагодження всіх процесів його нормального функціонування після припинення впливу конкретного виду негативних чинників.



n – кількість загальних цілей фінансово-економічної безпеки;
m – кількість локальних цілей фінансово-економічної безпеки;
l – кількість функціональних стратегій фінансово-економічної безпеки

Рис. 5.1. Набір стратегій фінансово-економічної безпеки підприємства

Критеріями вибору функціональних стратегій фінансово-економічної безпеки є значення показників безпеки складових фінансово-економічної безпеки. Правильний вибір функціональних стратегій дозволить виявити потенційні резерви комплексу заходів стосовно забезпечення фінансово-економічної безпеки підприємства.

Імовірні функціональні стратегії фінансово-економічної підприємства:

– стратегія збереження фінансової безпеки;
– стратегія підтримання фінансової безпеки;
– стратегія відновлення фінансової безпеки.

ТЕМА 6
РЕАЛІЗАЦІЯ СТРАТЕГІЇ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

6.1. Основні причини невдалої реалізації стратегії фінансово-економічної безпеки підприємства

6.2. Механізм реалізації стратегії фінансово-економічної безпеки: сутність та мета

6.3. Моніторинг реалізації стратегії фінансово-економічної безпеки

6.4. Моніторинг впливу чинників зовнішнього та внутрішнього середовища на процес реалізації стратегії фінансово-економічної безпеки

6.5. Безперервне навчання персоналу в процесі реалізації стратегії фінансово-економічної безпеки

6.1. Основні причини невдалої реалізації стратегії фінансово-економічної безпеки підприємства

Основні причини невдалої реалізації стратегії фінансово-економічної безпеки:

– невідповідність між обраною стратегією та організацією управління підприємством;

– відсутність оцінки невизначеності та ризиків реалізації обраної стратегії, що призводить до небажання керівниками брати відповідальність за прийняття ризикових рішень;

– нестача ресурсів для ефективної реалізації стратегії;

– неузгодженість обраної стратегії з іншими стратегіями діяльності підприємства;

– відсутність систематичного та безперервного спостереження за процесом реалізації стратегії;

– відсутність спостереження за негативним впливом зовнішнього та внутрішнього середовищ діяльності підприємства;

– недостатній рівень кваліфікації управлінського персоналу та відсутність ефективної системи мотивації працівників для успішної реалізації обраної стратегії;

– неефективне управління стратегічними змінами;

– відсутність контролю за реалізацією стратегії та оцінки ефективності цієї реалізації.

6.2. Механізм реалізації стратегії фінансово-економічної безпеки: сутність та мета

Ефективну реалізацію стратегії фінансово-економічної безпеки забезпечить **механізм реалізації стратегії.** Він надасть можливість підприємству до швидкого та гнучкого реагування на зовнішні та внутрішні негативні зміни.

Мета механізму реалізації стратегії фінансово-економічної безпеки – забезпечення динамічного процесу прийняття своєчасних управлінських рішень

стосовно стратегічних змін відповідно до умов обраної стратегії та швидких змін зовнішнього і внутрішнього середовищ функціонування підприємства.

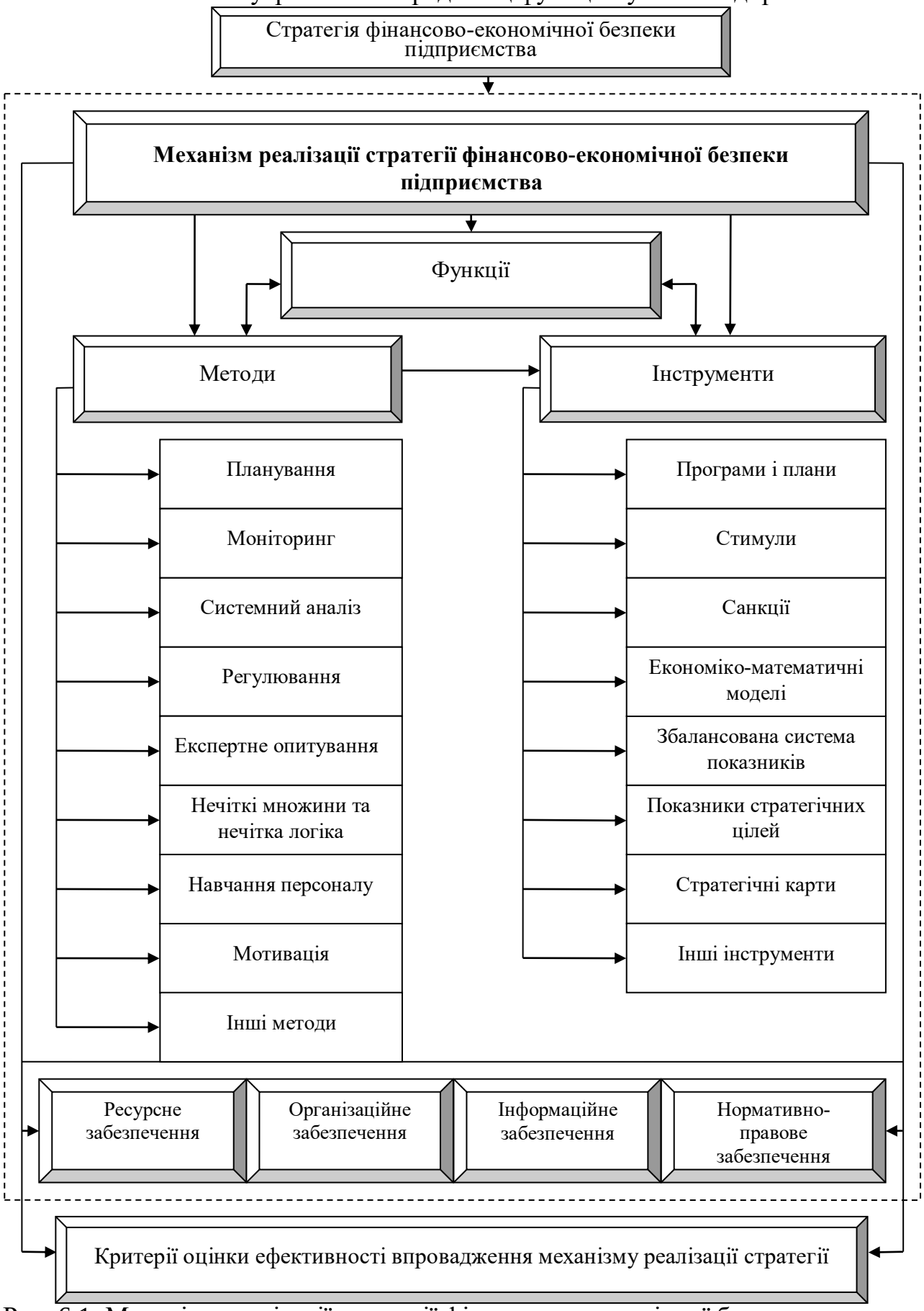


Рис. 6.1. Механізм реалізації стратегії фінансово-економічної безпеки

Побудова механізму реалізації стратегії базується на таких принципах:

– безперервного удосконалення процесу реалізації стратегії;

– адаптації механізму до релевантних зовнішніх та внутрішніх умов;

– систематичного та регулярного навчання персоналу та використання мотиваційних заходів для забезпечення виконання механізму;

– системності у прийнятті управлінських рішень щодо функціонування механізму;

– відповідності організаційної структури підприємства вимогам механізму реалізації стратегії;

– постійного спостереження за роботою механізму та визначення його ефективності.

Відповідно до мети та принципів побудови **механізм реалізації стратегії фінансово-економічної безпеки** – це сукупність методів та інструментів, властивих стратегічному управлінню підприємством, які використовуються для реалізації функцій механізму в умовах динамічних змін зовнішнього та внутрішнього середовищ функціонування підприємства.

Впровадження механізму реалізації стратегії фінансово-економічної безпеки здійснюється одночасно із розробленням ресурсного, організаційного, інформаційного та нормативно-правового забезпечення.

Організаційне забезпечення передбачає:

– формування моделі діяльності персоналу в процесі реалізації стратегії та організацію їхнього безперервного навчання;

– забезпечення адаптації працівників до стратегічних змін, що проявляється в усвідомленні необхідності здійснення цих змін та їхньої особистої і колективної значимості;

– формування організаційної структури відповідно до вимог розробленої стратегії, яка сприятиме чіткій координації роботи підприємства.

В рамках **ресурсного забезпечення** розробляються фінансові плани використання коштів на виконання механізму реалізації стратегії та відбувається розподіл ресурсів між підрозділами підприємства для ефективного виконання своєї частини стратегічного плану фінансово-економічної безпеки.

Сутність **інформаційного забезпечення** полягає у:

– налаштуванні ефективної інформаційної системи, яка допоможе учасникам прийняття рішень використовувати готові типові рішення;

– розробці інструктивно-методичних матеріалів для персоналу підприємства, необхідних для організації роботи в процесі реалізації стратегії.

Інформаційна система механізму реалізації стратегії фінансово-економічної безпеки – сукупність технічних, програмних, методичних та інформаційних засобів, спрямованих на підтримку і підвищення ефективності реалізації стратегії.

Нормативно-правове забезпечення покликане розробити ряд нормативних та розпорядчих документів: наказ про початок реалізації стратегії фінансово-економічної безпеки та організацію цього процесу на підприємстві, положення про окремі підрозділи з урахуванням особливостей реалізації

стратегії, положення про преміювання працівників в процесі реалізації стратегії, посадові та робочі інструкції тощо.

Формування та реалізація стратегії фінансово-економічної безпеки підприємств – частина загального стратегічного управління підприємством, тому стратегія фінансово-економічної безпеки повинна бути узгоджена із корпоративною стратегією та функціональними стратегіями фінансово-економічної безпеки підприємства.

Впроваджувати розроблений механізм реалізації стратегії фінансово-економічної безпеки в діяльність підприємства необхідно поетапно.

ЕТАП 1. Підготовчий (формування умов для впровадження розробленого механізму реалізації стратегії)

1.1. Перевірка узгодженості стратегії фінансово-економічної безпеки з іншими стратегіями підприємства.

1.2. Формування організаційної структури та культури відповідно до вимог розробленого механізму.

1.3. Розробка моделі роботи персоналу в процесі реалізації стратегії.

1.4. Проведення опитування персоналу з метою визначення мотиваційних факторів та розробка на основі його результатів системи мотивації персоналу для успішної реалізації стратегії.

1.5. Доведення до відома персоналу вимог до впровадження механізму та проведення корпоративного навчання і тренінгового адаптування.

1.6. Розробка системи збору, обробки, аналізу та зберігання інформації моніторингу впливу чинників зовнішнього та внутрішнього середовищ діяльності підприємства.

1.7. Розробка інформаційного забезпечення моніторингу реалізації стратегії та оцінювання його ефективності.

1.8. Розробка інформаційного забезпечення оцінки ризиків реалізації стратегії.

1.9. Розробка планів розподілу ресурсів підприємства в процесі реалізації стратегії.

1.10. Розробка нормативно-розпорядчих документів для впровадження механізму реалізації стратегії.

ЕТАП 2. Виконавчий (безпосереднє впровадження розробленого механізму реалізації стратегії)

2.1. Виконання сукупності дій з реалізації системи оперативних, тактичних і стратегічних планів досягнення довгострокових цілей підприємства щодо забезпечення фінансово-економічної безпеки.

2.2. Проведення моніторингу впливу чинників зовнішнього та внутрішнього середовищ діяльності підприємства.

2.3. Проведення моніторингу реалізації стратегії фінансово-економічної безпеки.

2.4. Оцінка та нівелювання ризиків у процесі реалізації стратегії фінансово-економічної безпеки

ЕТАП 3. Заключний

3.1. Оцінка ефективності впровадження механізму реалізації стратегії фінансово-економічної безпеки.

3.2. Формування висновків про ефективність механізму реалізації стратегії та розробка рекомендацій (при потребі) для його удосконалення

Будь-який процес на підприємстві, в тому числі і механізм реалізації стратегії фінансово-економічної безпеки, повинен бути оцінений з точки зору досягнутого результату. Від загальної ефективності механізму реалізації стратегії фінансово-економічної безпеки та сприятливості зовнішнього і внутрішнього середовищ буде залежати розвиток підприємства у перспективі.

Виділяють такі важливі моменти для оцінки ефективності механізму реалізації стратегії фінансово-економічної безпеки:

1. Оцінку ефективності механізму реалізації стратегії необхідно здійснювати з чітко визначеною періодичністю.

2. Протягом усього періоду реалізації стратегії необхідно удосконалювати процес оцінки ефективності механізму шляхом використання передових методик з урахуванням змін умов реалізації стратегії економічної безпеки.

3. Розрахунок ефективності механізму повинен здійснюватися на основі ключових показників (зрозумілих для працівників підприємства), які дозволять кількісно виміряти успіхи підприємства у досягненні стратегічних цілей.

4. Здійснювати комплексний аналіз ефективності механізму шляхом порівняння поточних значень із попередніми значеннями, визначення закономірності їхньої зміни, пошук резервів підвищення ефективності механізму.

6.3. Моніторинг реалізації стратегії фінансово-економічної безпеки підприємства

Один із найважливіших напрямів дій менеджерів у процесі реалізації стратегії фінансово-економічної безпеки – *моніторинг*, який передбачає:

– моніторинг реалізації стратегії фінансово-економічної безпеки;

– моніторинг впливу чинників зовнішнього та внутрішнього середовищ діяльності підприємства.

Моніторинг реалізації стратегії фінансово-економічної безпеки – це безперервний процес збору, обробки й аналізу інформації про перебіг реалізації стратегії, аналіз відхилень у реалізації стратегії та їх причин, розроблення програм дій на нівелювання негативних відхилень.

Впровадження на підприємстві **моніторингу реалізації стратегії повинно базуватися на таких принципах:**

– *наукової обґрунтованості* – всі заходи, передбачені моніторингом, повинні розроблятися на основі сучасних наукових вітчизняних та зарубіжних досліджень;

– *достовірності та об'єктивності інформації* – зібрана інформація повинна бути достовірною для проведення якісного аналізу відхилень у реалізації стратегії;

– *безперервності* – моніторинг повинен проводитись не епізодично, а безперервно протягом усього періоду реалізації стратегії;

– *конфіденційності* – недопущення розголосу конфіденційної інформації про хід реалізації стратегії економічної безпеки та внесені до цього процесу зміни;

– *ефективності* – отримання позитивного ефекту від впровадження моніторингу, оптимізація витрат на проведення моніторингу;

– *інтегрованості* – моніторинг повинен перебувати у тісній взаємодії з усіма елементами механізму реалізації стратегії;

– *відповідності місії та цілям* – в кінцевому результаті здійснення моніторингу зіставляються результати діяльності підприємства із її цілями та місією.

Завданнями моніторингу реалізації стратегії фінансово-економічної безпеки підприємства є:

– організація безперервного спостереження за реалізацією стратегії фінансово-економічної безпеки;

– отримання достовірної та об'єктивної інформації про хід реалізації стратегії;

– надання посадовим особам підприємства та підрозділам управління підприємством інформації, отриманої при здійсненні моніторингу;

– виявлення проблем реалізації стратегії та підготовка рекомендацій на подолання негативних тенденцій для стабілізації процесу реалізації стратегії і підтримку позитивних тенденцій для активізації процесу реалізації стратегії;

– аналіз змін у діяльності підприємства в результаті виконання стратегії.

За допомогою моніторингу реалізації стратегії виявляються слабкі місця діяльності підприємства в процесі реалізації стратегії фінансово-економічної безпеки, які спонукають до вдосконалення управління та підвищення ефективності реалізації стратегії.

Проведенню моніторингу реалізації стратегії фінансово-економічної безпеки передує виконання таких дій:

1. Формування системи показників, які будуть визначатися в процесі моніторингу реалізації стратегії та встановлення періодичності його проведення.

2. Розробка форми звітності результатів моніторингу реалізації стратегії фінансово-економічної безпеки.

3. Розробка методик аналізу відхилень у реалізації стратегії фінансово-економічної безпеки.

Моніторинг реалізації стратегії фінансово-економічної безпеки доцільно здійснювати за такими показниками – кількісно-якісними характеристиками процесу реалізації стратегії:

– витрати на реалізацію стратегії фінансово-економічної безпеки – визначає економію або перевитрати щодо процесу реалізації стратегії фінансово-економічної безпеки;

– термін реалізації стратегії фінансово-економічної безпеки – дозволяє встановити фактично витрачений час на окремі етапи реалізації стратегії та реалізацію стратегії загалом;

– рівень виконання заходів щодо мотивації діяльності персоналу в процесі реалізації стратегії – визначає, чи в повній мірі виконуються заходи щодо мотивації персоналу і чи вони ефективні;

– рівень забезпеченості процесу реалізації стратегії ресурсами – характеризує здатність підприємства до ресурсного забезпечення процесу реалізації стратегії;

– повнота та правильність виконання всіх передбачених заходів – показує повноту здійснення запланованих процесом реалізації стратегії заходів та правильність їхнього виконання.

6.4. Моніторинг впливу чинників зовнішнього та внутрішнього середовища на процес реалізації стратегії фінансово-економічної безпеки

Підприємство як відкрита система перебуває під постійним впливом зовнішнього середовища, яке є одночасно і джерелом необхідних для підприємства ресурсів, і споживачем його продукції, та внутрішнього середовища.

Дестабілізуючий вплив обох середовищ призводить до виникнення негативних наслідків у реалізації стратегії фінансово-економічної безпеки.

Тому вважаємо за необхідне передбачити в механізмі реалізації стратегії процес моніторингу зовнішнього та внутрішнього середовищ діяльності підприємства.

Моніторинг впливу чинників зовнішнього та внутрішнього середовищ покликаний забезпечити безперервне протягом усього періоду реалізації стратегії спостереження за негативним впливом на процес реалізації стратегії.

Основне завдання моніторингу впливу чинників зовнішнього та внутрішнього середовищ – прийняття управлінських рішень щодо знешкодження негативного впливу на процес реалізації стратегії. Прийняття таких управлінських рішень базуються на попередній оцінці їх негативного впливу.

Чинники, які впливають на процес реалізації стратегії фінансово-економічної безпеки:

Рис. 6.2. Чинники, які впливають на процес реалізації стратегії фінансово-економічної безпеки

Чинники зовнішнього і внутрішнього середовищ діяльності підприємства та характер їхнього впливу на процес реалізації стратегії фінансово-економічної безпеки

Таблиця 6.1

Компонента макросередовища	**Чинник**	**Вплив чинника на процес реалізації стратегії**
1	2	3
Стан економіки	Фінансово-економічна політика держави	Високе податкове навантаження, рівень інфляції, який супроводжується знеціненням активів підприємства, призводить до зростання собівартості продукції і, відповідно, до зниження прибутковості підприємства
	Система оподаткування	
	Рівень інфляції	
Соціально-культурні обставини	Рівень освіти населення	Формує рівень попиту на продукцію підприємства
	Пануючі у суспільстві традиції і цінності	
	Смаки та уподобання споживачів	
	Стан соціального забезпечення громадян	
	Рівень доходу населення	
Демографічна ситуація	Рівень народжуваності	Визначає потребу у продукції підприємства
	Міграційні тенденції	
	Вікова структура населення	
	Розміщення населення на території країни	
Політико-правові	Стан законодавства, яке регулює господарську діяльність	Впливає на загальну стабільність функціонування підприємства
	Політична ситуація в країні	
	Стан законодавства, яке регулює трудову діяльність	
Технологічні	Тенденції технологічних змін в економічній діяльності	Впливає на забезпеченість виробничого процесу на підприємстві
	Державне регулювання наукових досліджень	
Компонента мікросередовища	**Чинник**	**Вплив чинника на процес реалізації стратегії**
Конкуренти	Частка ринку	Загострення конкуренції призводить до зменшення обсягів реалізації продукції та зниження доходу, що впливає на забезпеченість реалізації стратегії власними коштами
	Асортиментний ряд	
	Організація збутової діяльності	
	Стратегія розвитку	
Постачальники	Ціна товару	Несвоєчасна поставка необхідних ресурсів, незадовільна якість, підвищення цін на них, невиконання вимог постачання знижує ефективність реалізації стратегії
	Рівень спеціалізованості та якість товару	
	Умови постачання та оплати товару	
	Географічне розміщення від покупця	

Продовження табл. 6.1

1	2	3
Покупці	Соціально-психологічні характеристики (манера поведінки, смаки, традиції)	Відсутність орієнтації на потреби споживачів призведе до незадоволення потреб споживачів та зростання незабезпеченого попиту
	Ставлення до продукту	
	Лояльність клієнтської бази	
Органи державної влади	Вплив органів влади на діяльність суб'єкта господарювання	Зумовлює вплив на подальший загальний розвиток підприємства
	Рівень корумпованості органів влади	
Компонента внутрішнього середовища	**Чинник**	**Вплив чинника на процес реалізації стратегії**
Матеріально-технічна	Рівень фізичного та морального спрацювання обладнання	Здійснює вплив на виготовлення неконкурентоспроможної продукції, підвищення витрат на виробництво продукції та зниження її якості
	Рівень оновлення обладнання	
	Рівень використання новітніх технологій у виробництві продукції	
	Рівень своєчасності здійснення поточного та капітального ремонту обладнання	
	Рівень забезпечення матеріальними ресурсами	
Організаційно-економічна	Ефективність менеджменту підприємства	Впливає на рівень досягнення стратегічних цілей, ефективність та своєчасність прийняття управлінських рішень та визначення напряму розвитку підприємства
	Рівень контролю діяльності підприємства	
	Розподіл обов'язків між підрозділами підприємства	
Соціально-психологічна	Рівень кваліфікації персоналу	Характеризує вплив на рівень ефективності виконання завдань персоналом підприємства у реалізації стратегії
	Ставлення працівників до роботи	
	Ефективність матеріального стимулювання персоналу	
	Ефективність нематеріального стимулювання персоналу	
	Відсутність розуміння стратегії персоналом підприємства	
	Наявність навчальних корпоративних програм	
	Рівень готовності персоналу до змін на підприємстві	
	Несприятливий соціально-психологічний клімат в колективі	

Продовження табл. 6.1

1	2	3
Фінансово-інвестиційна	Рівень інвестиційної активності	Впливає на необхідність пошуку додаткових джерел інвестування, що сприятиме зростанню ефективності діяльності підприємства; незбалансованість інвестиційних потреб та можливостей підприємства
	Рівень забезпеченості власними фінансовими ресурсами	
	Ефективність системи збуту	
Інформаційна	Наявність точної та своєчасної інформації для прийняття управлінських рішень	Відсутність інформації про поточний стан діяльності підприємства, наявних відхилень від запланованих дій призведе до зниження ефективності виконання запланованих стратегічних дій

Аналіз впливу зовнішнього і внутрішнього середовищ на процес реалізації стратегії економічної безпеки здійснюється експертами підприємства. В процесі опитування експерти присвоюють кожному чиннику бальне значення рівня впливу на процес реалізації стратегії: “0” – вплив чинника відсутній; “1-4” – чинник справляє незначний вплив; “5-7” – середній вплив; “8-10” – сильний вплив. На основі результатів опитування визначається середнє бальне значення за кожним чинником та здійснюється статистична обробка результатів: оцінка узгодженості думок як всієї групи експертів на основі коефіцієнта конкордації, так і для пари експертів за допомогою коефіцієнта парної рангової кореляції.

Здійснюючи моніторинг впливу чинників на процес реалізації стратегії, необхідно формувати базу даних на основі проведеного спостереження та системного аналізу, яка буде використовуватися для порівняння результатів за різні періоди, що дозволить виявити тенденції і закономірності негативного впливу чинників. Це дасть можливість прогнозувати, які саме чинники в майбутньому здійснюватимуть негативний вплив, та на основі цих прогнозів розробляти заходи щодо його зменшення.

6.5. Безперервне навчання персоналу в процесі реалізації стратегії фінансово-економічної безпеки

Важливим напрямом дій у процесі реалізації стратегії фінансово-економічної безпеки є **безперервне навчання персоналу** за попередньо затвердженими на підприємстві програмами і графіком.

Основні завдання безперервного навчання персоналу в процесі реалізації стратегії фінансово-економічної безпеки:

– сприяння ефективному виконанню поставлених завдань досягнення запланованих стратегічних цілей;

– оволодіння методами реагування на проблемні ситуації в процесі реалізації стратегії;

– сприяння розвитку творчого потенціалу кожного працівника;

– налагодження лояльних взаємовідносин між працівниками підприємства, що сприятиме їхній злагодженій роботі в процесі реалізації стратегії;

– створення умов для обміну досвідом між працівниками різних підрозділів підприємства;

– створення команди, здатної реалізувати обрану стратегію.

Навчання персоналу в процесі реалізації стратегії фінансово-економічної безпеки включає такі етапи:

Етап 1 «Оглядовий» – передбачає:

– ознайомлення працівників із обраною стратегією;

– роз'яснення системи показників стратегічних цілей;

– встановлення рівня готовності персоналу до реалізації стратегії;

– визначення місця та ролі кожного працівника в процесі реалізації стратегії.

Етап 2 «Оперативний» – спрямований на надання допомоги кожному працівнику стосовно виконання обов'язків у процесі реалізації стратегії та вирішенні проблемних ситуацій як в окремих підрозділах підприємства, так і підприємства загалом.

Етап 3 «Кінцевий» – виявляють причини, які вплинули на невиконання чи неналежне виконання запланованих завдань окремими підрозділами та працівниками за звітний період, аналізують наслідки невиконання запланованих завдань та їхній вплив на процес реалізації стратегії фінансово-економічної безпеки підприємства.

Запровадження на підприємствах безперервної системи навчання персоналу сприятиме формуванню команди персоналу відповідно до потреб стратегії, дозволить швидше та якісніше вирішувати проблемні ситуації в процесі реалізації стратегії.

ТЕМА 7
ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ В СИСТЕМІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

7.1. Сутність фінансової безпеки підприємства

Фінансова безпека є однією з найважливіших складових системи фінансово-економічної безпеки суб'єктів підприємництва, оскільки саме фінансова складова є матеріальною основою в сучасній економіці як на макро- так і на мікрорівні.

В економічній літературі недостатньо уваги приділяється питанням фінансової безпеки підприємства тому, що деякі з їх аспектів розглядаються при розробці фінансової політики підприємства, управлінні фінансами, управлінні ризиками, проте комплексний підхід до цієї проблеми відсутній.

Фінансова безпека підприємства – це здатність підприємства ефективно і стабільно здійснювати свою господарську, в т.ч. й фінансову діяльність, шляхом використання сукупності взаємопов'язаних діагностичних, інструментальних та контрольних заходів фінансового характеру, які повинні оптимізувати використання фінансових ресурсів, забезпечити належний їх рівень та нівелювати вплив ризиків внутрішнього та зовнішнього середовищ.

Ключові риси фінансової безпеки підприємства:

− забезпечує рівноважний та стійкий фінансовий стан;

− сприяє ефективній діяльності підприємства;

− дозволяє на ранніх стадіях визначити проблемні місця в діяльності підприємства;

− нейтралізує кризи та запобігає банкрутству.

Фінансова безпека визначається такими факторами:

− рівнем забезпеченості фінансовими ресурсами;

− стабільністю і стійкістю фінансового стану підприємства;

− збалансованістю фінансових потоків і розрахункових відносин;

− ступенем ефективності фінансово-економічної діяльності;

− рівнем контролю за зовнішніми та внутрішніми ризиками.

Завдання, які висуваються перед фінансовою безпекою:

− ідентифікація ризиків і пов'язаних з ними потенційних загроз;

− визначення індикаторів фінансової безпеки підприємства;

− впровадження системи діагностики та моніторингу стану фінансової безпеки;

− контроль та оцінка ефективності дії системи фінансової безпеки;

− створення необхідних фінансових умов, що забезпечують стабільне зростання підприємства;

− створення умов для формування оптимального обсягу фінансових ресурсів із зовнішніх та внутрішніх джерел;

− підтримка фінансової стійкості та платоспроможності підприємства протягом усього періоду функціонування;

− створення умов, необхідних для забезпечення оптимального обсягу й рівня ефективності інвестицій;

− мінімізація фінансових ризиків підприємства;

− своєчасне впровадження у фінансову діяльність підприємства сучасних технологій управління та інструментарію їх забезпечення;

− ефективний та швидкий вихід підприємства з фінансової кризи та нейтралізація її наслідків.

Об’єктами впливу для реалізації цих завдань можуть бути:

− прибуток;

− капітал;

− інвестиції;

− інші джерела формування та використання фінансових ресурсів;

− фінансові та економічні ризики;

− кризи тощо.

Реалізація завдань, поставлених перед фінансовою безпекою підприємства, можлива при виконанні певних функцій управління, які можна об’єднати в дві групи:

1. Функції, характерні для кожної системи управління будь-якого рівня менеджменту.

2. Функції системи управління як спеціалізованого напряму фінансового менеджменту.

У першій групі основними функціями управління фінансовою безпекою підприємства є такі:

− формування повної та достовірної інформації, необхідної суб’єкту підприємництва для прийняття адекватних, ефективних і законних рішень у сфері забепечення власної фінансової безпеки;

− створення системи аналізу стану фінансової безпеки підприємства, визначаючи найважливіші її параметри шляхом виявлення ступеня деструктивного впливу економічного середовища на фінансові пріоритети підприємства;

− створення системи стимулів і заохочень для менеджерів за прийняття ефективних управлінських рішень і системи санкцій з неспроможністю їх дій;

− організація системи контролю з метою виявлення порушень при прийнятті упралінських рішень.

У другій групі функцій управління можна виділити такі:

− розробка стратегії забезпечення фінансової безпеки підприємства на основі системи довгострокового та поточного планування;

− управління рентабельністю підприємства, оптимізуючи процес використання власного капіталу для збільшення суми чистого прибутку, що припадає на його одиницю;

− управління фінансовими ресурсами підпрємства в процесі їх формування;

− управління фінансовою стабільністю підприємства, забезпечення фінансової стійкості та платоспроможності;

− управління інвестиційною діяльністю з метою підвищення її ефективності та забезпечення її активності;

− управління фінансовими ризиками підприємства з метою мінімізації їх наслідків;

− управління фінансовими інноваціями в сфері забезпечення фінансової безпеки підприємства.

7.2. Загрози фінансовій безпеці підприємства

Зовнішні загрози фінансовій безпеці – це різні негативні дії, які доводять підприємство до кризового становища, або погіршують конкурентноздатність підприємства на ринку.

До ним належать:

− несприятливі макроекономічні умови: загальноекономічна ситуація в країні і регіоні, кризи;

− урядові кризи;

− нестабільність нормативно-правової бази;

− нестабільність податкової, кредитної і страхової політики;

− рівень інфляції і прогноз інфляції;

− нестабільність валютної політики держави і/або валютного курсу;

− низький рівень інвестиційної активності регіону;

− несприятливі умови кредитування підприємств, зміна відсоткових ставок за кредитами;

− недобросовісна конкуренція на ринку;

− несприятлива криміногенна ситуація в регіоні, поширення кримінальних і фінансових злочинів у фінансово-кредитній сфері;

− спекулятивні операції на ринку цінних паперів;

− лобіювання конкурентами недостатньо виважених рішень органів влади;

− незаконне заволодіння майном окремими особами – рейдерство;

− форс-мажорні обставини: стихійні лиха, воєнні конфлікти, а також форс мажорні обставини економічного характеру (економічна криза, блокада, ембарго,несприятлива, або різка зміна курсу валюти, обвал фондових бірж).

Внутрішні загрози фінансовій безпеці – це недосконала діяльність самого підприємства, або різні прорахунки персоналу підприємства, через які підприємство неефективно проводить фінансові операції, виробляє неконкурентноздатну продукцію, що негативно впливає на діяльність підприємства.

До внутрішніх загроз відносять:

− некваліфіковане управління, помилки в стратегічному плануванні і ухваленні тактичних рішень;

− слабке маркетингове опрацювання ринку;

− недостатня ліквідність активів підприємства;

− низький рівень кваліфікації основного персоналу;

− неконкурентна цінова політика;

− слабке технічне озброєння підприємства;

− перебої в роботі устаткування і комунікацій;

− помилки в організації збереження фінансових і матеріальних цінностей;

− просочування стратегічної і фінансової інформації підприємства, недоліки в організації роботи служби безпеки підприємства;

− низький рівень бізнес-репутації підприємства;

− відсутність планування діяльності підприємства в аварійних ситуаціях;

− недотримання контрактів і договірних зобо'язань.

Однією з найважливіших загроз фінансовій безпеці є **фінансова нестабільність.** Критерієм стійкого фінансового стану є фінансова рівновага, що в загальному вигляді визначається збалансованістю фінансових активів та позикового капіталу. Порушення фінансової рівноваги призводить до появи кризи (нездатності здійснювати фінансове забезпечення поточної виробничої діяльності), і в подальшому може призвести до банкрутства.

Банкрутство – визнана господарським судом неспроможність боржника відновити свою платоспроможність та задовольнити визнані судом вимоги кредиторів не інакше як через застосування ліквідаційної процедури. Банкрутство підприємства − це підсумковий результат глибокої фінансової кризи, що унеможливлює нормальну діяльність підприємства та робить його неплатоспроможним.

7.3. Показники фінансової безпеки підприємства

Сутність фінансової безпеки підприємства полягає у досягненні та утриманні його фінансової стійкості, ліквідності, платоспроможності, забезпеченні оборотності активів та прибутковості, тобто характеризує фінансову забезпеченість діяльності підприємства.

Про ослаблення фінансової безпеки свідчить:

– зниження ліквідності підприємства;

– підвищення кредиторської та дебіторської заборгованості;

– зниження фінансової стійкості;

– зниження рентабельності підприємства;

– порушення ритмічності реалізації продукції тощо.

Показники, за допомогою яких можна оцінити стан фінансової безпеки на підприємстві:

1. Показники ліквідності:

– коефіцієнт загальної ліквідності

($К_{зл}$ = Поточні активи / Поточні зобов'язання);

– коефіцієнт швидкої ліквідності

($К_{шл}$ = Грошові кошти, поточні фінансові інвестиції, векселі одержані та

дебіторська заборгованість / Поточні зобов'язання);

– коефіцієнт абсолютної ліквідності

($К_{АЛ}$ = Грошові кошти та поточні фінансові інвестиції / Поточні зобов'язання).

2. Показники платоспроможності (фінансової стійкості):

– коефіцієнт автономії (фінансової незалежності)

($К_{ФН}$ = Власний капітал підприємства / Загальні джерела фінансування);

– коефіцієнт фінансового ризику

($К_{ФР}$ = Залучений капітал / Власний капітал підприємства);

– коефіцієнт забезпечення боргів

($К_{ЗБ}$ = Власний капітал / Залучений капітал підприємства).

3. Показники ділової активності:

– коефіцієнт оборотності оборотних активів

($К_{ОА}$ = Чиста виручка від реалізації / Середній залишок оборотних активів);

– коефіцієнт оборотності необоротних активів

($К_{ОН}$ = Чиста виручка від реалізації / Середній залишок необоротних активів);

– коефіцієнт оборотності кредиторської заборгованості

($К_{ОКЗ}$ = Чиста виручка від реалізації / Середній залишок кредиторської заборгованості);

– коефіцієнт оборотності дебіторської заборгованості

($К_{ОДЗ}$ = Чиста виручка від реалізації / Середній залишок дебіторської заборгованості);

– коефіцієнт оборотності власного капіталу

($К_{ОВК}$ = Чиста виручка від реалізації / Середня величина власного капіталу);

– період погашення дебіторської заборгованості

(Дебіторська заборгованість·365/виручка);

– період погашення кредиторської заборгованості

(Кредиторська заборгованість·365/виручка).

4. Показники рентабельності:

– рентабельність активів

($Р_{А}$ = Чистий прибуток х 100% / Середня вартість активів);

– рентабельність власного капіталу

($Р_{ВК}$ = Чистий прибуток х 100% / Середня величина власного капіталу);

– рентабельність продукції (Чистий прибуток/собівартість продукції).

7.4. Оцінювання стану фінансової безпеки підприємства

Для оцінювання стану фінансової складової безпеки підприємства використовують різноманітні методи залежно від наявної інформації про її індикатори. Оцінювання рівня фінансової безпеки залежить також від того, з якою метою проводять дослідження системи фінансової безпеки.

Можна виділити такі методи оцінювання рівня фінансової безпеки підприємства:

− моніторинг фінансової діяльності суб'єкта господарювання;

− методи експертних оцінок;

− метод аналізу й обробки сценаріїв;

− методи оптимізації;

− теоретико-ігрові методи;
− економетричні методи;
− методи прогнозування;
− методи теорії штучних нейронних мереж;
− методи нечіткої логіки і нечітких множин.

Під **моніторингом основних показників діяльності підприємства** розуміють механізм постійного спостереження за основними показниками поточної діяльності в умовах постійних змін кон'юнктури фінансового ринку.

Методи експертного оцінювання використовують для опису кількісних і якісних характеристик досліджуваних процесів, зокрема для побудови логічних правил вибору рішень, які формують експерти на основі власних уявлень та знань про будь-яку сферу проблем; розроблення бального оцінювання рівня фінансової безпеки на основі аналізу результатів розпізнавання фактичних індикаторів фінансової безпеки.

Метод аналізу й обробки сценаріїв (сценарний підхід) передбачає багатоваріантний ситуаційний розгляд системи фінансової безпеки підприємства. Сценарій – це динамічна модель майбутнього, яка описує хід подій із передбаченням ймовірності їх реалізації..

Для моделювання безпеки підприємства використовують **методи оптимізації,** які полягають у виборі найкращого варіанта рішення із багатьох можливих (допустимих). Допустимість кожного розв'язку визначається можливістю реалізації відповідних його наслідків за наявних ресурсів. Обмеженість ресурсів переважно виражають у вигляді системи рівнянь і(або) нерівностей, яка описує внутрішні технологічні й економічні процеси функціонування та розвитку виробничо-економічної системи, а також процеси зовнішнього середовища, які впливають на результат діяльності системи.

Оптимальність розв'язку задачі передбачає наявність деякої системи цілей, які називають критеріями оптимальності. Наближення діяльності економічної системи до поставленої мети функціонування та розвитку описують за допомогою цільової функції (функції мети).

У загальному випадку оптимізаційна модель має такий вигляд:

$$f(x) \rightarrow extr,$$

за обмежень

$$gi(x) = 0,\ i\ 1,\ m\ ,$$

де $x = (x1, x2, \ldots, xn)$ – сукупність невідомих змінних моделі;

$f(x)$ – цільова функція моделі;

$gi(x)$ –система обмежень моделі.

Застосування методів оптимізації до управління фінансовою безпекою підприємства дає змогу вибрати такий режим його функціонування, який забезпечить досягнення екстремального значення цільової функції системи фінансової безпеки. Оскільки стан системи фінансової безпеки підприємства характеризується великою кількістю показників (індикаторів), то під цільовою функцією переважно розуміють один із показників ефективності діяльності підприємства, наприклад величину прибутку (доходу) підприємства.

Теоретико-ігрові методи використовують для аналізу багатосторонніх конфліктних ситуацій, тобто ситуацій, коли інтереси учасників конфлікту є протилежними або не збігаються. Умовами застосування теоретико-ігрових методів є невизначеність та неповнота інформації. До них відносять теорію статистичних рішень, яку використовують у випадках, коли невизначеність навколишнього середовища викликана об'єктивними обставинами випадкового характеру, а також теорію ігор, яку використовують у тих випадках, коли невизначеність оточення викликана свідомими діями розумного супротивника.

Враховуючи, що динаміка кожного індикатора системи фінансової безпеки підприємства зумовлена впливом багатьох, часто випадкових чинників, цю систему можна представити у вигляді багатовимірного випадкового вектора, компонентами якого виступають індикатори фінансової безпеки підприємств. Для дослідження стану та поведінки таких багатовимірних об'єктів доцільно застосовувати добре розвинутий апарат економетрії, наприклад **методи кореляційно-регресійного аналізу.**

Економетричне дослідження системи фінансової безпеки підприємства дозволяє досліджувати залежності між окремими чинниками цієї системи, а також аналізувати характеристики швидкості та інтенсивності динаміки стану фінансової безпеки суб'єкта господарювання.

Залежно від джерел інформації щодо майбутнього і способу його прогнозування виділяють такі **методи прогнозування,** що взаємно доповнюють одне одного:

1. Експертний метод прогнозування, заснований на мобілізації професійного досвіду та інтуїції висококваліфікованих експертів для одержання прогнозів, що не мають кількісних характеристик.
2. Екстраполяція, яка полягає у дослідженні ретроспективних даних про розвиток об'єкта та перенесення закономірностей цього розвитку на майбутнє.

Під **нейронними мережами** розуміють обчислювальні структури, що моделюють прості біологічні процеси, які асоціюються з процесами людського мозку. Можливості методів теорії штучних нейронних мереж щодо моделювання складних нелінійних залежностей зумовлюють їхнє використання для аналізу динаміки економічної безпеки. Нейронні мережі можна також використовувати для дослідження задач, розв'язування яких здійснюють за допомогою лінійних методів і алгоритмів, а також статистичних методів аналізу (кореляційно-регресійний, кластерний, дискримінантний аналіз, аналіз часових рядів тощо).

Математична теорія нечітких множин і нечітка логіка є узагальненням класичної теорії множин і класичної формальної логіки. Методи нечіткої логіки використовують для моделювання фінансових систем в умовах істотної невизначеності та інтерпретації класичних ймовірнісних й експертних оцінок рівня фінансової безпеки підприємства. Теорія нечітких множин надає дослідникам високорозвинутий формальний апарат для адекватного перенесення якісних висловлювань експерта у деяке кількісне вираження.

Варто зробити висновок, що особливості методів оцінювання рівня фінансової безпеки підприємства пов'язані з вибором індикаторів фінансової

безпеки, використанням різних процедур згортки множини індикаторів та виділенням рівнів фінансової безпеки підприємства.

Оцінювання рівня фінансової безпеки підприємства можна здійснювати за допомогою **інтегрального показника** через зважування й підсумовування окремих індикаторів фінансової безпеки підприємства, або узагальнені значення окремих показників діяльності підприємства (ліквідності, фінансової стійкості, ділової активності та рентабельності).

Іншим підходом до визначення рівня фінансової безпеки підприємства є визначення ступеня досягнення підприємством деякого «ідеального» стану, який є найкращим з огляду на динаміку розвитку підприємства, результати його діяльності. Такий «ідеальний» стан задається граничними значеннями показників фінансового стану підприємства, перевищення або заниження яких негативно впливає на здатність підприємства до розвитку. Згідно з таким підходом пропонується оцінювати фінансову безпеку підприємства на підставі зіставлення граничних і фактичних значень індикаторів фінансового стану. Індикаторами рівня безпеки підприємства запропоновано використовувати нормовані значення показників безпеки:

Ілляшенко С. М. запропонував оцінювати фінансову безпеку підприємства на основі аналізу його фінансової стійкості, ступінь якої визначається, виходячи з достатності оборотних коштів (власних чи позичених) для здійснення виробничо-збутової діяльності.

Оцінними показниками є:

$\pm Ec$ – надлишок (+) чи брак (-) власних оборотних коштів (Ee), необхідних для формування запасів і покриття витрат (Z), пов'язаних із господарською діяльністю підприємства;

$\pm Em$ – надлишок чи брак власних оборотних коштів, а також середньострокових і довгострокових кредитів та позик (K);

$\pm Eн$– надлишок чи брак власних оборотних коштів, а також довго-, середньо- та короткострокових кредитів та позик ($Kт$).

Ці показники відповідають показникам забезпеченості запасів і витрат джерелами їхнього формування та розраховуються за такими формулами:

$$\pm Ec = Ee - Z,$$
$$\pm Em = (Ee + K) - Z,$$
$$\pm Eн = (Ee + Kт + K) - Z.$$

Наведені вище показники є основою формування п'яти рівнів фінансової безпеки підприємства:

− абсолютний – для функціонування підприємства достатньо власних оборотних коштів:

$$\pm Ec \geq 0, \pm Em \geq 0, \pm Eн \geq 0;$$

− нормальний – підприємство практично обходиться власними джерелами формування запасів і покриття витрат:

$$\pm Ec \approx 0, \pm Em \geq 0, \pm Eн \geq 0;$$

− хиткий – підприємству недостатньо власних оборотних коштів і воно вдається до середньострокових та довгострокових позик і кредитів:

$$\pm Ec < 0, \pm Em \geq 0, \pm Eн \geq 0;$$

− критичний – підприємство для фінансування своєї діяльності вдається до короткострокових кредитів:

$$\pm Ec < 0, \pm Em < 0, \pm Eн \geq 0;$$

− кризовий – підприємство неспроможне забезпечити фінансування діяльності ні власними, ні позиченими коштами:

$$\pm Ec < 0, \pm Em < 0, \pm Eн < 0.$$

Потрібно зауважити, що такий підхід до оцінювання рівня фінансової безпеки є досить вузьким, оскільки досліджує тільки платоспроможність підприємства і не охоплює таких аспектів фінансової діяльності, як ділова активність і рентабельність.

Результатом наявності постійної фінансової небезпеки може бути банкрутство підприємства. Для прогнозування кризових станів у діяльності підприємства дуже часто використовують **моделі оцінювання схильності до банкрутства.**

Історично проблемою прогнозування криз та ймовірності настання банкрутства зацікавилися на Заході (переважно США) ще по закінченні Другої світової війни. Проте серйозно цією проблемою почали займатися в 60-х роках XX ст. із застосуванням методів математичного аналізу. З того часу і до наших днів розроблено безліч методик прогнозування банкрутства підприємтв, які можна поділити на дві групи: *кількісні* (моделі Альтмана, Фултона, Лиса, Бівера) та *якісні* (модель Аргенті).

Перша відома модель діагностики з метою оцінки ймовірності настання кризи розроблена в 30- роках XX ст. Бівером для підприємтв Англії у вигляді так званого коефіцієнта Бівера (КБ), що розраховується як відношення припливу грошових коштів до залучених коштів.

Першою серйозною кількісною моделлю проозування банкрутства була 5-ти факторна модель Альтмана.

Найбільш відомою серед якісних методик прогнозування настання криз є метод Аргенті (розроблений професором Аргенті у 1976 році). Крім того, є універсальні методи діагностики, наприклад, SWOT аналіз. Його основним змістом є дослідження характеру сильних та слабких сторін підприємства в розрізі окремих внутрішніх факторів, а також позитивного чи негативного впливу окремих зовнішніх факторів, що обумовлюють кризовий фінансовий стан підприємства.

7.5. Система фінансової безпеки підприємства

Система фінансової безпеки підприємства – це сукупність взаємопов'язаних діагностичних, інструментальних та контрольних заходів фінансового характеру, які покликані оптимізувати використання фінансових ресурсів, забезпечити належний їх рівень та нівелювати вплив ризиків внутрішнього та зовнішнього середовищ.

Мета системи фінансової безпеки підприємства – забезпечення стабільної, безризикової та ефективної діяльності підприємства.

Функції системи фінансової безпеки підприємства:

− ідентифікація потенційно проблемних ситуацій, що полягає у визначенні проблемних мість у діяльності, оцінка причин їх виникнення та масштабів наслідків;

− ліквідація проблемних ситуацій, яка полягає у сукупності заходів з вибору важелів впливу на проблему та методів її усунення;

− контроль, що містить у собі всебічну оцінку ефективності вжитих заходів та аналіз поточного стану щодо наявності проблемних ситуацій;

− оптимізація фінансового управління, що полягає в забезпеченні оптимального використання фінансових ресурсів і потенціалу підприємства шляхом використання відповідного фінансового інструментарію та специфічних методів фінансового управління

Система фінансової безпеки повинна будуватися на таких принципах:

− мінливості;

− об'єктивності;

− обачності;

− безперервності та оперативності;

− конфіденційності;

− комплексності і системності;

− інтерпретації результатів.

Основні складові системи фінансової безпеки:

− підсистема діагностики;

− підсистема важелів і методів забезпечення фінансової безпеки;

− підсистема контролю й оцінки результатів дії системи в цілому та окремих її частин.

Однією з ключових складових системи є підсистема фінансової діагностики. Саме від її ефективності, своєчасності наданої інформації залежатиме результативність системи загалом.

Функції підсистеми фінансової діагностики:

– прогнозування настання кризи;

– оцінка ймовірності бакрутства підприємства;

– визначення масштабів кризи та її причини.

Діагностика – це певний набір методичних розробок, який дозволяє на ранніх стадіях визначити кризові ситуації, оцінити міру їх загрози для підприємства та фактори, що їх викликали.

Основна мета цієї підсистеми – вчасно інформувати про можливі проблемні місця в роботі підприємства, а також оцінювати ступінь загрози.

Основні завдання підсистеми фінансової діагностики:

– аналіз внутрішнього та зовнішнього середовищ підприємства;

– визначення кризового середовища підприємства і виділення критичних ризиків;

– оцінка ймовірності настання криз та можливості банкрутства;

– виділення проблемних місць у роботі підприємства, спираючись на результати проведеного аналізу;

– оцінка ефективності діяльності підприємства.

Підсистема фінансової діагностики включає такий комплекс діагностичних заходів:

– експрес діагностика (проводиться щомісяця);

– комплексна діагностика (щокварталу і складається з двох типів аналізу: якісний аналіз діяльності підприємства; комплексний аналіз із застосуванням коефіцієнтів);

– фундаментальна діагностика (раз на рік, проводяться такі заходи:: визначення стадії життєвого циклу піддприємства, якісний аналіз діяльності підприємства, визначення критичних ризиків підприємства, комплексний аналіз із застосуванням коефіцієнтів).

Центральною підсистемою системи фінансової безпеки підприємства є **підсистема фінансових важелів і методів забезпечення фінансової безпеки.**

Основна мета підсистеми – усунення кризових явищ і процесів, а також їхніх причин.

Основні завдання підсистеми:

− вибір оптимальної антикризової стратегії та інструментарію;

− нейтралізація кризових явищ;

− усунення причин криз;

− усунення наслідків криз;

− забезпечення ефективної діяльності підприємства.

Інструментарій, який повинен забезпечити ефективне виконання системою поставлених перед нею функцій, поділяють на дві групи:

– *фінансові методи* – управління прибутком, витратами, капіталом, управління грошовити потоками фінансовий аналіз, фінансове планування, фінансове регулювання, страхування тощо;

– *фінансові важелі* – прибуток, дохід, фінансові санкції, дивіденди, ціна, заробітна плата тощо.

Мета підсистеми контролю та оцінки результатів – контроль за належним виконанням своїх функцій іншими підсистемами та достовірна оцінка результативності й ефективності їх діяльності.

Підсистема контролю та оцінювання результатів виконує такі завдання:

− контроль за виконання своїх функцій іншими підсистемами системи фінансової безпеки підприємства;

− на підставі даних інших підсистем – визначення причин і масштабів кризи, а також результатів, яких необхідно досягти в рамках реалізації антикризових заходів;

− порівняння досягнутих результатів з очікуванити показниками;

− визначення ступеня відхилення фактичних результатів від запланованих;

− контроль за розробкою оперативних рішень з нормалізації фінансової діяльності підприємства;

− оцінка ефективності заходів щодо нейтралізації кризи, висновки про їх достатність та необхідність додаткових заходів;

− спостереження за ходом реалізації завдань з фінансового управління;

– забезпечення обміну інформаційними потоками між ключовими підсистемами та обробка інфомаційних потоків усередині системи.

У межах дії системи фінансової безпеки підприємства здійснюють два типи контролю:

– *поточний* (здійснюється під час виконання антикризових заходів та метою є відстеження відповідності фактичних результатів до поставлених завдань та оцінюється ступінь ефективності та адекватності дій щодо забезпечення фінансової безпеки);

– *підсумковий* (здійснюється за фактом закінчення звітного періоду чи реалізації комплексу антикризових заходів, його мета – перевірка відповідності досягнутих результатів поставленим цілям, а також оцінка ефективності розпочатих заходів та ухвалення рішення про необхідність додаткових заходів щодо забезпечення фінансової безпеки).

Функції підсистеми контролю та оцінювання результатів:

– оцінювання результатів дії системи фінансової безпеки та окремих її складових, ефективності їх функціонування та достатності. Підсумком дії функції є формування висновків за проведеною роботою;

– обмін інформаційними потоками між підсистемаи фінансової безпеки та аналітична робота;

–забезпечення взаємозв’язку між формуванням інформаційної бази, діагностикою, плануванням і контролюванням.

ТЕМА 8
ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛЬНО-КАДРОВОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

8.1. Сутність інтелектуально-кадрової безпеки виробничого підприємства

Відомий афоризм «кадри вирішують все» і сьогодні не втратив свого значення у забезпеченні фінансово-економічної безпеки підприємства.

Належний рівень фінансово-економічної безпеки залежить від складу кадрів, їхнього інтелекту та професіоналізму. Забезпечення інтелектуально-кадрової безпеки охоплює взаємопов'язані і водночас самостійні напрями діяльності, які спрямовані на роботу з персоналом.

З кадрами підприємства пов'язані основні внутрішні, а також зовнішні ризики, адже від економічних злочинів своїх працівників сьогодні страждають більше 40% підприємств, втрачаючи до 7% свого доходу.

Лише 20% спроб злому мереж і отримання несанкціонованого доступу до комп'ютерної інформації виникає ззовні, інші 80% випадків спровоковані за участі персоналу підприємства. Статистика свідчить, що 95% збитків на підприємствах США утворюється за особистої участі персоналу підприємств і тільки 5 % – унаслідок дій клієнтів та інших осіб. Статистичні дані Європейського Союзу показують, що приблизно 58% відомих випадків шахрайства й зловживань припадає на частку службовців, 30% – менеджерів, а 12% – топ-менеджерів і власників.

Персонал на сьогодні вважається тим цінним ресурсом, який впливає на усі аспекти життєдіяльності підприємства і дає змогу виходити на якісно новий рівень розвитку. Саме тому одним із актуальних питань є процес забезпечення високого рівня інтелектуально-кадрової безпеки, який є необхідним при запобіганні та нейтралізації загроз виробничо-комерційній діяльності підприємств. Тобто важливою постає проблема визначення інтелектуально-кадрової безпеки як самостійного об'єкту управління та розробки відповідних методів її забезпечення.

Сформоване на цей час поняття «інтелектуально-кадрова безпека» є синтезованим, інтегруючим у собі важливі характеристики категорій «персонал», «інтелектуальний потенціал», «кадрове забезпечення» та «безпека». Ці категорії достатньо глибоко розглядаються в сучасній літературі, що, дозволяє використовувати їх теоретичну основу при дослідженні змістовних характеристик поняття «інтелектуально-кадрова безпека» підприємства як окремого об'єкта управління. Однак, незважаючи на значний

інтерес вітчизняних та закордонних вчених і практиків до категорії «інтелектуально-кадрова безпека», це питання досі є маловивченим. Перш за все, це проявляється у тому, що переважна більшість науковців розглядає лише одну складову цієї категорії, а саме поняття «кадрова безпека». Натомість, тільки незначна частина дослідників переконана у необхідності використання комплексного поняття «інтелектуально-кадрова безпека» для всебічного аналізу його впливу на стан забезпечення фінансово-економічної безпеки підприємства.

Інтелектуально-кадрова безпека – це здатність підприємства запобігати ризикам і загрозам організації праці, безпосередньо персоналу, його трудовому та інтелектуальному потенціалу, трудовим відносинам в цілому.

До питань інтелектуально-кадрової безпеки належать:

− забезпечення підприємства необхідними працівниками;
− утримання працівників, їх розвиток;
− розробка мотиваційних схем і схем оплати праці;
− усунення збитку у зв'язку з трудовими суперечками;
− підвищення лояльності та відповідальності працівників;
− робота із сайтами вакансій та кадровими агентствами;
− аналіз ситуації на ринку праці в регіоні;
− оцінювання підприємства як працедавця (погляд з боку працівника);
− способи проектування кар'єри (також погляд з боку працівника).

Інтелектуально-кадрова безпека є комбінацією складових, пов'язаних між собою складними і часто завуальованими зв'язками:

1) Безпека життєдіяльності, яка включає:

– створення певних умов праці працівникам щодо запобігання травматизму, захворювання на підприємстві;

– виконання комплексу заходів, щодо недопущення порушень правил безпеки.

2) Соціально-мотиваційна безпека, яка включає:

– фінансову, грошово-кредитну платоспроможність працівників;

– оплату праці з урахуванням обсягу, кваліфікації, професіоналізму і якості виконаної роботи;

– професійно-кваліфікаційне та посадове просування працівників, заохочення в пристосуванні своєї кваліфікації до вимог робочого місця, в гарантіях виробничого зростання (планування кар'єри);

– підвищення особистої мобільності на ринку робочої сили; отримання шансів для самореалізації на робочому місці;

– проведення загальноосвітніх семінарів, конференцій, дискусій;

– мотивація задоволення персоналу своєю роботою;

– поліпшення власного іміджу кожного працівника;

– створення умов для відсутності можливості призначення непідготовлених і некомпетентних кадрів до керівництва

3) Професійна безпека, яка включає:

– систему принципів, підходів, дій направлених на створення певних умов праці (рівень оплати праці, посада, обладнання робочого місця), з урахуванням новітнього, передового досвіду на ринку праці;

– інформаційне забезпечення персоналу щодо прогнозування його структури, визначення потреби в кадрах, плануванні, залученні та розміщенні персоналу; оцінювання результатів праці для виявлення потенціалу кожного працівника;

– соціальний захист працівників (страхування, медичне обслуговування);

– впровадження новітніх технологій у розвиток персоналу, удосконаленні рівня професійних знань, навичок, умінь, здібностей у зв'язку з розвитком науково-технічного прогресу.

4) Антиконфліктна безпека, яка включає:

– створення психологічного клімату в колективі на основі позитивного відношення до підприємства, що характеризується психологічними показниками об’єднаності працівників, яка забезпечує узгодженість, безконфліктність спілкування, відповідальність та обов’язок, товариську допомогу, вимогливість до себе та іншого в інтересах виробництва;

– сприяння міжособистісним комунікаціям і створення сприятливого мікроклімату;

– врахування інтересів і побажань працівників, їх особистого потенціалу;

– сприяння задоволеності міжособистісними стосунками по вертикалі (керівник-підлеглі) та горизонталі (виконавці).

Інтелектуально-кадрова безпека підприємства побудована на трудових та етичних відносинах інтелектуального потенціалу, які забезпечують стабільну і прибуткову роботу підприємства, запобігаючи як внутрішнім, так і зовнішнім загрозам, що сприяє розвиткові людського та соціального потенціалу, підвищення рівня і якості життя населення, що притаманні цивілізованому суспільству.

8.2. Загрози інтелектуально-кадровій безпеці виробничого підприємства

Загрози інтелектуально-кадровій безпеці підприємства − існуючі або потенційні суперечності, що ускладнюють або унеможливлюють реалізацію пріоритетних інтересів за рахунок використання інтелектуально-кадрового ресурсу.

Зовнішні загрози інтелектуально-кадровій безпеці підприємства:

− інфляційні процеси, що впливають на доходи працівників;

− зовнішній тиск на працівників;

− переманювання працівників, що володіють конфіденційною інформацією, конкурентами;

− прямий підкуп працівників конкурентами;

− засилання агентів до конкурентів;

− помилкові пропозиції роботи працівникам конкурентів з метою вивідування інформації;

− кращі умови мотивації у конкурентів;

− несанкціонований доступ конкурентів до конфіденційної інформації (промислове шпигунство).

Внутрішні загрози інтелектуально-кадровій безпеці підприємства:

− недостатня кваліфікація працівників;

− невідповідність кваліфікації працівника займаній посаді;

− нецільове використання кваліфікованих працівників;

− слабка організація системи навчання;

− неефективна система мотивації;

− неякісні перевірки кандидатів під час прийому на роботу;

− відсутність або слабкість корпоративної політики;

− нездоровий соціально-психологічний клімат у колективі підприємства;

− психологічна схильність працівників до зловживання службовим становищем;

− неефективна організація системи управління персоналом;

− звільнення провідних висококваліфікованих працівників, що призводить до ослаблення інтелектуального потенціалу;

− зниження частки інженерно-технічних працівників і науковців у загальній чисельності працівників;

− зниження винахідницької та раціоналізаторської активності;

− зниження освітнього рівня працівників.

Вважаємо, що феномен загрози інтелектуально-кадровій безпеці підприємства, перш за все, слід розглядати через призму його персоналу, що виступає одночасно як суб'єктом, так і об'єктом впливу дестабілізуючих чинників. У цьому сенсі за відношенням до персоналу підприємства пропонуємо розрізняти такі види загроз:

1. Загрози по відношенню до персоналу підприємства – це загрози, джерелом яких є зовнішнє середовище, а об'єктом – персонал підприємства. До них слід віднести:

– промислове шпигунство (вид несумлінної конкуренції, діяльність щодо незаконного одержання інформації, що представляє собою комерційну цінність);

– хедхантінг (від англ. headhunting – «полювання за головами») – під яким розуміють прямий цілеспрямований пошук і переманювання керівників вищої ланки і кращих фахівців з вузького кола професіоналів;

– зазіхання на життя, здоров'я, волевиявлення, майно персоналу тощо.

2. Загрози з боку персоналу підприємства – це найбільш численний, не прогнозований та небезпечний з точки зору деструктивного впливу на реалізацію інтересів підприємства вид загроз, які зазвичай, виявляються у вигляді:

– афер з боку провідних спеціалістів (менеджерів і керівників середньої ланки, відповідальних за конкретний напрямок діяльності підприємства);

– фальсифікації готівки у касі і сум на банківських рахунках, підробці чеків підприємства;

– несанкціонованого продажу і використанні майна (власності) підприємства з корисливою метою;

– оплаті роботи фіктивних осіб;

– фальсифікації документації підприємства за допомогою електронної техніки й Інтернету (наприклад, перерахування засобів підприємства на свій особистий рахунок, внесення несанкціонованих змін у звітні документи);

– незаконних операціях з цінними паперами, матеріальними і нематеріальними активами підприємства;

– фальсифікації звітів про використання грошових коштів, виділених на відрядження, на інші потреби підприємства тощо.

Працівники організації можуть вдаватися до здійснення афер з різних мотивів, серед яких найпоширенішими вважаються:

1) особисті фінансові труднощі, неможливість задоволення життєвих потреб;

2) низька кваліфікація керівництва підприємства;

3) нездоровий діловий клімат у колективі підприємства (наявність «скривджених»);

4) психологічна готовність (схильність) працівника до зловживання службовим становищем;

5) порочні зв'язки, вчинки, захоплення;

6) слабкий кадровий менеджмент, неефективна персональна робота з кадрами.

З огляду на різноманітність зовнішніх і внутрішніх загроз, порушень з боку персоналу та широку мотиваційну сферу працівників, інтелектуально-кадрова безпека підприємства завжди повинна бути під пильною увагою керівництва. Саме тому для попередження загроз інтелектуально-кадровій безпеці необхідно планувати і організовувати заходи для її забезпечення в усіх напрямах кадрової політики організації.

Часто підприємства потерпають від зловживань з боку персоналу. Такими зловживаннями можуть бути *дрібні разові розкрадання*. Люди схильні іноді здійснювати дрібні крадіжки (наприклад, розкрадання товарів у магазинах самообслуговування). Такі крадіжки не є системними і не дають помітної економічної вигоди. Їх здійснюють швидше з пустощів у випадках, коли людина впевнена у своїй безкарності. До них бувають схильні люди незалежно від матеріального статку.

Крім дрібних разових крадіжок, існують *систематичні розкрадання середнього розміру*. Ця група розкрадань відрізняється від першої тим, що здійснюється з економічних мотивів, має систематичний характер, є продуманою і зазвичай забезпечується заходами безпеки. Такі розкрадання, на відміну від попередньої групи крадіжок, завдають значних збитків підприємству. Їх легко оцінити, підрахувавши суму зарплати працівників, посадова позиція яких допускає можливість розкрадань.

Найбільш небезпечний тип зловживань –«*внутрішнє підприємництво»*, що виникає там, де працівники можуть розпоряджатися значними сумами і самостійно ухвалювати важливі фінансові рішення. Формально працюючи на організацію, такі люди створюють на її основі внутрішній «приватний бізнес».

Тут ідеться вже не про «додаткову зарплату», а про привласнення великих сум грошових коштів. Цей тип зловживань поширений у:

а)владних структурах, де чиновники беруть хабарі за сприятливе для «клієнта» вирішення питань;

б) промислових підприємствах, де наймані керівники і працівники відділів постачання і збуту беруть «комісію» з постачальників і клієнтів (якщо продукція дефіцитна);

в) комерційних структурах, де окремі наймані працівники (зокрема, в торгівлі) здійснюють операції на значні суми, особисто спілкуються з клієнтами, мають доступ до готівки і можливість так чи інакше привласнювати частину цих сум.

Ознаки правопорушення в поведінці працівника і його неправомірні дії:

1) незвичне поводження працівника (нервозність, дратівливість, занепокоєння, перепади настрою, підозріла покірність тощо);

2) поява нестандартних даних і відхилення від звичайних (середніх) показників у бухгалтерських й/або інших документах;

3) зникнення окремих форм обліку та звітності (зокрема бланків) у бухгалтерській або іншій документації;

4) проведення сторонніх фінансових документів;

5) поява підроблених підписів і підчищень (виправлень) даних у звітній документації;

6) надання ксерокопій документів замість оригіналів;

7) різке поліпшення матеріальних можливостей працівника, не обґрунтоване його легальною діяльністю.

8.3. Показники оцінки інтелектуально-кадрової безпеки підприємства

Для оцінки рівня інтелектуально-кадрової безпеки, насамперед, необхідно сформувати систему показників (індикаторів), що дозволяють здійснювати діагностику її рівня, а також встановити їх порогові (критичні) значення. До таких показників належать:

1. Показники чисельного складу персоналу підприємства і їхню динаміку (середньооблікова чисельність персоналу підприємства, динаміка її зміни; плинність кадрів; віковий, соціальний і кваліфікаційний склад підприємства, показники стабільності та забезпеченості персоналу).

2. Показники ефективності використання персоналу підприємства (показники продуктивності праці, валового і чистого прибутку на одного працюючого, фондоозброєності праці).

3. Показники якості мотиваційної системи підприємства (показники середньої зарплати працівників підприємства в цілому і по професіях, показник матеріального заохочення персоналу, показник соціальної захищеності).

4. Показники рівня стану інтелектуального потенціалу підприємства (рівень освіти персоналу, кількість винаходів і пропозицій раціоналізаторського характеру на одного працівника, кількість патентів і одержуваних підприємством доходів від ліцензійної діяльності на одного працівника, показник інтелектуального рівня персоналу, а також абсолютні і питомі

значення отриманого підприємством ефекту від впровадження пропозицій його співробітників).

5. Показники ефективності прийнятих заходів для забезпечення інтелектуально-кадрової безпеки.

8.4. Методи забезпечення інтелектуально-кадрової безпеки підприємства

Заходи забезпечення інтелектуально-кадрової безпеки підприємства:

1. Підбір кандидатів на вакантні посади, передбачає такі заходи:

− перевірка анкетних та біографічних даних;

– перевірки попередньої діяльності кандидата для виявлення схильностей, що можуть завдати шкоди підприємству;

– перевірка даних з обліку МС, нарко- та психдиспансерів;

– перевірка документації щодо кваліфікації та акредитації кандидата;

– перевірка рекомендацій та відгуків попередніх роботодавців;

– спостереження за реакціями кандидата під час анкетування та інтерв'ю.

2. Робота з трудовим колективом передбачає:

− аналіз можливих загроз від діяльності персоналу, моніторинг внутрішніх загроз;

− вивчення лояльності і надійності персоналу;

− розробка документального забезпечення інтелектуально-кадрової безпеки;

− соціально-психологічне дослідження трудового колективу на предмет сумісності працівників і формування груп для вирішення поставлених задач;

− розробка професійної атестації персоналу, спрямованої на нейтралізацію ризиків, пов'язаних із професійною некомпетентністю працівників.

3. Службові розгляди у зв'язку з надзвичайними подіями:

− виявлення і вивчення ознак розкрадань, шахрайства, посадових зловживань персоналу;

− визначення кола підозрюваних у здійсненні службового порушення;

− встановлення осіб, що причетні до посадової правопорушення.

4. Планування звільнення працівників:

− розробка технології звільнення для конкретних посад;

− запобігання ймовірних ризиків, пов'заних зі звільненням персоналу (витік конфіденційної інформації, розкрадання баз даних тощо);

− розробка системи заходів, які повинні знизити психологічну напругу працівників, що звільняються.

Один із найважливіших методів запобігання загроз – вироблення у працівників лояльності та прихильності до підприємства.

Лояльність персоналу – це доброзичливе, коректне, щире ставлення до керівництва, працівників, інших осіб, їх дій, до підприємства в цілому; свідоме виконання працівниками своєї роботи відповідно до цілей і завдань в інтересах підприємства, а також дотримання норм, правил і зобов'язань відносно підприємства, керівництва, працівників та інших суб'єктів взаємодії.

Організаційна прихильність – це позитивна оцінка працівником свого перебування на підприємстві, намір діяти на благо цього підприємства заради його цілей та зберігати членство у ньому. Відсутність прихильності є фактором недостатнього, невмілого управління підприємством, чинником функціонування слабких соціальних технологій і виражається у відчуженні працівника від підприємства.

Основні методи профілактики правопорушень персоналу:

1. Висококваліфікований кадровий менеджмент, використання сучасних технологій, персональна робота з кадрами й управління поведінкою персоналу.
2. Здійснення зовнішнього й внутрішнього аудиту діяльності керівних кадрів, розподіл їхніх функцій.
3. Періодичне відновлення повноважень (анулювання доручень, переділ функціональних обов'язків тощо).
4. Доручення комерційних справ не одному фахівцеві, а декільком − на конкурентній основі.
5. Розробка й дотримання сучасних методів охорони власності (майна) підприємства, зокрема коштів, інформаційних комунікацій.
6. Обмежити доступ (допуск) працівників до документів фінансової та бухгалтерської звітності.

Для збереження інтелектуально-кадрової безпеки варто використовувати **сучасні HR-технології**:

– *рекрутинг* – пошук і набір персоналу. Цей процес може здійснюватися як у звичайному режимі, так і в різних агресивних формах, найпоширеніша серед яких «хед-хантінг». Ця форма набору персоналу полягає в переманюванні з інших компаній висококваліфікованих спеціалістів шляхом пропозиції їм набагато кращих умов оплати праці. Причому іноді ця міра застосовується не стільки для посилення власного кадрового потенціалу, скільки для завдання збитків конкурентові, а також з метою отримання цінного джерела інформації про його комерційні секрети;

– *тестування*, основним завданням якого на етапі співбесіди визначити професійні та моральні якості претендента та усунути сумнівних кандидатів;

– *навчання та тренінг* – процес підвищення кваліфікації персоналу, розширення й поліпшення функціональних і моральних якостей колективу. Як правило, працівники позитивно ставляться до проходження будь-яких тренінгів, вважаючи їх, з одного боку, певною розрядкою в монотонній роботі, а, з іншого – реальним засобом підвищення своєї кваліфікації, що поліпшує перспективи кар'єрного зростання;

– *ефективна мотивація*. Вона є тим чинником, що залучає та утримує персонал на підприємстві. Причому мотивація не зводиться тільки до грошової винагороди, хоча цей бік її є дуже важливий. Багато в чому мотивація залежить і від інших її елементів – престижності роботи, медичного обслуговування, охорони праці, психологічного клімату, корпоративної культури тощо;

– *прискорена адаптацію* (за рахунок наставництва) – повинна забезпечити гармонічне введення працівника в колектив, налагодження та полегшення функціональної комунікації;

– *своєчасне запобігання конфліктним ситуаціям*;

– *компенсація* – працівники зазнають стресу, фрустрації, професійних відхилень у психіці через специфіку їхньої діяльності. Емоційне й психологічне розвантаження працівників, компенсування всіх незручностей захистить підприємство від неадекватних дій персоналу. Для цього можна: створити кімнати відпочинку; створити затишну обстановку в робочих приміщеннях; організувати дозвілля; урізноманітнити роботу; звільняти від рутини; стежити за їхнім здоров'ям; ввести в штат психолога, який знає специфіку роботи, або запрошувати його зі спеціалізованих оганізацій для моніторингу ситуації за допомогою тренінгів.

– *вирішення особистих проблем працівника*. Іноді особисті проблеми прпрацівника перестають бути винятково його справою. Часто саме проблеми в родині або загроза близьким стає причиною нелояльності. Допомогти співробітникові можна тоді, коли керівник має на це моральне право, тобто коли працівник розуміє необхідність втручання у своє особисте життя. Для цього необхідно зробити хоча б кілька кроків: 1) створення атмосфери, що сприяє відкритому вирішенню всіх конфліктів; 2) боротьба з байдужістю як з боку колективу, так і з боку начальства; 3) залучення психолога, який займається проблемами співробітників; 4) культивування певних моральних цінностей, які допоможуть працівникам встановити для себе певні принципи поведінки;

– *розумна політика звільнення*. Людина повинна піти з почуттям, що її тут ніхто не кривдив, її радо зустрінуть як гостя. Не можна допускати погляду «ворога». Це бомба сповільненої дії. Є багато причин звільнення, 10–15 хвилин розмови керівника зі звільненим − і знешкоджено ще одну загрозу інтелектуально-кадровій безпеці підприємства.

– *пропаганда корпоративності*. Зміцненню корпоративного патріотизму службовців сприяють:

– знання історії створення й розвитку компанії;

– постійне нагадування про конкуренцію;

– інформація про результати діяльності компанії. Порівняння з конкурентами, як правило, є потужним імпульсом виховання лояльності;

– установлення «неформальних» відносин усередині колективу, нормальних міжособистісних відносин;

– *врахування думки колективу;*

– *моніторинг (контроль) колективу.*

8.5. Надійність персоналу: поняття, чинники та методи забезпечення

Надійність – одна з важливих складових професійної придатності працівників. Працівники, що володіють такою якістю, зберігають моральну стійкість і лояльність до компанії, в якій працюють, відчувають себе «прив'язаними» до неї, сама робота має для них високу мотиваційну значимість, а її втрата оцінюється як серйозна життєва невдача.

Якщо серед персоналу підприємства зустрічаються ненадійні працівники, то говорити про те, що це підприємство може бути успішним не можна.

Людський ресурс володіє одним істотним недоліком – він може втрачати при певних умовах надійність і ставати непотрібним і навіть небезпечним для інтересів підприємства.

Надійність персоналу (працівників) – властивість людини зберігати здатність здійснювати професійну діяльність у повному обсязі з необхідною якістю протягом необхідного проміжку часу, в тому числі в екстремальних ситуаціях.

Надійність персоналу складається з *професійної надійності*, *соціально-психологічної надійності* та *психофізіологічної* надійності.

Основні критерії надійності персоналу:

Освіта – повинна відповідати встановленим вимогам. Знання повинні відповідати диплому.

Здоров'я – повинні бути відображені будь-які фізичні, психологічні або розумові вади, які суттєво впливають на виконання прямих функціональних обов'язків.

Вживання наркотиків та спиртного – випадкове вживання, по святах в невеликих дозах або систематичне зловживання. В останньому випадку людина стає рабом поганої звички і за свої вчинки повністю відповідати не може.

Пристрасть до азартних ігор на гроші – регулярна участь в азартних іграх з великими ставками призводить до нестачі коштів і їх розкраданню для задоволення своєї пристрасті.

Стійкі звички – схильність міняти роботу, не розраховуючись з боргами, часті звільнення через некомпетентність.

Кримінальне минуле – звинувачення в кримінальних правопорушення та судово караних вчинках протягом останніх п'яти років.

Нерозкриті правопорушення – вчинені, але не розкриті злочини, придбання крадених товарів, приховування доходів, пред'явлення вимог про необґрунтовані страхові компенсації, зловмисне псування матеріальних цінностей, втеча з місця ДТП, приховування знайдених грошей, хоча їх власник відомий, анонімні дзвінки тощо.

Крадіжки на робочих місцях – крадіжки в недалекому минулому, підробка фінансових документів, отримання грошей за підробленими документами, очевидні нахили до розкрадань.

Фінансові аспекти – серйозні фінансові проступки, борги, приписки, судові розгляди, привласнення грошей.

Чинники, які визначають надійність працівників:

– професійна компетентність та дієздатність працівників – здатність нормально підготовленого працівника за відведений для роботи час успішно справлятися з поставленими завданнями без фізичних і психічних перевантажень;

– соціально-корпоративна зрілість працівника – збіг особистих цілей працівника з цілями організації, згоду працівника з системою винагороди за працю та системою санкцій за порушення виробничого процесу, готовність працівника діяти з необхідною для організації напруженістю;

– внутрішня цілісність і стійкість особистості – чесність, відкритість, порядність, доброзичливість.

Діагностика перерахованих чинників здійснюється в організаціях за допомогою різних опитувань, структурованих інтерв'ю, а також за допомогою методів прикладної психофізіології.

Психологічні чинники низької надійності персоналу:

1. Зневага і навіть презирство по відношенню до загальноприйнятих моральних норм. Людина вважає себе не зобов'язаною дотримуватися загальноприйнятих норм (не красти, не обманювати, не заподіювати зла людям, з якими вона разом живе і працює); вона ставиться до них із зневагою і цинізмом. Такий працівник не буде відчувати докорів сумління від того, що підводить або зраджує колег, організацію, в якій працює.

2. Індивідуалістична спрямованість особистості, невміння і небажання працювати в єдиній команді, стійке прагнення протиставити себе колегам, відсутність корпоративних почуттів, прихильності до місця роботи і колективу.

3. Завищена самооцінка, що не відповідає реальним можливостям людини, віра у власну безпомилковість, непомірне марнославство, незадоволені амбіції, заздрість. Істотну роль при цьому може грати незадоволеність кар'єрою, протиріччя між високими вимогами і реальним кар'єрним зростанням.

4. Риси характеру, що зумовлені психопатією і характеризуються мстивістю, злопам'ятністю, підвищеною уразливістю. Такі люди довго не можуть звільнитися від своїх негативних переживань, пробачити образу і зачеплене самолюбство. Їм зазвичай властива конфліктність з оточуючими (навмисне протиставлення себе іншим людям). Ці особи можуть переживати конфлікт протягом тривалого часу. Особливо небезпечний стійкий конфлікт «по вертикалі», коли працівник надовго зберігає бажання помститися за нанесені образи своєму керівникові.

5. Інфантилізм (особистісна незрілість), відсутність самостійності суджень, орієнтація на інших, більш сильних у психологічному відношенні людей, у прийнятті рішень і діях (легка добровільна підпорядкованість впливу з боку). Таким людям не вистачає самоорганізації. Вони не вміють планувати свій бюджет, своє життя, не здатні протистояти зовнішньому тиску і шантажу, проявляють лякливість, боягузтво. Ними легше управляти, їх легше втягнути у вчинення протиправних або аморальних дій і вчинків.

6. Імпульсивність, яка є домінуючою в поведінці. Вона проявляється у тому, що людину легко «завести», призвести до втрати самоконтролю і абсолютно необдуманих, безрозсудних дій. Такі люди нерідко бувають балакучими, їх легко розговорити з будь-яких питань, в тому числі і з тих, які становлять комерційну таємницю. Особливо часто у них»розв'язується мова» у неформальній обстановці, після прийняття алкоголю, при залученні в суперечку або полеміку та ін.

7. Невлаштованість в особистому житті, відчуженість від інших, самотність, «втрата коренів», відсутність близьких людей, зв'язку з ними. Така соціальна «відірваність» багато в чому полегшує вчинення ненормативних,

аморальних вчинків, оскільки людина вважає, що в разі «проколу» він один буде нести відповідальність, і страждати або переживати буде нікому.

8. Гостра ситуативна життєва потреба (наприклад, в дорогому лікуванні будь-кого з близьких), яку людина не може реалізувати самостійно. Даний фактор є найменш прогнозованим, а значить і найменш керованим. У той же час оперативне отримання повної і достовірної інформації про виникнення такої ситуації може знизити її негативний вплив на надійність працівника.

9. Наявність зв'язку даної людини з кимось із представників конкуруючих організацій. Це дуже небезпечний фактор, оскільки найбільш значний збиток в умовах жорсткої конкуренції можуть завдати саме ті, хто можуть бути спеціально впроваджені конкурентами в компанію для з'ясування інформації про стан справ у ній «зсередини» або використаний іншим чином завдяки родинним або іншим близьким зв'язкам.

Основна увага в забезпеченні інтелектуально-кадрової безпеки підприємства має бути зосереджена на попередженні, недопущення випадків порушення надійності персоналу або на створенні умов, при яких такі випадки були б зведені до мінімуму.

Напрями роботи, які сприяють підвищенню надійності та попередженню нелояльності працівників:

1. Проведення серйозного і всебічного відбору кадрів, при якому: не допускається прийняття на роботу осіб, які мають серйозні особисті недоліки; біографію, яка свідчить про наявність у них моральних дефектів; обов'язково встановлюється випробувальний термін для всіх найманих працівників. Наявність випробувального терміну дозволяє більш точно оцінити особисті та ділові якості співробітника, визначити його придатність до виконання тих завдань, які перед ним планується поставити. На жаль, життєвий досвід свідчить про те, що тільки в порівняно невеликій кількості організацій серйозно ставляться до застосування методів, за допомогою яких дана задача може бути успішно вирішена. Дуже часто тестування є формальним чи рішення про прийом на роботу приймається за іншими критеріями. Тому доцільно доповнити загальні умови такими заходами, як особисте поручительство працівників, за рекомендацією яких береться на роботу кандидат, отримання інформації з колишніх місць навчання або роботи, аналіз результатів його попередньої діяльності тощо.

2. Створення умов, при яких працівнику буде невигідно здійснювати дії, що завдають шкоди організації та її керівництву. Ці умови повинні включати цілу систему заходів з морального і матеріального стимулювання, формуванню престижності роботи саме в цій компанії, турботі про зовнішній та внутрішній імідж компанії, створенню в ній сприятливого соціально-психологічного клімату.

3. Формування корпоративного духу у працівників, тобто вживання заходів по створенню у них почуття належності до організації з тим, щоб вважати її «своєю», і в разі ускладнень звертатися за допомогою до компанії, а не шукати її на стороні.

4. Попередження ситуацій, при яких працівник або близькі йому люди можуть опинитися в безвихідному критичному положенні при виникненні гострих життєвих проблем. Профілактика таких ситуацій (зокрема, боргів, матеріальних труднощів) повинна здійснюватися шляхом кредитування працівників, створення каси взаємодопомоги та ін Працівники повинні бути впевнені в тому, що у разі виникнення у них матеріальних чи інших труднощів, організація прийде до них на допомогу. Потрібно також не допускати випадки байдужого ставлення до прохань та скарг кожного працівника, а при виникненні таких випадків – оперативно і жорстко реагувати на них.

5. Введення прогресивної системи матеріального та інших видів стимулювання, що додатково «прив'язують» працівника до організації, та які він не зможе отримати в конкуруючих організаціях. Така система може включати заохочення за сумлінну роботу, дотримання трудової дисципліни і лояльність компанії (вручення премій, цінних подарунків чи інших нагород, туристичних путівок тощо).

6. Забезпечення змішаного стилю керівництва. Це означає, що стиль роботи керівників будь-якого рангу в організації не повинен бути жорстко авторитарним, приводити до приниження гідності підлеглих з тим, щоб не провокувати зворотної негативної реакції.

7. Створення та зміцнення в компанії морально-психологічного клімату, що перешкоджає виникненню надзвичайних подій (тобто не допускає виникнення випадків порушення надійності), а також сприятливого для ефективної роботи кожного. Цьому сприяє, зокрема, організація колективних неформальних заходів, в яких працівники можуть спільно проводити час, брати участь у них сім'ями. Подібні заходи не тільки сприяють корпоративній згуртованості, але, певною мірою, дозволяють визначити відносини між працівниками та їх сім'ями.

8. Проведення періодичних атестацій працівників, за допомогою яких необхідно отримати об'єктивні відповіді на наступні питання:

– Чи хоче людина працювати в компанії?

– Чи може він працювати на тому рівні, який від нього вимагається?

– Наскільки він в змозі виконувати покладені на нього обов'язки?

– Чи справляється він зі своїми обов'язками?

– Як ставиться до своєї роботи?

– Чи задоволений він роботою?

– До категорії яких працівників можна його віднести (відмінних, гарних, посередніх, слабких)?

– Який рівень його амбіцій?

– Наскільки він вміє працювати в колективі?

– Чи здатний слідувати корпоративній культурі?

– Чи не є він джерелом постійних конфліктів, сварок, дрібних суперечок, що відволікають від основної роботи питань тощо.

9. Формування «командного духу», згуртованості. Вирішуючи це завдання, слід мати на увазі, що згуртованість персоналу не повинна означати кругової поруки, потурання, коли випадки явного відступу від прийнятих норм

замовчуються, працівники покривають порушення дисципліни їхніми колегами і не доводять ці випадки до відома керівництва. Керівник організації повинен бути проінформований про кожний такий випадок. Крім того, така поведінка має отримати відповідну суспільну оцінку. Між тим, дуже часто співробітники ставляться співчутливо до винуватця, вільно чи мимоволі ставлячи себе на його місце, у кращому випадку колектив виявляє байдужість до неналежної поведінки свого колеги. При такій суспільній реакції розраховувати на надійність персоналу не варто.

10. Взяття підписки про нерозголошення службової інформації і необхідність дотримання правил поведінки, що перешкоджають випадкам прояву ненадійності. В підписку обов'язково повинен включатися пункт про те, що у випадках прояву моральної ненадійності або виявлення фактів нелояльності, що завдають матеріальних збитків компанії або заподіюють шкоду її діловій репутації, її керівництво залишає за собою право притягнути працівника до відповідальності відповідно до чинного законодавства. Персонал повинен бути інформований про можливі наслідки в разі порушення конкретних норм встановленої дисципліни (догана, позбавлення премії, пониження в посаді, позбавлення певних пільг, попередження про звільнення, та ін.) У цьому ж документі повинен бути пункт про згоду працівника на можливі заходи по перевірці його надійності по відношенню до компанії. Для того, щоб довести нормальність такої перевірки керівництво організації повинне показати особистий приклад, взявши участь у цих заходах, з тим, щоб не викликати пересудів і вираження непотрібних образ з боку персоналу. Наприклад, у договір може вноситися пункт про добровільну згоду працівника на перевірку за допомогою приладу «Поліграф» у необхідних випадках.

11. Періодичне (щорічне або щоквартальне) нагадування працівникам про необхідність дотримання певних правил поведінки з відновленням відповідної підписки. Зазвичай такі заходи через свою формалізовану процедуру перетворюються в чисто номінальні. Тому, як керівнику організації, так і працівникам кадрової служби і служби безпеки варто задуматися над тим, щоб знизити формалізм у проведенні цих заходів і психологічно підняти їх значимість і дієвість.

12. Організаційні заходи, що сприяють збереженню комерційної та іншої службової таємниці. Кожен працівник повинен володіти тільки тією інформацією, яка необхідна йому для якісного та успішного виконання своїх обов'язків (і не більше). Прояв інтересу до відомостей, що виходять за рамки службової компетенції, не повинно залишатися без уваги колег. Про них слід негайно інформувати службу безпеки і керівництво організації.

13. Звільнення працівника за грубі порушення дисципліни і нелояльність – «розставання» має бути «мирним». Іноді воно навіть навмисно камуфлюється і представляється як вимушене. Можуть бути вжиті й інші доступні та прийнятні з точки зору закону заходи для того, щоб після відходу з компанії працівник не робив спроб помститися або заподіяти шкоду.

У разі нанесення компанії значного матеріального або морального збитку працівник (діючий або колишній) може бути притягнутий до відповідальності.

Програма надійності персоналу – це механізм реалізації комплексу організаційних, соціально-економічних, матеріально-технічних, морально-психологічних, медичних вимог і заходів, з метою досягнення і підтримки необхідного рівня надійності працівників.

Метою ПНП є забезпечення надійності працівників, за рахунок своєчасного виявлення факторів ризику, тобто тих обставин, які перешкоджають влаштуванню особи на роботу, призначенням на посаду або продовження виконання особою посадових (спеціальних) обов'язків.

Програма спрямована на зменшення внутрішньої загрози вчинення працівниками протиправних дій, за рахунок:

– підвищення якості проведення професійного відбору громадян, які влаштовуються на роботу;

– постійної і пильної оцінки мотивів професійної діяльності працівників;

– здійснення ефективного контролю за соціально-психологічними та психофізіологічними характеристиками працівників.

Реалізація програми надійності персоналу включає наступні етапи:

1-й етап – розробка науково-методичного апарату, який включає: розробку науково-методичних положень ПНП; розробку методичних (нормативних) документів з проведення соціально-психологічних і психофізіологічних обстежень працівників; розробку освітніх модулів з підготовки фахівців, які проводять соціально-психологічні та психофізіологічні обстеження працівників; розробку переліку необхідного обладнання для підготовки фахівців та проведення перевірок працівників. Іншими словами створення жорсткої та ефективної науково-обгрунтованої нормативної бази.

2-й етап – закупівля необхідного обладнання та оснащення їм навчальних класів для підготовки фахівців, які проводять соціально-психологічні та психофізіологічні обстеження працівників, а також спеціалізованих кабінетів для проведення обстежень працівників на об'єктах ПНП.

3-й етап – підготовка фахівців з ПНП, які проводять соціально-психологічні та психофізіологічні обстеження працівників.

4-й етап – реалізація заходів забезпечення надійності працівників.

5-й етап – аналіз ефективності ПНП та вдосконалення науково-методичного апарату. Перепідготовка фахівців, які проводять соціально-психологічні та психофізіологічні обстеження працівників.

Науково-методичні положення (основи) програми надійності персоналу є концептуальним документом, що відображає ідеологію ПНП і служать базою для розробки методичних (нормативних) документів та освітніх модулів по всім напрямкам діяльності ПНП.

Структурно науково-методичні положення включають:

1) призначення, цілі та завдання ПНП;

2) етапи реалізації ПНП;

3) види соціально-психологічних і психофізіологічних обстежень передбачені ПНП;

4) соціальні, психологічні та медичні вимоги, що пред'являються до працівників;

5) понятійний апарат у галузі забезпечення надійності працівників;

6) умови, що визначають необхідність залучення працівників до обстежень передбаченим ПНП;

7) працівників відносно, яких доцільно проводити обстеження передбачені ПНП;

8) структура органів управління з реалізації ПНП;

9) права, відповідальність і обов'язки посадових осіб групи по реалізації ПНП і груп ПНП структурних підрозділів;

10) функції групи з реалізації ПНП;

11) вимоги до підготовки фахівців, які здійснюють обстеження в рамках ПНП.

8.6. Мотивація персоналу в системі інтелектуально-кадрової безпеки підприємства

Мотивація – це процес спонукання й стимулювання окремої людини або групи людей до діяльності, до активності, до ініціативи. Вона необхідна для ефективної реалізації ухвалених рішень і для виконання окреслених робіт.

Методи мотивації в системі інтелектуально-кадрової безпеки:

– примушування;

– винагорода;

– солідарність (ототожнення);

– пристосування.

Примушування засноване на страху покарання та переживанні при цьому негативних емоцій. У матеріальній сфері примус пов'язаний зі штрафами, звільненнями, переведенням на іншу, низькооплачувану посаду або роботу. У соціально-психологічній сфері управління метод примусу найчастіше використовує форми, пов'язані зі страхом публічного приниження, образами та стресом. Людина, боячись бути ображеною чи турбуючись за своє здоров'я, стає покірною. Метод примушування веде не до узгодження цілей та інтересів організації та її працівників, а лише до посилення їх покірності. Але покірність – це не те, що потрібно для ефективності. Майже всі передові країни відмовляються від використання такого роду примусу. Однак американські та європейські компанії і зараз застосовують загрозу звільнення співробітників, у той час як Японія намагається не використовувати методів примусу.

Проте, коректне застосування методів примусу, характерних для адміністративних систем, заснованих на наказах і розпорядженнях, необхідне.

Винагорода може здійснюватися як у грошовій формі, так і у формі подарунка, додаткової відпустки, а також у нематеріальній формі – нагорода, подяка, популяризація працівника через публікацію матеріалів про нього у ЗМІ.

Метод солідарності (ототожнення) застосовується через переконання, виховання, навчання та створення сприятливого морально-психологічного клімату. Це дуже ефективний сучасний метод мотивації, в основі якого – знання соціальної психології, створення атмосфери єдиної команди, сімейного стилю менеджменту тощо.

Пристосування як метод мотивації найбільш застосовується менеджерами середнього і навіть верхнього рівнів управління. Цей метод дозволяє співробітникам впливати на цілі і завдання самої організації, пристосовуючи їх частково до своїх цілей. Ефективність даного методу полягає, перш за все, у тому, що у працівників, які здійснюють вплив на цілі і завдання організації, з'являється відчуття співвласника, співучасника, навіть стосовно найважливіших стратегічних питань існування організації або свого підрозділу. Цей метод супроводжується широким делегуванням повноважень, що сприяє полегшенню вибору цілей і завдань організації дедалі більшою кількістю співробітників.

Принципи мотивуючої організації праці, яка впливає на забезпечення інтелектуально-кадрової безпеки підприємства:

Принцип 1. ***Об'єднання завдань.***

Замість того, щоб розділяти завдання між кількома працівниками, вся робота (наприклад, виробництво певного продукту) може бути доручено одному працівнику. Це забезпечує більшу різноманітність навичок і велику закінченість (цілісність) завдання.

Принцип 2. ***Завершеність і цілісність робочих завдань.***

Можливість співробітника виконати від початку до кінця хоча б частину своїх робочих завдань. Наприклад, одній секретарці доручається надрукувати весь звіт, а не його частину. Така організація роботи підвищує ступінь її відповідальності, надає осмисленість і значимість виконуваної роботи.

Принцип 3. ***Встановлення відносин зі споживачами.***

Така організація роботи, коли працівник вступає в безпосередній контакт зі споживачем результатів його праці, послуг, не тільки допомагає забезпечити зворотний зв'язок, але вимагає від працівника більшої різноманітності професійних навичок, підвищуючи ступінь його самостійності. Наприклад, автомеханік, окрім ремонту машини, може і погоджувати умови ремонту з власниками машин, закуповувати чи замовляти необхідні деталі або комплектуючі.

Принцип 4. ***Делегування повноважень.***

Передача відповідальності і контролю над роботою від керівників до підлеглих посилює самостійність працівників, підвищує рівень їх трудової мотивації.

Принцип 5. ***Встановлення зворотного зв'язку.***

Існує багато типів зворотного зв'язку, який можуть отримувати працівники, і роботу слід організувати так, щоб надавати виконавцю якомога більше видів зворотного зв'язку. Чим більша кількість каналів зворотного зв'язку задіяна, тим більш точне уявлення будуть мати працівники про те, як вони працюють, і тим вищою буде їх мотивація до досягнення необхідних робочих показників, до поліпшення своєї роботи.

Принципи мотивації в практиці менеджменту безпеки персоналу:

Поводьтеся зі своїми підлеглими як з особистостями.

Більшість працівників цінують можливість висловити свої ідеї і вислухати думку про них з боку керівника. Це підвищує відчуття включеності

працівників у виконувану роботу, підвищує самоповагу і відчуття їх власної значущості.

Будьте щирі, хвалячи підлеглих. Нещира похвала відразу розпізнається й буде марною, а щира – може стати потужним засобом підвищення рівня мотивації підлеглого. Правило тут одне: будьте справедливі й відверті у похвалі та визнанні своїх підлеглих.

Залучайте підлеглих до активної участі у справах організації. Хороший керівник заохочує працівників до участі в постановці цілей і визначенні стандартів виконання роботи. Працівники, які беруть участь у постановці цілей або розробці програм удосконалення роботи, працюють більш напружено, прагнучи досягти успіху, тому що це ті програми, які вони допомагали розробляти.

Зробіть роботу цікавою. Часто робота є одноманітною і нудною, в результаті чого працівники втрачають інтерес до неї, хоча їх можуть влаштовувати умови роботи, стосунки з товаришами і власна організація. Тому слід виявляти нецікаві, монотонні обов'язки й урізноманітнювати їх. Можливі підходи – розширення, збагачення праці і делегування повноважень.

Заохочуйте працівників та групову роботу. В організаціях, де заохочуються дружні відносини, працівники з більшою готовністю співпрацюють один з одним. Це дозволяє створити і зміцнити командний дух і підвищити ефективність роботи підрозділу й організації в цілому.

Давайте працівникам можливість зростання. Проявляйте щиру зацікавленість щодо працівників, їх зростання та прогресу. Це може виражатися в тому, що працівникові буде доручена більш складна робота, він може бути скерований на навчання до інституту чи на курси підвищення кваліфікації; можна делегувати працівнику більше відповідальності за виконання певної роботи. Якщо працівник зростає професійно, він зазвичай має більш високу мотивацію і більше задоволений своєю роботою.

Встановлюйте реалістичні цілі для себе і для інших – досить складні, цікаві і реальні.

Давайте регулярний зворотний зв'язок: повідомляйте своїм підлеглим, як вони, на вашу думку, працюють, чого досягли і які проблеми їх очікують. Зворотній зв'язок підвищує мотивацію працівників для підвищення якості роботи.

Частіше спілкуйтеся зі своїми підлеглими, пояснюючи їм, що робиться і чому це має бути зроблено. Відкрите спілкування дозволяє посилити довіру і взаєморозуміння між керівником і підлеглими.

Підтримуйте своїх підлеглих, коли це необхідно. Таке ставлення підвищує рівень співпраці між працівниками і керівництвом, підсилює мотивацію до виконання виробничих завдань.

Переконайтеся в тому, що працівники розуміють, як їх робота пов'язана із задоволенням потреб і досягненням їхніх особистих цілей. Мотивація працівників підвищується, якщо вони бачать, як досягнення цілей підрозділу та організації допомагає їм у досягненні власних цілей.

Визначте заохочення, значимі для кожного підлеглого. Легше впливати на трудову мотивацію підлеглих, якщо ви знаєте, які з них більш привабливі для працівників.

Пов'яжіть заохочення з результатом. Мотивація працівників до досягнення поставлених цілей вища, якщо вони попередньо проінформовані про характер виконуваної роботи і її результат, який надасть можливість отримати винагороду.

Організації зазвичай отримують те, що вони заохочують. Система стимулювання повинна бути спроектована так, щоб ініціювати, викликати бажані види поведінки.

Не слід заохочувати всіх працівників однаково. Для того, щоб підкріплення поведінки було ефективним, заохочення повинні ґрунтуватися на результатах роботи. Однакове заохочення всіх працівників буде стимулювати середніх або поганих працівників та ігнорувати високу продуктивність кращих працівників.

Відсутність реакції теж може впливати на мотивацію підлеглих. Керівники впливають на своїх підлеглих як тим, що вони роблять, так і тим, чого вони не роблять. Наприклад, відсутність похвали щодо працівника, який відзначився, може призвести до того, що наступного разу він проявить менше завзяття для досягнення високого результату.

ТЕМА 9
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

9.1. Сутність інформації та інформаційної безпеки підприємства. Принципи інформаційної безпеки

9.2. Характеристика загроз інформаційній безпеці підприємства

9.3. Методи забезпечення інформаційної безпеки підприємства

9.1. Сутність інформації та інформаційної безпеки підприємства. Принципи інформаційної безпеки

Давно відомо, що інформація може бути справжнім скарбом. Саме тому часто багато зусиль витрачається як на охорону інформації, так і на добування її.

Інформація з погляду безпеки – це дані, відомості, документи, які повинні бути захищеними через їх важливість для суб'єкта господарювання від незаконного втручання, розкриття чи розголошення.

Основу правового статусу інформації визначає Закон України «Про інформацію». **Інформацію** у ст. 1 вищезазначеного Закону визначено як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформацію поділяють за такими видами, як:

– інформація про фізичну особу;
– інформація довідково-енциклопедичного характеру;
– інформація про стан довкілля (екологічна інформація);
– інформація про товар (роботу, послугу);
– науково-технічна інформація;
– податкова інформація;
– правова інформація;
– статистична інформація;
– соціологічна інформація тощо.

Основні характеристики інформації: цільове призначення, обсяг, цінність, повнота, надійність, вірогідність, надмірність, правдивість, доступність, швидкість передавання та переробки інформації.

Цільове призначення інформації – одна з найважливіших її характеристик, оскільки одна і та ж інформація часто використовується з різною метою. Наприклад, одні і ті ж дані можуть бути використані як для аналізу оперативної обстановки, так і для проведення оперативно-пошукових заходів.

Для передачі та обробки інформації важливого значення набуває її ***обсяг,*** який в простішому випадку залежить від кількості знаків (символів), що передаються.

Цінність інформації багато в чому визначається як своєчасністю її передачі, ступенем впливу на рішення, що приймається на її основі, так і

важливістю самого рішення. Цінність інформації залежить також від ряду інших характеристик інформації: повноти, надійності, вірогідності.

Така характеристика, як ***повнота*** використовується для визначення змісту найбільш істотних параметрів інформації, що передається. Інформація вважається повною, якщо вона відповідає необхідному обсягу. Невідповідність між інформацією, яка вимагається і яка здобута, свідчить або про неповноту, або про надлишок інформації.

За допомогою ***надійності*** характеризується наявність помилок в інформації, що передається. Надійність багато в чому залежить від технічних засобів, що використовуються.

Інформація може відповідати чи неповністю відповідати тому об'єктові, явищу чи процесу, який вона відображає. Для визначення ступеня відповідності використовують характеристику, яку називають ***вірогідністю***.

Правдивість надходження інформації визначається її вірогідністю, одноразовістю реєстрації, точністю передачі. Якщо інформація проходить три-чотири передавальних ланки, її правдивість знижується до 10% за рахунок старіння і викривлення.

Під ***надмірністю інформації*** розуміється збільшення обсягів даних, що передаються, але які не спричиняють одержання додаткових нових відомостей.

Доступність інформації міститься в тому, що вона знаходиться і накопичується в такому вигляді, що її можна було швидко і легко сприймати і використовувати в управлінні. Мова повідомлення повинна бути зрозумілою адресату, важливе значення має наочна інформація: графіки, планшети, світлове табло, слайди.

Остання характеристика – ***швидкість передавання та обробки інформації***. Вона залежить від швидкості технічних засобів та систем, що використовуються.

Залежно від способу передачі та сприйняття можна виділити такі види інформації:

– візуальна (передається і сприймається візуальними образами);
– аудіальна (звуками);
– тактильна (відчуттями);
– смакова (запахами);
– машинно-орієнтована (сприймається і обробляється ЕОМ).

За соціальною орієнтацією в науці виділяють масову, особисту і спеціальну інформацію. Якщо масова інформація адресується найширшому колові споживачів, то особиста орієнтована на точно визначеного індивідуума або певну групу осіб. Спеціальна інформація розрахована на спеціалістів. Вона може бути науковою або художньою, технічною або гуманітарною тощо. Спеціальну інформацію часто поділяють за сферами людської діяльності за галузевим принципом. Наприклад: машинобудівна, приладобудівна, енергетична, юридична, медична та ін.

Види інформації, які використовуються в управлінні, класифікуються за наступними ознаками :

– змістом – політична, директивна, правова, науково-технічна, економічна, планова, адміністративна, виробнича, бізнесова, нормативно-довідкова, обліково-бухгалтерська, статистична;

– напрямом руху – вхідна, вихідна;

– характером фіксації – фіксована, нефіксована;

– способом фіксації – документована, звукова, аудивізуальна;

– відношенням до суб'єкта управління – зовнішня, внутрішня;

– ступенем обробки – первинна, довільна, підсумкова;

– ступенем постійності – постійна, перемінна;

– форма надання – літерна, цифрова, кодована;

– можливості обробки – піддається і не піддається обробці;

– насиченості – достатня, недостатня, збиткова;

– правдивості – достовірна, недостовірна.

Політична інформація відображає політику держави щодо бізнесу, соціально-економічного розвитку, різних форм господарювання.

Директивну інформацію виробляють вищі органи, які визначають стратегію господарської діяльності менеджерів і яка слугує основою управління.

Правова інформація визначає статус кожного працівника, його посадове положення і за допомогою якої встановлюють норми господарського і адміністративного права, додержуються законності.

Науково-технічна інформація надає дані про досягнення науки і техніки, для ознайомлення з якою створюються в організаціях відділи або бюро.

Економічна інформація використовується для обґрунтування управлінських рішень і управління економічним розвитком організації. Вона включає розрахунки економічних показників, результати господарської діяльності, аналізу ринку, ціноутворення тощо.

Планова інформація представлена завданнями, технологічними картами, планами за періодами робіт, планами-нарядами тощо.

Адміністративна інформація призначена для оформлення ділових взаємовідносин між організаціями, громадянами і усунення недоліків; оформляється у вигляді наказів, розпоряджень, вказівок, положень.

Виробнича інформація містить оперативні відомості про техніку, технологію виконання планів виробництва і реалізації продукції.

Бізнесова інформація містить відомості про ринкові ціни та їх тенденції, рівень конкуренції, строки і об'єми надходження продукції, сервіс та рекламу, можливості комерційних операцій, підприємництво, комерційний ризик та ін.

Нормативно-довідкова інформація включає норми виробітку і обслуговування, тарифну систему оплати праці, розміри посадових окладів, довідкові дані про техніку, технологію, організацію праці.

Облікова-бухгалтерська інформація дозволяє контролювати хід виробництва і його результати, використання коштів, здобуття прибутку.

Статистична інформація представляє достовірні науково-обгрунтовані відомості, які дозволяють прийняти правильне рішення.

Інформація – умова ефективного здійснення підприємницької діяльності, вона використовується як засіб впливу на ринкову ситуацію, взаємовідносини суб'єктів, інформація має комерційну цінність і може виступати окремим видом економічної діяльності. Інформація є основою знань, тобто інтелектуального потенціалу підприємств, які необхідно захищати.

Інформаційна безпека підприємства – стан інформаційної роботи підприємства, за якого забезпечується ефективне інформаційне супроводження його діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на нього.

Інформаційна безпека підприємства – це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні.

Крім того, під інформаційною безпекою розуміють захищеність інформації та її підтримуючої інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі.

Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства в цілісності, захист і гарантування повноти і точності інформації, яку вона видає, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Основними принципами інформаційної безпеки є:

– забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;

– дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);

– доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;

– безперешкодний доступ до інформації в будь-який момент, коли вона буде необхідна.

Ці принципи неможливо реалізувати без особливої інтегрованої системи інформаційної безпеки, що виконує **наступні функції:**

– вироблення політики інформаційної безпеки;

– аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані);

– планування заходів щодо забезпечення інформаційної безпеки;

– планування дій в надзвичайних ситуаціях;

– вибір технічних засобів забезпечення інформаційної безпеки.

У практиці забезпечення інформаційної безпеки суттєве значення має визначення її видів. Особливо це необхідно з точки зору організації інформаційної безпеки в діяльності підприємств.

Види інформаційної безпеки підприємства:

– комп'ютерна безпека;

– інформаційно-психологічна безпека;

– комунікаційна безпека;

– документаційна безпека.

Комп'ютерна безпека передбачає: захист засобів комп'ютеризації, комп'ютерних технологій і інформації, що знаходиться на електронних носіях; отримання необхідної підприємству інформації із глобального інформаційного простору (мережі Інтернет) для формування його інформаційного ресурсу; протидія інформаційним загрозам в середовищі електронної інформації (комп'ютерні віруси, шкідливі програми, комп'ютерний тероризм тощо).

Інформаційно-психологічна безпека. Основними напрямами забезпечення інформаційної безпеки є організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин; збереження інформаційного здоров'я працівників суб'єктів підприємництва в умовах інформатизації виробництва; розробка технологій отримання знаннєвої інформації (наукові дослідження, конференції, семінари, курси, сімпозіуми і т. п.) для формування інформаційного ресурсу підприємства; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

Комунікаційна безпека включає захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок) та ділового спілкування (зустрічі, перемовини); проведення заходів пропаганди, контр-пропаганди та агітації в інформаційному середовищі підприємства; протидія поширенню негативної інформації засобами масової комунікації.

Документаційна безпека спрямована, перш за все, на захист документованої інформації та її носіїв, насамперед через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів з питань інформаційної безпеки; запровадження технологій отримання необхідних даних з різного роду документів (правових актів, звітів, звичайних публікацій, виступів, описів і т. п.) для формування інформаційного ресурсу суб'єктів підприємництва; документальне супроводження протидії інформаційним загрозам та інформаційно-психологічному впливу щодо суб'єктів підприємництва, їх діяльності та персоналу (документування фактів порушення інформаційного режиму, поширення неправдивої інформації чи маніпулювання нею, документальне спростування негативної інформації, документи щодо вимог відшкодування моральної шкоди і т. і.).

9.2.Характеристика загроз інформаційній безпеці підприємства

Інформаційний розвиток, що зумовив кардинальні зміни в економіці, праві, соціальному житті одночасно сприяв формуванню нових видів загроз у діяльності підприємств.

Забезпечення збереження інформації необхідно починати з визначення системи загроз, тобто негативних процесів, які сприяють витоку інформації. Для успішного захисту інформації необхідно знати весь перелік загроз безпеки. Якщо розробник має повний список загроз, то він зможе вибрати необхідні і застосувати потрібні для їх усунення засоби захисту.

В сучасному інформаційному середовищі існують два види загроз:

– інформаційні, які надходять від власне інформації та її технологій;

– загрози самій інформації, пов'язаних з різного роду посяганнями на інформацію та її об'єкти.

Отже, під **інформаційними загрозами** можна розуміти наявність в інформаційному середовищі шкідливої або небезпечної для його суб'єктів інформації, інформаційної продукції та технологій, здатних негативно впливати на їх стан, поведінку та взаємовідносини.

Загрози ж інформації – це дії, пов'язані з несанкціонованим доступом до об'єктів інформації або спрямовані на її викрадення, знищення, модифікацію, копіювання, блокування чи іншим чином позбавлення власника інформації переваг від її використання.

Інформаційні загрози:

– Загроза інформаційної залежності. Зауважимо, що загроза інформаційної залежності має подвійний характер. З одного боку це залежність від інформаційних технологій, а з іншого – залежність від постійно існуючої потреби в новій інформації. Залежність від інформаційних технологій проявляється у формуванні прихильності до різного роду інформаційних продуктів та способів їх подання в інформаційне середовище. Насамперед мова іде про продукти та технології засновані на комп'ютерній чи іншій електронній інформації. Першість тут тримають комп'ютерні ігри. Гра є одним із найбільш ефективних методик пізнання світу.

З розвитком інформаційних технологій з'явилась можливість перетворити гру в особливу, т. з. віртуальну реальність, яка усуває людину від реалій сьогодення. Віртуальна реальність та перебування в ній стає більш цікавим, захоплюючим чим існуюче життя.

Розвиток глобального інформаційного простору в останні роки, отримав тенденцію до інтеграції, можливості одночасного використання веб-платформ багатьма користувачами. Зазначені платформи дають змогу практично безмежного спілкування, перегляду новин, читання інформації, розважання (кіно, музика) і т. д. У наступному такі платформи з їх наповненням отримали назву соціальних мереж. Останні, як і комп'ютерні ігри володіють великим адекативним потенціалом і можуть загрожувати формуванням залежності від них. Залежність від перебування в соціальних мережах призводить до втрати продуктивного часу, зниження концентрації уваги на інформаційних повідомленнях, послаблення можливості приймати адекватні, зважені та обґрунтовані рішення. Крім того, наявність в соціальних мережах різних, зазвичай не повністю компетентних але переконливих точок зору, міркувань, коментарів може призводити до помилкових оцінок і рішень, якщо користувачі соціальних мереж будуть занадто «прив'язані» до них.

Сучасні комунікаційні мережі, побудовані на досягненнях інформаційного розвитку, також зумовило суттєву залежність від них. Насамперед мова іде про телефонну залежність, т. з. телефономанію, особливо з врахуванням сучасних можливостей мобільних засобів зв'язку.

– Наявні, практично безмежні обсяги необ'єктивної інформації, що наповнюють інформаційне середовище. Такими обсягами збагачується необхідна нам інформація, її досить складно не лише шукати, а і відрізняти від

об’єктивної. За таких умов події та явища, що відбуваються у процесі життєдіяльності, на ринку стають малозрозумілими, інформація про них може виявитись непридатною для прийняття рішень. Виконання ж роботи щодо більшої об’єктивності інформації потребує додаткового часу та фінансових витрат або моральної шкоди.

–Дискредитація суб’єктів (поширення негативної неправдивої інформації про суб’єктів, маніпулювання індивідуальною та колективною свідомістю працівників, клієнтів, акціонерів, споживачів або просто громадян, дезінформація різних осіб у взаємовідносинах з суб’єктами, поширення негативних чуток про останніх, здійснення актів інформаційного тероризму та провокування інформаційних конфліктів, втягування суб’єктів в інформаційну війну).

– Промислове шпигунство, яке охоплює практично всі складові ринкової економіки. Промислове шпигунство передбачає отримання інформації, яка тим чи іншим чином характеризує відповідні технології, плани, розробки, ідеї, рішення, що є цікавими для конкурентів. Не обов’язково, щоб інформація була таємною або конфіденційною, головне, щоб вона була корисною для конкурента або іншого суб’єкта.

– Кібертероризм. Особлива небезпечність кібертероризму полягає в тому, що він одночасно несе в собі загрозу інформаційним ресурсам суб’єктів підприємництва і загрозу їх іміджу, суспільній оцінці їх діяльності.

Враховуючи, що сучасна діяльність суб’єктів підприємництва значною мірою перебуває в інформаційній площині, вони завжди перебувають у полі різного роду небезпек і загроз, тобто є об’єктами інформаційних загроз і впливу інформаційних ризиків.

Основні загрози інформації і нормального функціонування інформаційної системи:

– розголошення інформації;
– просочування конфіденційної інформації;
– викрадення інформації;
– знищення інформації;
– модифікація інформації;
– несанкціоноване використання інформаційних ресурсів;
– помилкове використання інформаційних ресурсів;
– відмова від інформації;
– порушення інформаційного обслуговування.

Розголошення інформації розуміється як протиправні умисні чи необережні дії посадових або інших осіб, які призвели до несанкціонованого, без службової необхідності, оголошення (поширення) відомостей щодо яких встановлено відповідний порядок їх розкриття. Воно може здійснюватись шляхом повідомлення, передачі, пересилання, публікації, втрати чи іншим шляхом оприлюднення зазначених відомостей.

Просочування конфіденційної інформації – це її безконтрольний вихід за межі інформаційної системи або через коло осіб, яким вона була довірена за

видом служби або стала відома в процесі роботи. Цей витік може бути наслідком:

– розголошування конфіденційної інформації;

– витоку інформації різними, переважно технічними каналами;

– несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошування інформації, що призвело до ознайомлення з нею осіб, не допущених до цих відомостей, можна кваліфікувати як умисні або необережні дії посадових осіб і користувачів, яким ці відомості були довірені у зв'язку зі службовою потребою.

Можливий безконтрольний витік конфіденційної інформації візуально-оптичним, акустичним, електромагнітним та іншими каналами.

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, яка не має права доступу до відомостей, що охороняються. Найпоширенішими напрямами несанкціонованого доступу до інформації є:

– перехоплення електронних випромінювань;

– примусове електромагнітне опромінювання (підсвічування) ліній зв'язку з метою отримання паразитної модуляції;

– застосування підслуховуючих пристроїв (жучків);

– дистанційне фотографування;

– перехоплення акустичних випромінювань і відновлення тексту принтера;

– зчитування залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

– копіювання носіїв інформації з подоланням заходів захисту;

– маскування під зареєстрованого користувача;

– маскування під запити системи;

– використання програмних пасток;

– використання недоліків мов програмування і операційних систем;

– незаконне підключення до апаратури і ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ інформації;

– зловмисне виведення з ладу механізмів захисту;

– розшифровування спеціальними програмами зашифрованої інформації.

Викраденням інформації є таємне вилучення носіїв інформації (документів, електронних носіїв, відео- та аудиозаписів) з метою подальшого їх використання іншою особою чи передачі їх такій особі.

Знищенням є приведення носіїв інформації (документів, електронних носіїв, аудіо-, відеозаписів та інших носіїв, що мають матеріальний характер) в стан непридатний для їх подальшого використання або ж неможливості використання інформації, яка на них зберігалась.

Модифікацією інформації є внесення змін до змісту інформації, яка містилась на певних носіях або ж до самих носіїв (комп'ютерних програм) в результаті чого використання даної інформації стає неможливим взагалі чи така інформація вимагає суттєвого уточнення та аналізу.

Незаконне використання інформації означає використання певних даних, знань, технологій, які на праві власності належать певній юридичній чи фізичній особі без її згоди або з порушенням встановленого порядку їх використання особами, яким така інформація відома у зв'язку з їх службовою чи іншою діяльністю.

Несанкціонованим буде також доступ до інформації з порушенням встановлених правил доступу до неї.

Помилкове використання інформаційних ресурсів може призвести до знищення, розкриття або компрометації цих ресурсів. Така загроза є переважно наслідком помилок програмного забезпечення інформаційної системи.

Відмова від інформації полягає у невизнанні адресатом чи відправником цієї інформації, фактів її отримання або відправки.

Порушення інформаційного обслуговування полягає у затримці надання ресурсів абонентові, що може призвести до тяжких наслідків. Наприклад, відсутність в абонента даних, необхідних для прийняття рішень, може бути причиною його нераціональних або неоптимальних дій.

Існує безліч класифікацій видів загроз за принципами і характером їх дії на систему, щодо використовуваних засобів, за цілями атаки тощо.

Загрози інформаційній безпеці поділяються на **випадкові і навмисні**.

Джерелом **випадкових** можуть бути аварійні ситуації через стихійні лиха і відключення електроживлення, відмови і збої апаратури, помилки в програмному забезпеченні, помилки в роботі обслуговуючого персоналу і користувачів, перешкоди в лініях зв'язку через впливи зовнішнього середовища.

Навмисні загрози пов'язані з цілеспрямованими діями порушника, яким можуть виступати службовці, відвідувачі, конкуренти, працівники.

Навмисні загрози в свою чергу поділяються на **пасивні і активні**.

Пасивні загрози носять характер перехоплення або моніторингу переданої інформації і не пов'язані з якою-небудь зміною інформації. Їх можна умовно розділити на дві групи: розкриття вмісту повідомлення (телефонна розмова, електронна пошта) і аналіз потоку даних.

Пасивні порушення виявити дуже важко, але їх цілком реально попередити. **Активні** загрози пов'язані зі зміною потоку даних або зі створенням фальшивих потоків

Класифікація загроз інформаційній безпеці за засобами впливу на систему.

За засобами впливу розрізняють три основні класи загроз:

1. Втручання людини в роботу обчислювальної системи. До цього класу належать організаційні засоби порушення безпеки (крадіжка носіїв інформації, несанкціонований доступ до пристроїв зберігання і обробки інформації, псування устаткування тощо.) І здійснення порушником несанкціонованого доступу до програмних компонентів системи (всі способи несанкціонованого проникнення в систему, а також способи отримання користувачем-порушником незаконних прав доступу). Заходи, що протистоять таким загрозам, носять організаційний характер, а також включають в себе

вдосконалення систем розмежування доступу і системи виявлення спроб атак (наприклад, спроб підбору паролів).

2. Апаратурно-технічне втручання в роботу обчислювальної системи. Мається на увазі порушення безпеки та цілісності інформації за допомогою технічних засобів, наприклад, отримання інформації по електромагнітному випромінюванні пристроїв, електромагнітні впливи на канали передачі інформації та інші методи. Захист від таких загроз, крім організаційних заходів, передбачає відповідні апаратні і програмні заходи.

3. Руйнівний вплив на програмні компоненти системи за допомогою програмних засобів. Такі засоби називаються руйнівними програмним засобами (РПС). До них відносяться комп'ютерні віруси, троянські коні, засоби проникнення у віддалені системи з використанням локальних і глобальних мереж. Засоби боротьби з подібними атаками складаються з програмно-і (рідше) апаратно-реалізованих систем захисту.

Загрози інформаційній безпеці поділяються на внутрішні і зовнішні.

Внутрішні загрози інформаційній безпеці:

– некваліфікована політика щодо організації інформаційних технологій та управління безпекою підприємства;

– відсутність належної кваліфікації персоналу;

– навмисні і ненавмисні дії персоналу, що призводять до порушення інформаційної безпеки;

– техногенні аварії, пожежі тощо.

Внутрішні суб'єкти (джерела), як правило, представлені висококваліфікованими фахівцями у сфері розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі. До них відносяться:

– основний персонал (користувачі, програмісти, розробники);

– представники служби захисту інформації;

– допоміжний персонал (прибиральники, охорона);

– технічний персонал.

***Зовнішні загрози інформаційній безпеці*:**

– негативні дії недобросовісних конкурентів і державних структур;

– навмисні і ненавмисні дії зацікавлених структур і фізичних осіб (збір інформації, шантаж, погрози фізичного впливу тощо);

– витік конфіденційної інформації із носіїв інформації та каналів зв'язку;

– несанкціоноване проникнення на об'єкт захисту;

– несанкціонований доступ до носіїв інформації і каналів зв'язку з метою знищення, викривлення, викрадення, блокування інформації;

– стихійні лиха та інші форс-мажорні обставини;

– навмисні і ненавмисні дії постачальників послуг в сфері забезпечення безпеки, постачальників програмних продуктів тощо.

Джерела зовнішніх загроз можуть бути випадковими і запланованими та мати різний рівень кваліфікації. До них відносяться:

– кримінальні структури;

– потенційні злочинці і хакери;

– нечесні партнери;

– технічний персонал постачальників послуг тощо.

9.3. Методи забезпечення інформаційної безпеки підприємства

Для запобігання загрозам інформаційній безпеці та їх усунення використовують правові, програмно-технічні та організаційно-економічні методи.

Правові методи передбачають розроблення комплексу нормативно-правових актів і положень, що регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо гарантування інформаційної безпеки.

Програмно-технічні методи передбачають:

– запобігання витоку інформації;

– усунення можливості несанкціонованого доступу до інформації;

– запобігання впливам, які призводять до знищення, руйнування, переключення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;

– виявлення вмонтованих пристроїв;

– запобігання перехопленню інформації технічними засобами;

– використання криптографічних засобів захисту інформації під час передачі каналами зв’язку.

Організаційно-економічні методи передбачають:

– формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації;

– сертифікацію цих систем відповідно до вимог інформаційної безпеки;

– ліцензування діяльності у сфері інформаційної безпеки;

– стандартизацію способів і засобів захисту інформації;

– контроль за діями персоналу в захищених інформаційних системах.

Крім цих груп методів використовують ще й такі **методи забезпечення інформаційної безпеки:**

– ідентифікація та аутентифікації користувачів (так званий комплекс 3А);

– шифрування інформації, що зберігається на комп’ютерах і передається по мережах;

– міжмережеві екрани;

– віртуальні приватні мережі;

– засоби контентної фільтрації;

– інструменти перевірки цілісності вмісту дисків;

– протидія атакам шкідливих програм;

– системи виявлення вразливостей мереж і аналізатори мережевих атак;

– перешкода;

– регламентація;

– примус;

– спонука;

– мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу.

Кожен з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими.

«Комплекс ЗА» включає аутентифікацію (або ідентифікацію), авторизацію та адміністрування. Ідентифікація та авторизація – це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі?. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

Шифрування – криптографічне закриття інформації. Системи шифрування дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачу з мережних протоколах. Завдання цього засобу захисту – забезпечення конфіденційності. Основні вимоги, що пред'являються до систем шифрування – високий рівень криптостійкості та легальність використання на території держави.

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома чи більш мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів – перевірка кожного пакету даних на відповідність вхідної та вихідної IP адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркулюванням даних.

Говорячи про криптографію і міжмережеві екрані, слід згадати про захищені **віртуальні приватні мережі** (Virtual Private Network – VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам. Використання VPN можна звести до вирішення трьох основних завдань:

1. Захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу).
2. Захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через Internet.
3. Захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

Ефективний засіб захисту від втрати конфіденційної інформації – фільтрація вмісту вхідної і вихідної електронної пошти. Перевірка поштових повідомлень на основі правил, встановлених в організації, дозволяє також

забезпечити безпеку компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму.

Засоби контентної фільтрації дозволяють перевіряти файли всіх розповсюджених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки **технології перевірки цілісності вмісту жорсткого диска** (integrity checking). Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об'єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linux-системи, Novell) на процесорах різних типів.

Фільтри спаму значно зменшують невиробничі затрати праці, пов'язані з розглядом спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не включені до бази антивірусних програм) часто мають ознаки спаму і фільтруються.

Перешкода – метод фізичного втручання на шляху зловмисника до захищеної інформації (до документів, апаратури, носіїв інформації тощо).

Регламентація – створення таких умов автоматизованого опрацювання, зберігання і передавання інформації, що піддягає захисту, за яких норми і стандарти захисту найбільш ефективні.

Примус – метод захисту, за якого користувачі і персонал ІС змушені дотримуватися правил опрацювання, передавання і використання конфіденційної інформації через загрозу матеріальної, адміністративної або кримінальної відповідальності.

Спонука – метод захисту, що спонукає користувачів і персонал ІС не порушувати встановлених порядків за рахунок дотримання моральних і етичних норм, що склалися.

Для протидії природним загрозам інформаційної безпеки в компанії має бути розроблений і реалізований набір процедур щодо запобігання надзвичайних ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних – резервне

копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій тощо).

Існують такі засоби забезпечення інформаційної безпеки:

– технічні, які поділяють на апаратні та фізичні;
– програмні;
– організаційні;
– правові;
– морально-етичні.

Апаратні засоби – пристрої, які вбудовують безпосередньо в обчислювальну техніку або пристрої, які з'єднують із нею за стандартним інтерфейсом.

Фізичні засоби – це різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту і здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій (замки на дверях, фати на вікнах, засоби електронної охоронної сигналізації).

Програмні засоби – спеціальні програми і програмні комплекси, призначені для захисту інформації в ІС.

Організаційні засоби здійснюють регламентацію виробничої діяльності в ІС і взаємин виконавців на нормативно-правовій основі так, що розголошування, витік і несанкціонований доступ до конфіденційної інформації стають неможливими або досить складними за рахунок проведення організаційних заходів. Комплекс цих заходів реалізує група інформаційної безпеки, але має бути під контролем першого керівника.

Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, опрацювання і передавання інформації обмеженого доступу і встановлюють заходи відповідальності за порушення цих правил.

Морально-етичні засоби захисту – різні норми поведінки, які традиційно склалися раніше, формуються у спосіб розповсюдження ІС і ІТ в країні і світі або спеціально розробляються. Вони можуть бути неписані (чесність) або оформлені в якесь зведення (статут) правил чи розпоряджень. Ці норми зазвичай не є законодавчо затвердженими, але оскільки їх недотримання призводить до падіння престижу організації, вони вважаються обов'язковими для виконання. Характерним прикладом таких розпоряджень є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США, Кодекс честі аудиторів.

ТЕМА 10
КОМЕРЦІЙНА ТАЄМНИЦЯ ТА ОСОБЛИВОСТІ ЇЇ ДОТРИМАННЯ НА ПІДПРИЄМСТВІ

10.1. Розвиток, значення та сутність комерційної таємниці
10.2. Організація захисту комерційної таємниці на підприємстві
10.3. Право інтелектуальної власності на комерційну таємницю
10.4. Відповідальність за незаконні дії щодо комерційної таємниці на підприємстві

10.1. Розвиток, значення та сутність комерційної таємниці

Комерційну таємницю вважають одним із найдавніших способів охорони результатів інтелектуальної діяльності. Вона існує з давніх часів, ще до появи відповідних правових норм, коли майстри ретельно зберігали свої професійні секрети, передаючи їх з покоління у покоління. У Стародавньому Римі була вже запроваджена правова охорона комерційної інформації, за порушення якої передбачалася система штрафів, зокрема подвійний штраф за примушення рабів розкривати секрети професійної діяльності їх власників.

Сучасне розуміння комерційної таємниці сформувалося в період промислової революції в Англії. Перше судове рішення щодо захисту комерційної таємниці в США було винесене і документально оформлене у 1837 році.

В Росії у період правління царя Олександра II для захисту підприємців від недобросовісної конкуренції були вперше впроваджені правові норми щодо захисту “промислової таємниці”. У 1917 р. радянська влада прийняла Декрет “Про робітничий контроль”, який унеможливлював існування комерційної таємниці. Був прийнятий політичний курс на обов’язкове безоплатне розповсюдження досягнень, обмін досвідом кожного підприємства. Тільки у 90-х роках минулого століття у Законі СРСР «Про підприємства в СРСР» (№ 1529-1 від 04.06.1990) знову було законодавчо визначено термін «комерційна таємниця підприємства», а також склад, обсяг відомостей, що становлять цю таємницю, порядок їх захисту тощо.

В Україні регулювання комерційної таємниці здійснюється з 1991 р. положеннями Закону УРСР «Про підприємства в Українській СРСР», з 1992 р. – Закону України «Про підприємства в Україні», які були аналогічні вищеназваному Закону СРСР. З 1 січня 2004 р. набув чинності Господарський кодекс України, Цивільний кодекс України, де комерційній таємниці присвячене надзвичайно важливе місце.

Нині в умовах глобалізації економіки захист комерційної таємниці має надзвичайно велике значення. Так, за даними Комісії Конгресу США з міжнародної торгівлі, щорічні втрати американських компаній через недобросовісну конкуренцію іноземних компаній, у тому числі через промислове шпигунство сягають понад 70 млрд дол. США.

Тому виробники вживають всілякі заходи для захисту своїх комерційних таємниць. Наприклад, всесвітньо відома компанія «Coca-Cola», яка успішно

працювала в Індії протягом 25 років, маючи більше 550 млн потенційних споживачів, у 1997 р. з великими втратами припинила свій бізнес у цій країні для того, щоб зберегти таємницю рецептів приготування напоїв, яка зберігається вже більше ста років. Підставою для такого непростого рішення стало прийняття Індією закону, який зобов'язував іноземні компанії передати їх власні технологи індійським підприємствам. Зокрема, від компанії «Coca-Cola» вимагалося передати 60% акцій індійській дочірній компанії і розкрити свою технологію. Інакше їй пропонувалося припинити свою діяльність на території Індії.

Згідно зі ст. 505 ЦК України **комерційною таємницею** є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою і не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть належати до комерційної таємниці.

Отже, **комерційна таємниця** – це відомості технічного, організаційного, комерційного, виробничого та іншого характеру, які є об'єктом інтелектуальної власності, мають комерційну цінність, розголошення яких може завдати шкоди інтересам суб'єкта господарювання.

Відомості, що належать до комерційної таємниці, мають містити такі **ознаки:**

– не підпадають під державну таємницю;

– стосуються виробничої діяльності підприємства;

– не спричиняють збитків інтересам суспільства;

– мають дійсну або потенційну комерційну цінність і створюють переваги у конкурентній боротьбі;

– мають обмеження у доступі, що встановлюються керівництвом підприємства;

– щодо них на підприємстві вживаються заходи щодо їх охорони.

Отже, підприємство може вважати комерційною таємницею практично будь-яку інформацію про свою діяльність та свій персонал і самостійно організовувати її захист.

Усі види інформації, які можуть вважатися комерційною таємницею, можна умовно поділити на дві групи:

1) науково-технічна (технологічна) інформація;

2) ділова (комерційна) інформація.

До першої групи належать незапатентовані науково-технічні розробки, бази даних та інші комп'ютерні програми, створені підприємством, усі види «ноу-хау», технічні проекти, промислові зразки, незапатентовані товарні знаки тощо.

Ділова інформація містить:

– відомості про фінансову сторону діяльності підприємства, крім фінансових звітів (стан розрахунків з клієнтами, заборгованість, кредити та ін.);

– відомості про розмір прибутку, собівартості виробленої продукції та ін.;

– плани розвитку підприємства (тактичні і стратегічні);

– плани й обсяги реалізацій продукції (плани маркетингу, дані про характер і обсяг торгових операцій, про рівні цін, наявність то варів);

– аналіз конкурентоспроможності виробленої продукції, ефективність експорту та імпорту, прогнозований час виходу на ринок;

– плани рекламної діяльності;

– списки торгових та інших клієнтів, представників, посередників, конкурентів, відомості про взаємовідносини з ними, їх фінансове положення, проведені операції, умови діючих і нових контрактів та ін.

Інформація підприємства, що становить комерційну таємницю, за важливістю може належати до чотирьох рівнів:

1. Життєво важлива – незамінна інформація, наявність якої стратегічно необхідна для функціонування підприємства. Витік цієї інформації ставить під загрозу функціонування підприємства.

2. Важлива – інформація, процес ліквідації наслідків витоку якої складний або пов'язаний з великими витратами.

3. Корисна – інформація, витік якої завдає матеріальної шкоди підприємству, однак воно може ефективно функціонувати й у разі витоку цієї інформації.

4. Неістотна – інформація, витік якої не завдає матеріального збитку підприємству і не впливає на його функціонування.

Уся ця інформація має різну цінність для підприємця, і розголошування її може призвести (або не призвести) до загроз економічній безпеці різного ступеня важкості. Тому інформацію доцільно поділяти на три групи:

а) інформація для відкритого користування будь-яким споживачем у будь-якій формі;

б) інформація обмеженого доступу – тільки для органів, що мають відповідні законодавчо встановлені права (податкова поліція, прокуратура);

в) інформація тільки для працівників (або керівників) підприємства. Інформація, що належить до другої і третьої груп, є конфіденційною і має обмеження у розповсюдженні.

Такий вид таємниці як комерційна стосується лише суб'єктів господарювання: юридичних осіб та фізичних осіб зареєстрованих як суб'єкти підприємницької діяльності. Право власності на такий вид інформації вони отримують через створення її власними силами та засобами або іншими особами на договірних засадах з суб'єктами господарювання за їх кошти і на їх користь, придбанням такої інформації у інших осіб.

Окремо регулюється порядок захисту комерційної таємниці суб'єктів господарювання у їх конкурентних відносинах. Так, відповідно до гл. 4 Закону України «Про захист від недобросовісної конкуренції»:

– неправомірним визнається збирання протиправним способом відомостей, що становлять комерційну таємницю за умов коли це завдало чи могло завдати шкоди суб'єкту господарювання;

– неправомірним визнається впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу уповноваженої на те особи (неправомірне використання) відомостей, що становлять комерційну таємницю;

– неправомірним визнається розголошення комерційної таємниці, тобто ознайомлення іншої особи без дозволу особи, уповноваженої на те, з відомостями, що відповідно до законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням відповідних обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання;

– неправомірним вважається схилення до розголошення комерційної таємниці, тобто спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням відповідних обов'язків відомості, що відповідно до законодавства України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

Такі дії суперечать нормам чинного законодавства і переслідуються у кримінальному, адміністративному чи цивільному (відшкодування шкоди) порядку.

10.2. Організація захисту комерційної таємниці на підприємстві

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві створюється спеціальна комісія, яка займається групуванням і уточненням інформації для цього переліку. Чисельність такої комісії не повинна перевищувати чотирьох-п'яти осіб.

При оформленні переліку відомостей, що становлять комерційну таємницю, у своїй діяльності комісія має керуватися наступним:

– якщо підприємство має у своєму розпорядженні інформацію, яка належить до державної таємниці, її слід виділити в окрему позицію, оскільки цей вид інформації охороняється законодавством України про державну таємницю;

– в окрему позицію також слід виділити ту інформацію, яка не є комерційною таємницею згідно з Постановою № 611;

– обов'язково до комерційної таємниці мають бути віднесені різні види «ноу-хау»; різні договори також повинні вважатися комерційною таємницею, причому як сам текст договору, так і факт їх укладення; мають бути віднесені до комерційної таємниці й відомості про винаходи і рацпропозиції, які не захищені авторським або патентним правом.

Крім затвердження такого переліку на керівника підприємства покладається також обов'язок щодо встановлення порядку захисту комерційної таємниці. Серед методів такого захисту можна виділити:

– розробку положення про комерційну таємницю на підприємстві;

– розробку інструкцій щодо дотримання працівниками режиму нерозголошення комерційної таємниці;

– включення до статуту підприємства розділів, які регламентують захист комерційної таємниці;

– розробку угоди про нерозголошення комерційної таємниці, що укладається з особами, які мають доступ до цієї інформації.

Перед тим як взяти з працівників підписку про нерозголошення відомостей, що становлять комерційну таємницю, керівництву підприємства необхідно здійснити певні процедури:

– видати наказ по підприємству про встановлення комерційної таємниці;

– затвердити перелік відомостей, що становлять комерційну таємницю;

– затвердити форму зобов'язання (договору) про нерозголошення інформації, що є комерційною таємницею;

Незалежно від обраного підприємством шляху захисту комерційної таємниці працівник, приступаючи до виконання своїх обов'язків, має бути поінформований:

– про порядок і процедуру набуття матеріалами, документами та виробами статусу комерційної таємниці підприємця;

– про правила, пов'язані з доступом до інформації, що є комерційною таємницею;

– про обов'язки й обмеження, що покладаються на виконавців, допущених до відомостей конфіденційного характеру (наприклад, діловодство, облік, збереження, розмноження, обробка інформації тощо);

– про порядок прийому представників інших суб'єктів підприємницької діяльності та передачі їм інформації;

– про відповідальність за розголошення відомостей, що складають комерційну таємницю підприємства, або за порушення встановленого порядку роботи з ними.

Органи державної влади і місцевого самоврядування не мають права втручатися в охорону комерційної таємниці підприємства, за винятком випадків, передбачених законом.

Основна мета охорони конфіденційної інформації у тому, щоб вона не потрапила до конкурентів. У ряді випадків потрібна охорона й чужих комерційних таємниць, які можуть бути повідомлені підприємству іншими особами, організаціями. Відсутність такого захисту може позбавити підприємство вигідних партнерів, клієнтів.

Захист комерційної таємниці передбачає:

1. Визначення правил віднесення інформації до комерційної таємниці.

2. Розробку і доведення до осіб, які допущені до відомостей, що становлять комерційну таємницю, інструкцій за дотриманням режиму конфіденційності.

3. Обмеження доступу до носіїв інформації з комерційною таємницею.

4. Таке ведення діловодства, яке забезпечує виділення, облік і збереження документів з комерційною таємницею.

5. Використання організаційних, технічних та інших засобів захисту конфіденційності документів.

6. Здійснення контролю за дотриманням режиму охорони комерційної таємниці.

Для збереження доступу до інформації КТ керівник видає спеціальний наказ про введення «Переліку відомостей, що містять КТ підприємства», заходів з охорони цих відомостей, встановлення кола осіб, які мають доступ до такої інформації, правил роботи з документами, позначеними грифом «КТ». Співробітники підприємства повинні під розписку познайомитися з наказом і додатками до нього. Інколи порядок забезпечення КТ обумовлюється в трудовому контракті з працівником.

У випадку необхідності такий список може бути продовжений і також завірений підписом керівника з проставленням нової дати. Якщо відомості із «Переліку...» переносяться в документи, то документи стають конфіденційними, і від того, як буде організована робота з ними, багато в чому залежить успішна робота підприємства.

10.3. Право інтелектуальної власності на комерційну таємницю

Створення інформації, що становить комерційну таємницю іншими особами на користь суб'єктів господарювання стосується зазвичай продуктів інтелектуальної власності. Комерційною таємницею у таких випадках захищаються інформаційні характеристики зазначених продуктів. Право власності включає право володіння, право використання і право розпорядження чи поширення.

Враховуючи, що суб'єкти господарювання є власниками своєї комерційної таємниці, вони ж самі визначають умови та способи їх захисту, доступу до неї, в т. ч. і у будь-яких взаємовідносинах з іншими суб'єктами.

Згідно з положеннями Цивільного кодексу України (ст. 506) право розкриття комерційної таємниці належить особі, яка володіє майновими правами інтелектуальної власності на комерційну таємницю. Тобто, підстави, умови, способи захисту відомостей, що становлять комерційну таємницю у різних суб'єктів господарювання можуть бути різними, організуються кожним із них, виходячи з особливостей їх діяльності, інформаційних потреб та можливостей. Інформаційні відносини суб'єктів господарювання щодо комерційної таємниці, як правило, будуються на договірних засадах, з врахуванням нормативних документів суб'єктів у сфері їх інформаційної безпеки.

Право інтелектуальної власності на комерційну таємницю визначається Цивільним кодексом України.

Комерційна таємниця як об'єкт інтелектуальної власності має **свої особливості.**

По-перше, вона відрізняється найбільшою універсальністю, оскільки комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

По-друге, для виникнення прав на комерційну таємницю не вимагається виконання будь-яких формальностей, офіційного визнання її охороноздатності та державної реєстрації.

По-третє, оскільки в її основі лежить фактична монополія певної особи на деякі знання, то строк чинності права інтелектуальної власності на комерційну таємницю чітко не визначений і обмежується строком існування сукупності зазначених ознак комерційної таємниці.

Ознаками комерційної таємниці є:

– інформація, що становить комерційну таємницю має комерційну цінність;

– інформація, що становить комерційну таємницю, не відома іншим особам та відсутній вільний доступ до неї на законних підставах;

– вжито заходів для охорони конфіденційної інформації.

Ці ознаки комерційної таємниці є істотними, необхідними та невіддільними.

Майновими правами інтелектуальної власності на комерційну таємницю є (ст. 506 Цивільного кодексу):

– право на використання комерційної таємниці;

– виключне право дозволяти використання комерційної таємниці;

– виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;

– інші майнові права інтелектуальної власності, встановлені законом.

Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною, якщо інше не встановлено договором.

Саме ця особа може розпорядитися належним їй об’єктом, зокрема, шляхом розкриття відомостей невизначеному колу осіб.

Суб’єкт права інтелектуальної власності вправі в будь-який спосіб, не порушуючи прав інших осіб, використовувати комерційну таємницю. Він може передати іншій особі для використання останньою цієї інформації в її діяльності, зберігаючи чи не зберігаючи при цьому права на використання комерційної інформації у власній діяльності.

Особа, що порушила право інтелектуальної власності на комерційну таємницю, несе відповідальність, яка встановлена законом або договором. Зазвичай така відповідальність полягає у відшкодуванні шкоди. Якщо доступ до комерційної таємниці особа отримала на підставі договору, можливе встановлення договором неустойки за порушення права інтелектуальної власності на комерційну таємницю.

Суб’єктами, що несуть відповідальність перед власником комерційної таємниці, можуть бути юридичні особи, фізичні особи (якщо за них відповідно до законодавства не несе відповідальність юридична особа), в тому числі працівники юридичної чи фізичної особи — власника комерційної таємниці.

Інформація, що становить комерційну таємницю, має бути предметом адекватних існуючим обставинам заходів щодо збереження її конфіденційності, вжитих особою, яка законно контролює цю інформацію.

Строк чинності права інтелектуальної власності на комерційну таємницю визначається ст. 508 ЦК.

Строк чинності права інтелектуальної власності на комерційну таємницю обмежується строком існування сукупності ознак комерційної таємниці, встановлених частиною першою статті 505 Цивільного кодексу.

10.4. Відповідальність за незаконні дії щодо комерційної таємниці на підприємстві

За посягання на комерційну таємницю законодавство України передбачає дисциплінарну, кримінальну, адміністративну та цивільну відповідальність.

Тут слід виділити дві основні групи суб'єктів посягань на таку інформацію. Особи, що незаконно заволоділи інформацією та особи, що правомірно отримали таку інформацію, але порушили зобов'язання щодо збереження її в таємниці (працівники, контрагенти, партнери, клієнти, державні службовці).

Неправомірне збирання, розголошення та використання комерційної таємниці є видом недобросовісної конкуренції, який може становити досить серйозну загрозу економічній безпеці підприємства.

Адміністративна відповідальність. Ст.ст. 16–19 Закону України «Про захист від недобросовісної конкуренції» (07.06.1996 р. №236/96-ВР) визначено дії, які є видами недобросовісної конкуренції, а саме: неправомірне збирання комерційної таємниці (ст. 16), розголошення комерційної таємниці (ст. 17), схилення до розголошення комерційної таємниці (ст. 18), неправомірне збирання комерційної таємниці (ст. 19).

Вчинення вищезазначених дій, тягне за собою відповідальність, передбачену вищезазначеним законом.

За такі дії передбачено накладання штрафу Антимонопольним комітетом України, його територіальними відділеннями в розмірі до п'яти відсотків виручки від реалізації товарів, виконання робіт, надання послуг господарюючого суб'єкта за останній звітний рік, що передував року, в якому накладається штраф. Слід зазначити, що штраф накладається на юридичних осіб (ст. 21 Закону № 236).

У разі якщо обчислення виручки господарюючого суб'єкта неможливе або виручки немає, штрафи, зазначені в частині першій ст. 21, накладаються в розмірі до десяти тисяч неоподатковуваних мінімумів доходів громадян (170 тис. грн.).

Збитки, заподіяні внаслідок вчинення дій, визначених згаданим вище Законом як недобросовісна конкуренція, підлягають відшкодуванню за позовами зацікавлених осіб у порядку, визначеному цивільним законодавством України (ст. 24 Закону № 236).

Крім того, частиною третьою статті 164-3 Кодексу України про адміністративні правопорушення передбачено адміністративну відповідальність за отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця. За такі дії на правопорушника

накладається штраф у розмірі від дев'яти до вісімнадцяти НМДГ (від 153 грн. до 306 грн.). Нести адміністративну відповідальність, згідно із згаданою статтею, фізична особа може лише в тому випадку, коли вона вчинила дії, що свідчать про безпосереднє отримання, використання чи розголошення нею комерційної таємниці.

Щодо **цивільно-правової відповідальності** законодавство не встановлює спеціальних цивільних засобів охорони комерційної таємниці. Захист прав на комерційну таємницю можливий судом шляхом:

– визнання прав на комерційну таємницю;

– припинення дій, що порушують право на комерційну таємницю;

– компенсації моральної шкоди;

– стягнення з особи, яка порушила право, завданих збитків, включаючи неодержані доходи.

Крім того, у разі порушення комерційної таємниці можливим є застосування судом *спеціальних засобів захисту:*

– застосування негайних заходів щодо запобігання порушення прав на комерційну таємницю;

– вилучення товарів, виготовлених або введених у цивільний оборот з порушенням прав на комерційну таємницю;

– вилучення матеріалів та знарядь, які використовувалися переважно для виготовлення товарів з порушенням прав на комерційну таємницю;

– опублікування в засобах масової інформації відомостей про порушення права інтелектуальної власності на комерційну таємницю тощо.

Відповідальність в межах трудових відносин. За порушення режиму комерційної таємниці до працівника може застосовуватися матеріальна та дисциплінарна відповідальність. Дисциплінарна відповідальність передбачає застосування таких санкцій, як догана та звільнення.

Підставою застосування до працівника дисциплінарних заходів можливо за умови підпису працівником зобов'язання про не розголошення комерційної таємниці. Розмір штрафу обумовлюється в зобов'язанні і оформляється наказом підприємства.

Працівники несуть відповідальність перед роботодавцем за шкоду, заподіяну розголошенням комерційної таємниці відповідно до ст. 132 КЗпП (якщо працівник припустився розголошення комерційної таємниці при виконанні трудових обов'язків) або відповідно до п. 7 ст. 134 КЗпП (якщо розголошення комерційної таємниці допущене не при виконанні трудових обов'язків, хоч би комерційна таємниця і стала відома працівникові при виконанні трудових обов'язків). Не виключається повна матеріальна відповідальність працівників за шкоду, заподіяну розголошенням комерційної таємниці, на підставі п. 3 ст. 134 КЗпП, якщо дії працівника кваліфікуються як злочин, передбачений ст. 323 КК (розголошення комерційної таємниці, що завдало істотної шкоди суб'єкту господарської діяльності).

Кримінальна відповідальність. Кримінальним кодексом України (ККУ) за незаконне збирання з метою використання (комерційне шпигунство) або використання відомостей, що становлять комерційну таємницю (ст. 231 ККУ),

та за розголошення комерційної таємниці (ст. 232 ККУ) передбачено кримінальну відповідальність.

Так, статтею 231 ККУ умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, – караються штрафом від трьох тисяч до восьми тисяч НМДГ (від 51 тис. грн. до 136 тис. грн.).

Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, – карається штрафом від однієї тисячі до трьох тисяч НМДГ (від 17 тис. грн. до 51 тис. грн.) з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років (ст. 232 ККУ).

Слід звернути увагу, що за статтею 232 ККУ відповідальність може нести лише обмежене коло осіб – суб'єкти, яким такі відомості стали відомі у зв'язку з їхньою професійною чи службовою діяльністю, і які, згідно з чинним законодавством, повинні їх зберігати. До таких суб'єктів можуть відноситися працівники органів державної податкової служби, банків, правоохоронних органів, особи, яким комерційну таємницю було довірено її власником, та інші суб'єкти, які, згідно з чинним законодавством, мають право на ознайомлення з відомостями, що становлять комерційну таємницю, або мають доступ до таких відомостей по службі.

ТЕМА 11
ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ СИЛОВОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

11.1. Сутність силової безпеки виробничого підприємства

11.2. Завдання та функції служби безпеки підприємства щодо забезпечення захисту майна та особистої безпеки керівника підприємства

11.3. Організація діяльності підприємств, які надають послуги з охорони майна та фізичних осіб

11.4. Використання службових собак для забезпечення силової безпеки

11.5. Правове використання фізичної сили та спеціальних засобів при забезпеченні захисту та охорони майна підприємства

11.1. Сутність силової безпеки підприємства

Силова безпека підприємства характеризує захищеність інтересів підприємства від негативних фізичних впливів. Вона включає:

а) забезпечення фізичної безпеки (життя і здоров'я) працівників та керівника підприємства;

б) забезпечення захисту майна підприємства від негативних впливів, які можуть призвести до втрати цього майна або зниження його вартості;

в) забезпечення силових аспектів інформаційної безпеки підприємства.

Основні напрями діяльності підприємства щодо забезпечення силової безпеки:

– охорона керівника та персоналу підприємства від будь-яких посягань на здоров'я та життя;

– охорона будь-яких матеріальних цінностей керівника та персоналу підприємства;

– навчання персоналу розпізнавати небезпеки і вживати заходи самозахисту;

– захист особистої інформації;

– встановлення режиму охорони об'єктів (приміщень, ліній зв'язку, обладнання) підприємства;

– організація пропускного та допускного режимів;

– оснащення об'єктів підприємства сучасними технічними засобами охорони (охоронно-пожежні системи, відео- та радіоапаратура, огородження тощо);

– забезпечення захисту від комп'ютерних крадіжок;

– захист матеріалів та готової продукції всередині підприємства.

– розроблення заходів щодо попередження шахрайства, крадіжок.

Дії, що негативно впливають на рівень силової безпеки:

– фізичні й моральні впливи на конкретних особистостей (особливо на керівництво та провідних спеціалістів) з метою заподіяти шкоду їх здоров'ю та репутації;

– негативні дії, спрямовані на те, щоб завдати шкоди майну, зокрема, загрози зменшення активів підприємства і втрати ним фінансової незалежності;

– негативний вплив на інформаційне середовище підприємства (так зване промислове шпигунство).

–кримінальні мотиви одержання злочинними юридичними (фізичними) особами доходів через шантаж, шахрайство або крадіжки;

– некомерційні мотиви посягань на життя та здоров'я керівників і працівників підприємства , а також на майно підприємства.

Показники, за допомогою яких можна оцінити стан силової безпеки:

– коефіцієнт захищеності майна підприємства

($К_{ЗМ}$ = Витрати на охорону майна підприємства / Загальні витрати підприємства);

– ефективність роботи служби охорони та режиму

($Е_{СОР}$ = Приріст прибутку, одержаного в результаті роботи служби охорони та режиму / Витрати на діяльність служби охорони та режиму);

– коефіцієнт захищеності персоналу підприємства

($К_{ЗП}$ = Витрати на охорону персоналу підприємства / Загальні витрат підприємства);

– коефіцієнт захищеності підприємства від незаконного проникнення

($К_{ЗНП}$ =Кількість відвернутих спроб незаконного проникнення на територію підприємства, од. / Загальна кількість спроб незаконного проникнення на територію підприємства, од);

– коефіцієнт комп'ютерного захисту

($К_{КЗ}$ = Кількість відвернутих спроб комп'ютерних крадіжок, од / Загальна кількість спроб комп'ютерних крадіжок, од.);

– коефіцієнт фізичного захисту працівників (керівників)

($К_{ФЗП}$ = Кількість відвернутих спроб заподіяти фізичну шкоду працівникам (керівникам), од. / загальна кількість спроб заподіяти фізичну шкоду працівникам (керівникам), од.);

– коефіцієнт надійності персоналу, що забезпечує силову безпеку

($К_{НП}$ = (загальна кількість звільнених працівників, осіб – кількість працівників, звільнених за причиною спроби нанесення збитків (матеріальних або нематеріальних) підприємству, осіб) / загальна кількість звільнених працівників, осіб);

Розрахунок силової безпеки підприємства за цими показниками дозволить оцінити:

1) рівень захищеності підприємства від незаконного проникнення;

2) рівень захищеності підприємства від комп'ютерних крадіжок;

3) рівень захищеності працівників та керівництва підприємства від фізичних негативних впливів;

4) надійність персоналу, що забезпечує силову безпеку;

5) рівень фінансування силових служб підприємства.

11.2. Завдання та функції служби безпеки підприємства щодо забезпечення захисту майна та особистої безпеки керівника підприємства

Основними напрямами охоронної діяльності служби безпеки є:

– захист життя і здоров'я громадян;

– охорона майна власників;

– проектування, монтаж і експлуатаційне обслуговування засобів охоронно-пожежної сигналізації.

Кожен із зазначених напрямів має свої особливості при гарантуванні

безпеки конкретного об’єкта захисту.

Об’єктами охорони є: стаціонарні об’єкти, рухомі об’єкти, персонал, грошові кошти, цінні папери та інші цінності.

До функцій із забезпечення захисту майнової власності підприємства належать:

– визначення системи охорони підприємства, дислокація посад, технічних засобів безпеки, протипожежної автоматики, зв’язку;

– виділення приміщень (ділянок), де зберігаються ТМЦ (кошти), і здійснення через керівників відповідних підрозділів заходів для підвищення надійності їх фізичного захисту;

– визначення ділянок, які уразливими у вибухопожежному відношенні і які можуть завдати серйозної шкоди підприємству, та вироблення заходів для нейтралізації загроз;

– визначення технічного устаткування, яке може призвести до великих економічних втрат, і розробка заходів для нейтралізації загроз;

– визначення уразливих місць у технології виробничого циклу, несанкціонована зміна яких може призвести до втрати якості продукції, що випускається, і завдати матеріальної шкоди, та вироблення відповідних заходів;

– розробка, впровадження в дію і підтримка на території, що охороняється пропускного та внутрішньооб’єктового режиму (порядок, час проходження працівників, відвідувачів на територію підприємства, в тому числі і у святкові дні; порядок ввезення (вивезення) матеріальних цінностей, готової продукції, матеріалів тощо; місце розташування і кількість контрольних проходів і проїздів; приміщення і підрозділи, доступ у які обмежений; система перепусток і документації);

– розробка документів, які регламентують адміністративно-правову основу діяльності з охорони майнових цінностей підприємства (інструкція про порядок забезпечення схоронності матеріальних і документальних цінностей підприємства; інструкції про пропускний і внутрішньооб’єктний режими);

– доведення вимог із питань охорони, пропускного і внутрішньооб’єктного режимів до персоналу підприємства;

– контроль виконання та аналіз стану надійності збереження матеріальних цінностей, охорони, пропускного і внутрішньооб’єктного режимів);

– проведення службових розслідувань із фактів порушення порядку роботи з майновими цінностями;

– організація взаємодії з державними органами безпеки та органами внутрішніх справ із забезпечення безпеки підприємства (з урахуванням компетенції цих органів).

У комплексних системах безпеки комерційних об’єктів одним з найбільш складних напрямів в даний час є забезпечення особистої безпеки керівників та персоналу підприємств. Актуальність та гострота цієї проблеми визначаються наростанням кількості терористичних актів та інших тяжких злочинів відносно громадян, що працюють в сферах підвищеного ризику.

Для такої ситуації ще характерна і та обставина, що використання найсучасніших видів зброї, а також мобільних засобів пересування дозволяє злочинцям здійснювати свої задуми з більшим ступенем безпеки для себе. Разом з тим невиправдана безтурботність і відсутність елементарного порядку у питаннях збереження інформації про системи охорони часто допомагають злочинцям детально вивчити образ життя своєї жертви, виявити вразливі місця охорони, вибрати відповідний спосіб і засіб вчинення злочинного акту.

Природно, що в кожному конкретному випадку неможливо з абсолютною точністю передбачити, який засіб і метод обере злочинець, але, з урахуванням великої практики, можна дати рекомендації, як діяти в тих чи інших ситуаціях і яким чином можна спробувати попередити, що готується злочин.

До функцій із забезпечення особистої безпеки підприємства належать:

– розробка заходів забезпечення фізичного захисту персоналу; організація охорони (особистої охорони, охорони засобів пересування), пропускного та внутрішньооб'єктного режимів; встановлення відповідного порядку приймання відвідувачів, роботи секретарів-референтів тощо);

– забезпечення персоналу засобами технічного захисту від несанкціонованого проникнення в приміщення, в автомашини, на автостоянки, у квартири, для фіксації спроб злочинних дій (установка магнітофонів, кінокамер), для прихованого зв'язку керівника з охороною підприємства;

– визначення переліку інформації, що не підлягає розголошенню (яка не входить до комерційної таємниці) стороннім особам;

– збирання службою безпеки інформації про ознаки, характерні для конкретних видів загроз персоналу;

– забезпечення контролю за проведенням ремонтних, профілактичних робіт, здійснюваних сторонніми організаціями на підприємстві (в разі необхідності проводяться спеціальні обстеження після завершення робіт цих приміщень, автомашин, пристроїв, приладів);

– підготовка персоналу до дій в екстремальних ситуаціях (вироблення навичок оцінки інформації, яка відповідає нормам поведінки та прийняття рішень;

– навчання персоналу і членів їх родин виявленню ознак, які вказують на підготовку спрямованих проти них дій;

– встановлення і підтримка практичних форм взаємодії служби безпеки із правоохоронними органами щодо надання безпеки персоналу.

– запобігання фізичному та іншому насильству з боку злочинних груп і стосовно працівників підприємства та його ділових партнерів з числа українських та іноземних бізнесменів, тобто захист їх життя та здоров'я;

– усунення або ослаблення причин і обставин, внаслідок яких може виникнути загроза життю і власності громадян;

– локалізація шкідливих наслідків протиправних дій до осіб, що охороняються;

– отримання та аналіз попереджувальної інформації про зовнішні загрози життю і здоров'ю осіб, що охороняються.

Слід пам’ятати, що від фізичного впливу з боку «професійно» підготовлених кримінальних елементів захиститися складно. Тому головне завдання охоронця – передбачити і запобігти загрозі життя особи, що охороняється, перетворити конфліктну ситуацію в безконфліктну. Для охоронця головне не стільки відбити напад, скільки його не допустити, майстерно вивести особу, що охороняється, з небезпечної ситуації, не піддавшись на різного роду провокації. При цьому значну роль у роботі охоронця відіграє психологічний фактор, тобто його вміння справляти враження, нібито об’єкт захисту абсолютно недоступний для зазіхань.

Фахівці вважають, що повного захисту від дій терористів гарантувати не може ні одна служба, оскільки існує чимало об’єктивних причин, через які ефективність роботи охоронця і служб безпеки може бути зведена до нуля.

Жоден серйозний фахівець ніколи нікому стовідсоткової гарантії у цій сфері послуг не дає. Навіть потужна охоронна урядова служба, яка має на озброєнні найсучаснішу техніку, не завжди в змозі спрацювати надійно. На думку професіоналів, охорона однієї особи силами 200 осіб, з яких 40 працює “у відкриту”, а решта “під прикриттям”, може забезпечити лише 90% захисту під час замаху.

11.3. Організація діяльності підприємств, які надають послуги з охорони майна та фізичних осіб

Сферу охоронних послуг в Україні представляє Управління поліції охорони (до листопад 2015 року – Державна служба охорони при Міністерстві внутрішніх справ України) та майже 3 тисячі недержавних охоронних структур. Окрім цього вона включає внутрішні служби безпеки банків, великих підприємств, що не отримують окремої ліцензії, а працюють відповідно до внутрішніх наказів. У сфері охоронної діяльності України наразі зайнято сотні тисяч громадян.

Охоронна діяльність (зг. із ЗУ «Про охоронну діяльність» від 22.03.2012р.) – надання послуг з охорони власності та громадян.

Згідно із Законом України «Про ліцензування видів господарської діяльності» від 02.03.2015 року (ст. 7) охоронна діяльність підлягає ліцензуванню. Видає ліцензії на здійснення охоронної діяльності центральний орган виконавчої влади у сфері охоронної діяльності – Міністерство внутрішніх справ України. **Крім видачі ліцензій центральний орган виконавчої влади у сфері охоронної діяльності:**

– затверджує ліцензійні умови провадження охоронної діяльності;

– затверджує порядок контролю за додержанням ліцензійних умов провадження охоронної діяльності;

– переоформляє ліцензії на здійснення охоронної діяльності, видає дублікати таких ліцензій та приймає рішення про визнання їх недійсними;

– здійснює у межах своєї компетенції контроль за додержанням суб’єктами охоронної діяльності ліцензійних умов шляхом проведення планових та позапланових перевірок;

– приймає рішення про усунення недоліків, анулювання ліцензій на охоронну діяльність;

– вносить до Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань відомості про ліцензування господарської діяльності суб'єкта охоронної діяльності.

Суб'єкт охоронної діяльності – суб'єкт господарювання будь-якої форми власності, створений та зареєстрований на території України, що здійснює охоронну діяльність на підставі отриманої у встановленому порядку ліцензії.

Види охоронних послуг, які надаються суб'єктом охоронної діяльності:

– охорона майна громадян;

– охорона майна юридичних осіб;

– охорона фізичних осіб.

Охорона майна та фізичних осіб забезпечується персоналом охорони шляхом здійснення таких заходів:

– використання пунктів централізованого спостереження, технічних засобів охорони, транспорту реагування, службових собак (*пункт централізованого спостереження* – центр з працюючим персоналом, який спостерігає за станом систем передавання тривожних сповіщень; *технічні засоби охорони* – технічні засоби, що використовуються під час здійснення охоронної діяльності: системи, прилади та обладнання для виявлення, оповіщення і попередження про наявність небезпеки для життя людей та/або майна; *транспорт реагування* – транспортний засіб, що знаходиться у власності суб'єкта охоронної діяльності, призначений для забезпечення негайного реагування персоналу охорони на протиправні дії щодо об'єкта охорони або на події та обставини, що завдають (можуть завдати) майнової шкоди або створюють можливу загрозу особистій безпеці громадян чи персоналу охорони на об'єктах охорони);

– контроль за станом майнової безпеки об'єкта охорони;

– запобігання загрозам особистій безпеці фізичної особи, що охороняється;

– реагування в межах наданих законом повноважень на протиправні дії, пов'язані з посяганням на об'єкт охорони.

Відповідно до Закону України «Про охоронну діяльність» (22.03.2012 року), Закону України «Про ліцензування видів господарської діяльності» постановою КМУ від 18.11.2015 року №960 затверджено ліцензійні умови, які визначають організаційні, кадрові та технологічні вимоги провадження охоронної діяльності.

Організаційні вимоги.

Суб'єкт охоронної діяльності зобов'язаний:

1) зберігати протягом строку дії ліцензії документи, копії яких подавалися органу ліцензування, а також ті, що підтверджують достовірність даних, що зазначалися здобувачем ліцензії у документах, які подавалися органу ліцензування для отримання ліцензії;

2) повідомляти органу ліцензування про всі зміни даних, які були зазначені у документах, що додавалися до заяви про отримання ліцензії.

У разі зміни таких даних ліцензіат не пізніше одного місяця з дня їх настання подає органу ліцензування відповідне повідомлення в письмовій формі разом з копіями документів, які підтверджують зазначені зміни (крім даних щодо персоналу охорони, що містять інформацію про загальну кількість персоналу охорони та рівень його кваліфікації, про зміну яких органу ліцензування повідомляється щороку до 15 грудня (станом на 1 грудня);

3) забезпечити присутність керівника ліцензіата, його заступника або іншої уповноваженої особи під час проведення органом ліцензування в установленому законом порядку перевірки додержання ліцензіатом Ліцензійних умов;

4) зберігати відео- та фотоматеріали, отримані під час здійснення заходів охорони, протягом одного року з можливістю використання їх виключно у службовій діяльності. Після закінчення строку зберігання зазначених матеріалів проводиться їх знищення комісією у складі трьох представників суб'єкта охоронної діяльності із складенням акта знищення відео- та фотоматеріалів;

5) надавати послуги з охорони власності та громадян на підставі письмових цивільно-правових договорів охорони, які укладаються за наявності в замовників охоронних послуг документів, що підтверджують їх повноваження на володіння (користування) об'єктом охорони на законних підставах, а також правомірність перебування майна, транспортного засобу чи особи у визначеному місці охорони;

6) вести письмовий або електронний облік договорів охорони, виконувати умови договорів з надання охоронних послуг на користь третіх осіб лише за їх письмовою згодою. Під час укладання договорів зазначаються конкретний об'єкт охорони, його місцезнаходження;

7) зазначати в договорах охорони відповідно до Цивільного кодексу України умови відшкодування шкоди, завданої через неналежне виконання ним своїх зобов'язань перед замовником;

8) розміщувати на видному місці на центральному посту стаціонарного об'єкта (за згодою замовника охоронних послуг), який охороняється персоналом охорони, інформацію про найменування ліцензіата, його місцезнаходження, ідентифікаційний код юридичної особи, дату і номер рішення про видачу ліцензії;

9) повідомляти негайно у будь-який можливий спосіб територіальному органу Національної поліції про:

– факти припинення правопорушень стосовно персоналу охорони, майна або фізичних осіб, які охороняються, застосування заходів фізичного впливу, спеціальних засобів, використання службових собак персоналом охорони, а в разі заподіяння тілесних ушкоджень правопорушнику – негайно викликати екстрену (швидку) медичну допомогу та надавати першу долікарську допомогу;

– виявлення ознак кримінального правопорушення, порушення громадського порядку;

10) до прибуття працівників правоохоронних органів вжити всіх можливих заходів для охорони місця події та збереження слідів злочину, виявлення очевидців і фіксації їх персональних даних. Після прибуття

працівників правоохоронних органів персонал охорони зобов'язаний діяти за їх вказівкою.

Суб'єкт охоронної діяльності забезпечує:

1) наявність у персоналу охорони під час виконання функціональних обов'язків посвідчень, з підписом керівника суб'єкта охоронної діяльності, в якому зазначаються прізвище, ім.'я, по батькові особи, яка належить до персоналу охорони, дата видачі і термін дії посвідчення та міститься фотокартка особи, якій видано посвідчення;

2) виконання функції з охорони майна за обов'язкової наявності на одязі персоналу охорони ознак належності до відповідного суб'єкта охоронної діяльності згідно з його статутними документами;

3) дотримання порядку застосування персоналом охорони заходів фізичного впливу та спеціальних засобів;

4) використання службових собак у визначному законодавством порядку.

Обладнання транспорту реагування засобами радіотехнічного зв'язку, кольорографічними схемами (написами), світловими та звуковими сигналами здійснюється з урахуванням таких вимог:

1) засоби радіотехнічного зв'язку, експлуатація яких потребує наявності відповідних дозволів, використовуються після отримання таких дозволів;

2) на транспорт реагування суб'єкта охоронної діяльності наносяться кольорографічні схеми (написи), які ідентифікують суб'єкта охоронної діяльності, зокрема його скорочене найменування, номер телефону та емблема (у разі наявності);

3) на транспорт реагування, обладнаний кольорографічними схемами (написами), установлюються спеціальні світлові сигнальні пристрої автожовтого (оранжевого) кольору та спеціальні звукові сигнали (далі - спеціальні пристрої);

4) використання спеціальних пристроїв дозволяється виключно у випадках оперативного реагування на тривожні сповіщення, що надійшли до пункту централізованого спостереження суб'єкта охоронної діяльності.

Під час організації та провадження охоронної діяльності забороняється:

1) придбавати та використовувати майно, визначене законодавством для виключного використання військовими формуваннями та правоохоронними органами;

2) використовувати не сертифіковані в установленому порядку технічні засоби охорони спеціального призначення, засоби радіозв'язку без наявності дозволу на їх використання на наданих радіочастотах, а також інші технічні засоби, що завдають шкоди життю, здоров'ю громадян, довкіллю;

3) використовувати ознаки належності (елементи символіки, формений одяг тощо) до МВС, СБУ, Управління державної охорони, Збройних Сил та інших утворених відповідно до законів військових формувань, правоохоронних, природоохоронних, контролюючих або інших органів виконавчої влади, їх спеціальних підрозділів, у тому числі в найменуванні суб'єкта охоронної діяльності, на одязі, транспорті реагування, будівлях, у документації;

4) створювати перешкоди чи заважати діяльності представників правоохоронних та інших органів державної влади, органів місцевого самоврядування, їх посадових осіб, а також громадянам у здійсненні ними повноважень, наданих їм законами та іншими нормативно-правовими актами;

5) розголошувати відомості про вжиті заходи до організації та провадження охоронної діяльності, а також інформацію з обмеженим доступом та інформацію про особу, яка охороняється, що стали відомі у зв'язку з провадженням такої діяльності, крім випадків, передбачених законодавством;

6) приховувати відомості про кримінальні правопорушення, що вчиняються або готуються, незалежно від інтересів замовника послуг з охорони;

7) охороняти фізичну особу, яка вчиняє злочинні дії, адміністративне правопорушення або намагається їх учинити;

8) вчиняти дії, що посягають на права, свободи та власність фізичних осіб, а також ставлять під загрозу їх життя та здоров'я, честь, гідність і ділову репутацію;

9) здійснювати заходи, що належать до оперативно-розшукових відповідно до Закону України «Про оперативно-розшукову діяльність»;

10) залучати до охоронних заходів осіб, які не подали документів, необхідних для прийняття на роботу, або не відповідають кваліфікаційним вимогам;

11) брати участь у виконанні судових рішень під час виконавчого провадження;

12) вчиняти дії, спрямовані на силове протистояння між персоналом охорони різних суб'єктів господарювання;

13) охороняти об'єкти, включені до переліку особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями, визначеного в порядку, затвердженому Кабінетом Міністрів України;

14) використовувати спеціальні засоби, не включені до переліку спеціальних засобів, придбання, зберігання та використання яких здійснюється суб'єктами охоронної діяльності, затвердженого постановою Кабінету Міністрів України від 11 лютого 2013 р. № 97 (Офіційний вісник України, 2013 р., № 12, ст. 456);

15) застосовувати заходи фізичного впливу та спеціальні засоби проти жінок з явними ознаками вагітності, осіб похилого віку або з вираженими ознаками інвалідності та малолітніх осіб, а також проти осіб, які відповідно до законодавства є носіями спеціального статусу недоторканності, крім випадків учинення ними нападу, що становить загрозу життю та здоров'ю фізичних осіб, персоналу охорони, або збройного нападу чи збройного опору;

16) застосовувати спеціальні засоби в місцях значного скупчення людей, якщо це може призвести до заподіяння шкоди життю та здоров'ю сторонніх осіб, крім випадків самооборони (самозахисту);

17) використовувати в охоронній діяльності у громадських і загальнодоступних місцях службових собак без провідника собаки.

Кадрові вимоги.

До штату суб'єкта охоронної діяльності, його філії, іншого відокремленого підрозділу повинен входити фахівець (фахівці) з організації заходів охорони.

Під час прийняття на роботу фахівець (фахівці) з організації заходів охорони подає (подають) документи:

– документи, які підтверджують проходження особою обов'язкового попереднього (періодичного) психіатричного огляду та профілактичного наркологічного огляду, які видані в установленому порядку;

– документ, який підтверджує, що такі особи не мають непогашеної чи не знятої в установленому законом порядку судимості за скоєння умисних злочинів;

– документ, що підтверджує відсутність в особи обмежень за станом здоров'я для виконання функціональних обов'язків, який видається в установленому порядку;

– копію паспорта громадянина України;

– документ, що підтверджує набуття кваліфікації.

Зазначений фахівець повинен мати один з таких освітніх та (або) **кваліфікаційних рівнів:**

– вищу освіту і стаж роботи не менше трьох років на посадах офіцерського складу в оперативних і слідчих підрозділах органів внутрішніх справ, міліції охорони, СБУ або стаж не менше трьох років на командних посадах стройових частин та навчальних закладів Збройних Сил, на посадах середнього та старшого начальницького складу правоохоронних органів, військових формувань, утворених відповідно до законів, та відомчої воєнізованої охорони;

– вищу освіту і стаж роботи на керівних посадах (директора, заступника директора, керівника філії, іншого відокремленого підрозділу) суб'єкта охоронної діяльності не менше трьох років або стаж не менше трьох років на посадах, відповідальних за напрям охорони;

– вищу юридичну освіту і стаж роботи за спеціальністю в суб'єкта охоронної діяльності не менше трьох років.

Охоронники, охоронці повинні входити до штату суб'єкта охоронної діяльності та залежно від об'єкта, що охороняється, відповідати кваліфікаційним вимогам, визначеним наказом Мінпраці від 29 грудня 2004 р. № 336 «Про затвердження Випуску 1 «Професії працівників, що є загальними для всіх видів економічної діяльності» Довідника кваліфікаційних характеристик професій працівників». Рівень відповідності кваліфікаційним вимогам документально підтверджується згідно із законодавством.

Працівники, залучені до роботи на пункті централізованого спостереження, повинні входити до штату суб'єкта охоронної діяльності та подати необхідні для прийняття на роботу документи: документи, які підтверджують проходження особою обов'язкового попереднього (періодичного) психіатричного огляду та профілактичного наркологічного огляду, які видані в установленому порядку; документ, який підтверджує, що такі особи не мають непогашеної чи не знятої в установленому законом

порядку судимості за скоєння умисних злочинів; документ, що підтверджує відсутність в особи обмежень за станом здоров'я для виконання функціональних обов'язків, який видається в установленому порядку; копію паспорта громадянина України;

Освітня підготовка персоналу пункту централізованого спостереження, який спостерігає за станом систем передавання сповіщень, повинна бути не нижче повної загальної середньої освіти.

Професійна підготовка персоналу пункту централізованого спостереження забезпечується суб'єктом охоронної діяльності.

Персоналом охорони можуть бути дієздатні громадяни України, які досягли 18-річного віку, пройшли відповідне навчання або професійну підготовку, уклали трудовий договір із суб'єктом охоронної діяльності (входять до штату суб'єкта охоронної діяльності).

Під час прийняття на роботу ліцензіат зобов'язаний отримати від зазначених осіб документи, необхідні для прийняття на роботу до суб'єкта охоронної діяльності.

Технологічні вимоги.

У разі використання суб'єктом охоронної діяльності пункту централізованого спостереження він забезпечує:

– цілодобовий режим чергування операторів такого пункту;

– наявність транспорту реагування;

– ведення електронного журналу реєстрації подій (тривога, несправність, відсутність живлення тощо), що передбачає збереження запису про відповідну подію протягом не менш як 30 діб;

– наявність резервної персональної електронної обчислюваної машини;

– наявність джерела безперебійного резервного живлення.

Пункт централізованого спостереження повинен розташовуватися у нежилому приміщенні і бути обладнаним:

– системою цілодобової аудіореєстрації звукового фону операційного залу такого пункту і телефонних розмов у режимі реального часу з обсягом архівації запису не менше ніж за 14 діб;

– системою відеоспостереження за операційним залом з цілодобовою реєстрацією відеоінформації у режимі реального часу з обсягом архівації запису не менше ніж за 14 діб;

– аудіовідеопереговорним пристроєм і засобами технічної укріпленості, які унеможливлюють доступ до приміщення пункту централізованого спостереження сторонніх осіб.

11.4. Використання службових собак для забезпечення силової безпеки

Персонал охорони під час і в місцях виконання заходів охорони має право використовувати службових собак, які пройшли у встановленому порядку відповідний курс дресирування, визнані придатними для службового використання та мають ветеринарний паспорт, винятково для виявлення:

1) проникнень (спроб проникнень) на об'єкти, що охороняються;

2) осіб, які незаконно перебувають на об'єктах, що охороняються.

Забороняється використання службових собак в охоронній діяльності без наявності провідника собаки в громадських і загальнодоступних місцях. При цьому собаки мають бути на повідку та стосовно них мають дотримуватися установлені ветеринарні правила.

На закритих територіях, де відсутні люди, дозволяється тримати собак без прив'язі, якщо на видних місцях розміщені чіткі та розбірливі попереджувальні написи про охорону об'єкта за допомогою службових собак. При цьому за ними повинен забезпечуватися постійний контроль з боку персоналу охорони.

Незважаючи на широке розповсюдження технічних охоронних пристроїв, не слід забувати про можливість використання в цих цілях приручених тварин.

В основному для цієї мети використовуються собаки службових порід, що пройшли дресирування на спеціальних курсах. Найбільш придатними для виконання функцій собаки-охоронці, охоронця житла або автомобіля вважаються такі породи, як східноєвропейська, німецька, кавказька південноросійська вівчарки, ротвейлер, різеншнауцер, доберман, ірландський вовкодав. Також непогано можуть вирішувати такі завдання доги, ердельтер'єр, боксери, ірландські тер'єри і деякі інші породи. Для пошуку мін, вибухових вкладень у поштову кореспонденцію можна використовувати собак дрібних порід, які пройшли спеціальну підготовку.

На думку фахівців, середній вік собак, що використовуються для пошуку вибухових речовин, має дорівнювати два з половиною роки, а тренувати їх слід починати з 18 місяців.

Переваги використання собак у порівнянні із застосуванням з тією ж метою газоаналізаторів полягають в наступному:

– собака виявляє вибухові речовини швидше детекторів і може працювати повний восьмигодинний робочий день з короткими перервами на відпочинок;

– собака може бути натренований на пошук різних речовин, вона веде пошук ретельніше і повніше;

– на нюх собаки не впливають хімічні препарати, використовувані для освіження повітря і сильно пахучі сполуки, такі, як нафта і дезінфікуючі речовини.

Проте у використання собак для забезпечення особистої безпеки підприємця є певні тонкощі, які обов'язково треба враховувати:

1. Собака – жива істота, дуже розумна та емоційна. Придбавши собаку, ви берете на себе відповідальність за неї.

2. Людина яка гратиме роль провідника службового собаки, обов'язково повинна пройти курс підготовки і провести дресирування собаки. Кваліфікованою є лише тварина, яка навчилася правильно діяти в екстремальних ситуаціях нападу. Це означає, що вона вміє розпізнавати небезпеку, атакувати озброєних злочинців, захищатися від них, виконує команди свого провідника.

3. Собака повинен жити в належних умовах. Неприпустимі для нього надто ніжні й надто суворі умови. Собаку має годувати тільки одна особа – її провідник. З чужих рук дресирована собака їжу брати не повинна.

4. Собаку потрібно регулярно тренувати у спеціально обладнаному місці: вона повинна бігати, стрибати через перешкоди, повзати, нападати на навчальний макет, на людину, що зображує злочинця, вислизати від наведеного на неї ствола пістолета, рушниці, автомата.

5. Категорично забороняється бити собаку, кричати на нього, відбирати їжу, жартома нацьковувати на людей (собака жартів не розуміє), знущатися з нього (знущання собака розуміє дуже добре).

6. За своєю конституцією (статурою) собак поділяють на три основних типи:

– *важкі* (наприклад, доги, ротвейлери, чорні тер'єри);

– *середні* (німецькі вівчарки, різеншнауцери, великі добермани);

– *малі* (ердельтер'єри, боксери).

Оптимальний варіант – середній тип. А найкращий собака – вівчарка або лайка, за умови, що вівчарка зліша, а лайка розумніша.

7. Основні варіанти атаки собак "середнього" типу полягають у стрибку на плечі, в ударі всіма чотирма лапами (або грудьми) в поперек, а також в ударі головою під коліна. Як тільки людина впала, собака пускає в хід зуби. Дресировані собаки вміють кусати за ноги, горло, пах. Особливо важливо виробити у собаки рефлекс укусу тієї руки, яка тримає зброю, і нападати не тільки заду або збоку (так чинять ненавчені собаки), а й спереду. Всі види атак потрібно відпрацювати з твариною до повного автоматизу дій.

Вченими неодноразово робилися спроби оцінити чутливість собак і порівняти її з чутливістю різних детекторів, які використовуються на практиці. Однак поки що механізм виявлення собаками вибухових речовин ще не вивчений. Фахівці вважають, що в багатьох випадках застосування собак у цій сфері може виявитися більш ефективним, ніж інші спеціальні засоби.

11.5. Правове використання фізичної сили та спеціальних засобів при забезпеченні захисту та охорони майна підприємства

Під час здійснення охоронної діяльності персонал охорони має право застосовувати до осіб, які посягають на об'єкт охорони, заходи фізичного впливу та спеціальні засоби в особливих випадках, якщо інші заходи не привели до припинення посягання або до виконання особою законної вимоги персоналу охорони, у разі:

– захисту себе або іншої особи від нападу, що становить загрозу життю та здоров'ю або майну;

– запобігання незаконній спробі насильницьким шляхом заволодіти спеціальними засобами;

– необхідності затримати правопорушника, який незаконно проник на об'єкт, що охороняється, або який вчиняє інші протиправні дії та чинить опір;

– знешкодження тварини, що загрожує життю та здоров'ю персоналу охорони або інших осіб.

Затримання особи персоналом охорони не є адміністративним затриманням. Затримана особа негайно передається органу внутрішніх справ за місцем вчинення правопорушення.

Застосовувати заходи фізичного впливу та спеціальні засоби дозволяється тільки після попередження голосом і жестами про намір їх застосування.

Заходи фізичного впливу та спеціальні засоби можуть застосовуватися без попередження у разі:

– раптового нападу;

– нападу чи опору з використанням зброї або предметів, що становлять загрозу життю та здоров'ю особи, або з використанням механічних транспортних засобів.

Забороняється застосовувати заходи фізичного впливу та спеціальні засоби проти жінок з явними ознаками вагітності, осіб похилого віку або з вираженими ознаками інвалідності та малолітніх осіб, а також проти осіб, які відповідно до законодавства є носіями спеціального статусу недоторканності, крім випадків учинення ними нападу, що становить загрозу життю та здоров'ю фізичних осіб, персоналу охорони, або збройного нападу чи збройного опору.

У разі якщо неможливо уникнути застосування заходів фізичного впливу та спеціальних засобів, їх застосування має здійснюватися в межах правомірності з дотриманням умов і обставин, які виключають злочинність діяння, і повинно обмежуватися заподіянням мінімальної шкоди здоров'ю особи чи інших негативних наслідків. У разі заподіяння такої шкоди персонал охорони повинен негайно викликати швидку медичну допомогу та надати першу долікарську допомогу потерпілим.

Персоналу охорони забороняється застосовувати спеціальні засоби в місцях значного скупчення людей, якщо це може призвести до заподіяння шкоди життю та здоров'ю сторонніх осіб, крім випадків самооборони (самозахисту).

Про всі факти припинення правопорушення стосовно персоналу охорони, майна або фізичних осіб, які охороняються, застосування заходів фізичного впливу, спеціальних засобів, використання службових собак персонал охорони зобо'язаний негайно в усній або письмовій формі повідомити свого безпосереднього керівника і територіальний орган внутрішніх справ, а в разі нанесення тілесних ушкоджень правопорушнику – негайно викликати швидку медичну допомогу.

У разі виявлення ознак кримінального правопорушення персонал охорони зобов'язаний до прибуття працівників правоохоронних органів вжити всіх можливих заходів для охорони місця події та збереження слідів кримінального правопорушення, виявлення очевидців і фіксації їхніх персональних даних. Після прибуття працівників правоохоронних органів персонал охорони зобов'язаний діяти за їх вказівкою.

ТЕМА 12
ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ТЕХНІКО-ТЕХНОЛОГІЧНОЇ, ПОЛІТИКО-ПРАВОВОЇ ТА РИНКОВОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

12.1. Сутність та загрози техніко-технологічної безпеки підприємства

12.2. Показники оцінки техніко-технологічної безпеки та заходи її забезпечення

12.3. Поняття політико-правової безпеки, показники оцінки та заходи забезпечення

12.4. Сутність ринкової безпеки підприємства та показники

12.1. Сутність та загрози техніко-технологічної безпеки підприємства

Техніко-технологічна безпека – це складова фінансово-економічної безпеки, пріоритетним завданням якої є захист від негативних чинників з метою створення та найбільш ефективного використання технічної бази та технологічних процесів для забезпечення високого рівня конкурентоспроможності підприємства.

До **техніко-технологічної безпеки** підприємства належить створення й використання технічної бази, основних засобів виробництва і таких технологій та бізнес-процесів, які посилюють конкурентоздатність підприємства.

Ця складова є захистом від можливих витрат унаслідок використання застарілої техніки і технології виробництва продукції, неефективної організації виробничого процесу. Вона повинна відображати ступінь відповідності технологій, які застосовуються на підприємстві, сучасним світовим аналогам щодо оптимізації витрат ресурсів.

Техніко-технологічна безпека характеризується такими ознаками:

– якістю і відповідністю технологічного процесу виробництва та основного капіталу потребам ринку;

− захищеністю техніко-технологічної сфери підприємства від негативного впливу зовнішніх і внутрішніх загроз;

− здатністю техніко-технологічної сфери підприємства забезпечувати його високу конкурентоспроможність;

− за рахунок високої ефективності використання основного капіталу забезпечувати сталий розвиток підприємства.

Негативно впливають на цю складову:

– дії, спрямовані на зниження технологічного потенціалу підприємства;

– порушення технологічної дисципліни;

– моральне старіння використовуваних технологій;

– відсутність зовнішніх і внутрішніх інвестицій;

– неможливість отримання довгострокових кредитів від банків не дають змоги поповнювати обігові кошти підприємства і спрямовувати їх на оновлення парку обладнання;

– підвищення цін на енергоносії (призводить до зростання собівартості продукції);

– неефективна організація виробничого процесу;

– високий ступінь спрацювання основного капіталу;

– неефективне управління оборотними активами на всіх етапах виробничого процесу.

Забезпечення техніко-технологічної безпека передбачає здійснення кількох послідовних етапів.

Перший етап охоплює аналіз ринку технологій стосовно виробництва продукції, аналогічної профілю досліджуваного підприємства чи організації проектувальника.

Другий етап − це аналіз конкретних технологічних процесів і пошук внутрішніх резервів поліпшення використовуваних технологій.

На третьому етапі здійснюється:

а) аналіз товарних ринків за профілем продукції, що виготовляється підприємством, та ринків товарів-замінників;

б) оцінка перспектив розвитку ринків продукції підприємства;

в) прогнозування можливої специфіки необхідних технологічних процесів для випуску конкурентоспроможних товарів.

Четвертий етап присвячується переважно розробці технологічної стратегії розвитку підприємства.

На п'ятому етапі оперативно реалізуються плани технологічного розвитку підприємства в процесі здійснення ним виробничо-господарської діяльності.

Шостий етап є завершальним, на якому аналізуються результати практичної реалізації заходів щодо охорони техніко-технологічної складової фінансово-економічної безпеки.

12.2. Показники оцінки техніко-технологічної безпеки та заходи її забезпечення

Техніко-технологічну безпеку підприємства можна проаналізувати за допомогою **наступних показників:**

– фондовіддача

($Ф_В$ = Чиста виручка від реалізації продукції / Середньорічна вартість основних засобів);

– фондоозброєність праці

($Ф_О$ = Середньорічна вартість основних засобів / Середньооблікова чисельність персоналу);

– коефіцієнт оновлення

($К_О$ = Вартість придбаних у звітному періоді основних засобів / Вартість основних засобів на кінець звітного періоду);

– коефіцієнт зносу

($К_З$ = Сума зносу основних засобів / Первісна вартість основних засобів);

– коефіцієнт завантаження виробничих потужностей

($К_{ЗВП}$ = Обсяг виготовлення продукції х 100% / Максимально можлива потужність підприємства);

– коефіцієнт витрат на одиницю продукції

($В_{ОП}$ = Собівартість реалізованої продукції / Виручка від реалізації продукції);

– коефіцієнт виконання виробничої програми за обсягом

($К_{ВП}$ = Фактичний обсяг виготовленої продукції х 100% / Плановий обсяг виготовленої продукції);

– рентабельність виробництва

($Р_В$ = Прибуток від звичайної діяльності до оподаткування х 100% / (Середня вартість основних засобів + Вартість нормованих оборотних активів);

– коефіцієнт використання сировини

($К_{ВС}$ = (Вартість сировини – Вартість непридатної для переробки сировини) / Загальна вартість сировини);

– матеріаловіддача

($М_В$ = Чиста виручка від реалізації продукції / Загальна сума матеріальних витрат);

– коефіцієнт браку

(Бракована продукція / Загальний обсяг продукції·100);

– коефіцієнт повернень

(Величина поверненої продукції / Загальний обсяг продукції·100);

– коефіцієнт рекламацій

(Обсяг рекламацій / Загальний обсяг продукції·100);

– рівень прогресивності технологій

(К-сть використовуваних прогресивних сучасних технологій / Загальна к-сть технологій);

– рівень прогресивної продукції

(К-сть найменувань вироблених нових прогресивних видів продукції / Загальна к-сть найменувань продукції);

– рівень технологічного потенціалу

(К-сть технічних і технологічних рішень на рівні винаходів / Згальна к-сть нових рішень, використовуваних у виробничому процесі).

Заходи забезпечення техніко-технологічної безпеки:

– реконструкція та модернізація діючого обладнання;

– механізація та автоматизація виробничих процесів на основі більш прогресивної техніки та технології;

– перепрофілювання, будівництво цехів для виробництва нових видів продукції, виконання робіт, надання послуг;

– впровадження нових, ефективніших ресурсозберігаючих та екологічно безпечних технологій;

– фінансування НДДКР, спрямованих на пошук виробничо-технічних інновацій.

12.3. Поняття політико-правової безпеки підприємства

Політико-правова безпека – складова фінансово-економічної безпеки, яка полягає у правовому забезпеченні діяльності підприємства і дотриманні чинного законодавства.

Основними загрозами політико-правовій безпеці підприємства є:

Внутрішні:

– недостатня правова захищеність інтересів підприємства в договірній та іншій діловій документації;

– недостатнє фінансування юридичного забезпечення підприємницької діяльності;

– порушення юридичних прав підприємства та його працівників;

– низька кваліфікація працівників юридичної служби підприємства та помилки у підборі персоналу цієї служби;

– нестабільність системи оподаткування;

– непродумані норми внутрішнього розпорядку, посадові положення, інструкції, розпорядження, рішення трудового колективу.

Зовнішні негативні впливи мають подвійний характер:

1) політичний;

2) законодавчо-правовий.

До першої групи можна віднести: а) зіткнення інтересів суспільних груп (верств) населення з економічних, національних, релігійних та інших мотивів; б) військові конфлікти (дії); в) економічна й політична блокада, ембарго; г) фінансові та політичні кризи світового характеру.

У другій групі виокремлюють: а) здійснення власних політичних та інших цілей партіями (суспільними рухами), що перебувають при владі; б) зміна положень чинного законодавства з питань власності, господарського і трудового права, оподаткування; надмірні втручання держави у справи діяльності підприємств; відсутність правових гарантій у разі насильницького відчуження власності, заблокування рахунків підприємств тощо.

Показники, за допомогою яких можна оцінити стан політико-правової безпеки:

– коефіцієнт платіжної дисципліни

($К_{ПД}$ = (прибуток від операційної діяльності -штрафні санкції) / прибуток від операційної діяльності);

– коефіцієнт якості юридичних послуг

($К_{ЯЮП}$ = судові справи, виграні в суді, од. / загальна к-сть судових позовів, од.);

– ефективність правового забезпечення діяльності підприємства

($К_{ЕПЗ}$ = Сума збитків від неналежного юридичного оформлення господарської діяльності / Загальні витрати підприємства).

– питома вага судових справ у загальній сумі господарських договорів підприємства;

– питома вага одержаних і сплачених штрафних санкцій в загальній сумі зобов'язань за господарськими договорами підприємства (Кш).

Чим вище значення показників платіжної дисципліни, якості юридичних послуг та частки витрат на юридичне забезпечення діяльності підприємства в загальній структурі його виробничих витрат і чим нижче значення показників питомої ваги судових справ загальній сумі господарських договорів підприємства та питомої ваги одержаних і сплачених штрафних санкцій у загальній сумі зобов'язань за господарськими договорами підприємства, тим вище рівень політико-правової безпеки підприємства.

Загальний процес забезпечення політико-правової безпеки здійснюється за схемою, яка охоплює такі елементи (дії) організаційно-економічного спрямування:

1) аналіз загроз негативних впливів;

2) оцінка поточного рівня забезпечення;

3) планування комплексу заходів, спрямованих на підвищення цього рівня;

4) здійснення ресурсного планування;

5) планування роботи відповідних функціональних підрозділів підприємства;

6) оперативна реалізація запропонованого комплексу заходів щодо забезпечення належного рівня безпеки.

Передовсім детально аналізують загрози внутрішніх і зовнішніх негативних впливів на політико-правову безпеку та причини їх виникнення.

12.4. Сутність ринкової безпеки підприємства та показники

Ринкова складова фінансово-економічної безпеки підприємства – це захист від неефективно обраної моделі поведінки на ринку, помилок у товарній збутовій політиці, політиці ціноутворення, виготовлення неконкурентоспроможної продукції. Ця складова фінансово-економічної безпеки характеризує ступінь відповідності внутрішніх можливостей розвитку підприємства зовнішнім можливостям, які генеруються ринковим середовищем.

Про ослаблення ринкової безпеки свідчать:

– зменшення частки ринку, яку займає підприємство;

– ослаблення конкурентних позицій і спроможності протидіяти конкурентному тиску;

– зниження адаптаційних можливостей підприємства до змін ситуації на ринку, відставання від вимог ринку;

– нечесні дії конкурентів;

– рівень платоспроможності покупців;

– нестабільна політична ситуація в країні і світі;

– неузгоджена робота маркетологів, дизайнерів, конструкторів, економістів, фінансистів;

– низька якість виготовленої продукції%

– невчасне реагування на зміну кон’юнктури ринку;

– неефективна збутова мережа.

За ринкову складову безпеки на підприємстві має відповідати служба маркетингу. Ця складова відображає рівень відповідності внутрішніх виробничих можливостей підприємства зовнішнім, які формуються в ринковому середовищі, тобто наскільки науково-дослідна робота, виробнича і збутова діяльність відповідають запитам ринку і конкретним потребам споживачів.

Значимість ринкової безпеки полягає в тому, що вона відповідає за доведення виготовленої продукції до конкретного споживача. Відомо, що всі

зусилля з виробництва будуть зведені нанівець, якщо продукція не буде продана.

Що більше уваги приділяє підприємство вивченню навколишнього середовища, стежить за ним, аналізує всі зміни, то швидше можна передбачити небезпеку, вигідніше використати внутрішні можливості, прибутковіше вести бізнес.

Ринкова безпека підприємства характеризується наступними показниками:

– коефіцієнт ринкової віддачі активів:

$К_{РВА}$ = Чистий прибуток підприємства / Активи підприємства;

– частка підприємства на ринку

($Ч_Р$ = Обсяг продажу підприємства упродовж звітного періоду / Загальний обсяг продажу підприємств (за звітний період), що функціонують на ринку);

– конкурентоспроможність продукції

($К_П$ = Ціна виробу підприємства / Ціна еталонного виробу);

– темп приросту ринкової частки підприємства

($Т_{ПР}$ = Частка ринку підприємства у звітному періоді / Частка ринку підприємства у попередньому період);

– коефіцієнт ефективності рекламної політики підприємства

($К_{ЕРК}$ = Обсяг продажу продукції / сума рекламних витрат).

– ритмічність збуту продукції

($Р_{ЗБУТ}$ = 1- ((Плановий обсяг продажу продукції – Фактичний обсяг за той самий період) / Фактичний обсяг продажу).

ТЕМА 13
РИЗИКИ В СИСТЕМІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

13.1. Сутність та класифікація ризиків реалізації стратегії фінансово-економічної безпеки

13.2. Оцінка ризиків реалізації стратегії фінансово-економічної безпеки

13.3. Методи нівелювання ризиків реалізації стратегії фінансово-економічної безпеки підприємства

13.1. Сутність ризиків реалізації стратегії фінансово-економічної безпеки

Ризики реалізації стратегії фінансово-економічної безпеки виникають безпосередньо в процесі її реалізації, і їхня сутність полягає в ймовірності неправильного або невчасного виконання передбачених стратегією фінансово-економічної безпеки дій.

Ризики реалізації стратегії фінансово-економічної безпеки підприємства – це ймовірність того, що стратегічні дії, передбачені процесом реалізації, не забезпечать позитивного результату або й взагалі призведуть до негативних наслідків.

Помилки в реалізації стратегічних рішень – найбільш дороговартісні помилки діяльності підприємства.

Чим більший ризик реалізації стратегії фінансово-економічної безпеки, тим більша ймовірність невдач і пов’язаних з нею втрат.

Існування ризиків реалізації стратегії фінансово-економічної безпеки підприємства пояснюються такими умовами:

– відсутність досвіду менеджерів у прийнятті ефективних управлінських рішень щодо реалізації стратегії;

– достатньо тривалий період часу між формуванням стратегії і отриманим результатом від її реалізації;

– великий обсяг втрат від прийняття неправильних управлінських рішень;

– неможливість прогнозування розвитку науково-технічного прогресу та передбачення дій споживачів, змін кон’юнктури ринку, різні природні явища тощо;

– відсутність чітко визначених критеріїв оцінки ризиків реалізації стратегії та методів їх мінімізації;

– динамічність змін внутрішніх та зовнішніх умов розвитку економіки.

Класифікація ризиків реалізації стратегії фінансово-економічної безпеки підприємства:

1. За рівнем передбачуваності слід виділяти такі види ризиків:

– відомі – виникають в результаті конкретних дій або змін чинників, що впливають на процес реалізації стратегії фінансово-економічної безпеки;

– передбачувані – ризики, можливість появи яких передбачувана накопиченим досвідом діяльності підприємства;

– непередбачувані – ризики, можливість появи яких прогнозується відсутністю необхідної інформації.

2. За ступенем ризиконасиченості рішень доцільно виділяти такі види ризиків:

– несуттєві – ризики, наслідками яких є незначні відхилення у процесі реалізації стратегії та які повністю можна виправити без додаткових фінансових витрат і незначних зусиль;

– прийнятні – ризики, які вимагають здійснення окремих додаткових заходів на усунення відхилень та невеликих фінансових витрат;

– високі – ризики, що призводять до коригування всього процесу реалізації стратегії фінансово-економічної безпеки та великих втрат;

– руйнівні ризики – спричиняють крах реалізації стратегії фінансово-економічної безпеки та економічної системи підприємства загалом.

3. Ризикотвірні чинники – сутність процесів та явищ, що впливають на виникнення (зумовлюють виникнення) того чи іншого виду ризику й характеризують його. Отже, за ризикотвірними чинниками варто виділяти:

– об'єктивні ризики реалізації стратегії фінансово-економічної безпеки, які виникають під впливом тих чинників, які не залежать безпосередньо від підприємства та ОПР;

– суб'єктивні ризики – виникають під впливом внутрішніх чинників (виробничий потенціал підприємства, організація праці на підприємстві, технологічне забезпечення, рівень компетентності ОПР тощо).

4. За чисельністю осіб, що приймають рішення, виділяємо такі ризики реалізації стратегії фінансово-економічної безпеки:

– індивідуальні ризики – рішення приймає директор підприємства чи відповідальна особа;

– колективні ризики – рішення приймає рада директорів, збори акціонерів тощо.

5. За функціональними складовими фінансово-економічної безпеки розрізняємо ризики забезпечення фінансової безпеки, інтелектуально-кадрової безпеки, техніко-технологічної безпеки тощо.

6. За причинами невдалого забезпечення процесу реалізації стратегії фінансово-економічної безпеки підприємства виділяємо такі ризики:

– організаційні ризики – ризики, які викликані невідповідністю організаційних форм і систем організації діяльності підприємства до процесу реалізації стратегії;

– мотиваційні ризики – ймовірність неможливості залучення кваліфікованих працівників або відсутність зацікавленості працівників у результатах реалізації стратегії;

– фінансові ризики – ймовірність відсутності у підприємства власних та залучених коштів для фінансування процесу реалізації стратегії;

– інформаційні ризики – ймовірність несвоєчасного отримання детальної та достовірної інформації про всі процеси, пов'язані з реалізацією стратегії, або повної обмеженості інформації про наявні відхилення під час реалізації стратегії фінансово-економічної безпеки.

7. За частотою прояву виділяють такі ризики:

– періодичні – ризики, які виникають час від часу з конкретною частотою або без неї;

– постійні – ризики, які існують постійно, змінюючи лише свою величину або залишаються без змін.

13.2. Оцінка ризиків реалізації стратегії фінансово-економічної безпеки

Розрізняють якісну та кількісну оцінку ризиків.

Якісна оцінка ризиків полягає у виявленні та ідентифікації всіх можливих ризиків, визначенні причин їх виникнення та виділенні факторів, що впливають на інтенсивність негативного впливу. Важливим аспектом у процесі якісної оцінки ризику є виявлення можливих втрат ресурсів, які супроводжуються настанням ризикових подій.

Кількісна оцінка ризиків передбачає визначення числового значення ризику, дослідження тенденцій зміни за конкретний період та прогнозування його рівня на майбутнє.

Сьогодні широко використовують математичні моделі для оцінки ризику.

Залежно від характеру вихідної інформації та обраного способу описання невизначеності виділяють такі класи математичних моделей як детерміновані, стохастичні, лінгвістичні та нестохастичні (ігрові).

Детерміновані моделі застосовують тоді, коли причини та фактори ризику визначені. Для побудови таких моделей використовують класичні математичні методи аналізу, програмування, математичної логіки.

В стохастичних моделях, коли природа причин і факторів ризику випадкова, ризик описується розподілом ймовірностей на заданій множині. Необхідною передумовою для обґрунтованого використання стохастичних моделей є наявність статистично значимої інформації про попередні значення невизначеної змінної.

Лінгвістичні і нестохастичні моделі застосовують у тому випадку, коли природа причин ризику має нечіткий характер. У лінгвістичних моделях невизначеність описують вербально сформованою функцією належності на основі апарату нечіткої логіки. При побудові нестохастичних моделей задається множина окремих значень наслідків ризикової події, що може бути реалізована, при цьому використовуються методи стратегічних і статистичних ігор, теорії ймовірності тощо.

В тому випадку, коли не можна описати невизначеність і неможливо розрахувати ризик, ризикові рішення доречно приймати на основі *евристики,* тобто сукупності логічних прийомів і методичних правил знаходження істини.

13.3. Методи нівелювання ризиків реалізації стратегії фінансово-економічної безпеки підприємства

Повністю позбутися ризиків реалізації стратегії фінансово-економічної безпеки практично неможливо, проте цілком реально їх знівелювати або знизити.

Можна виділити такі групи заходів нівелювання ризиків реалізації стратегії фінансово-економічної безпеки підприємства:

1. Оптимізація ризику стратегії охоплює здійснення таких превентивних заходів: уникнення ризику, попередження ризику, розподіл ризику та лімітування ризику.

Уникнення ризику (ухилення від ризику) – передбачає здійснення процесу реалізації стратегії в такий спосіб, щоб якнайменше ризиків впливало на нього, або й взагалі відмовитися від певних дій, пов'язаних з ризиком. Уникнення ризику – найпростіший спосіб зниження ризику, в той же час він унеможливлює одержання запланованого результату.

Попередження ризику (запобігання втратам) – здійснення заходів, які сприяють зведенню до мінімуму ймовірність частини втрат. Попередження ризику пов'язане з розробленням і впровадженням програми превентивних заходів, виконання яких слід контролювати і періодично уточнювати з урахуванням змін, що відбулися. Використання цього методу доцільне лише в тому випадку, коли ймовірність реалізації ризику досить велика та прогнозовані витрати на реалізацію превентивних заходів менші, ніж втрати, спричинені ризиком.

Розподіл (дисипація) ризику – залучення до впровадження дій стосовно реалізації стратегії інших суб'єктів господарювання, кожен із них у випадку невдачі понесе втрати пропорційно до своєї участі та внеску.

Лімітування ризику – встановлення внутрішніх фінансових нормативів (максимальний обсяг товарного кредиту, максимальний період залучення засобів в дебіторській заборгованості тощо), що будуть враховуватись у процесі реалізації стратегії.

2. Фінансування наслідків ризику – забезпечення економічної можливості компенсацій матеріальних збитків, які виникли внаслідок несприятливих випадкових подій (втрати майна, відповідальності за зобов'язання, фінансових втрат, збитків, завданих персоналу, відповідальності за збитки, завдані третім особам тощо). Фінансування наслідків ризику реалізації стратегії фінансово-економічної безпеки передбачає компенсацію ймовірних втрат і збитків у процесі реалізації, використовуючи такі заходи: покриття ризику, страхування ризику, нестрахове передавання ризику.

Покриття ризику – формування грошових резервів на покриття непередбачуваних витрат у процесі реалізації стратегії фінансово-економічної безпеки. Покриття ризику може бути як запланованим, так і незапланованим. При запланованому покритті ризику вдаються до самострахування, тобто створюють власні резервні фонди усередині самого підприємства – так звані фонди самострахування. При незапланованому покритті ризику втрати покриваються із залишків ресурсів.

Страхування ризику (передавання ризику) – договірне передавання відповідальності за всеможливі ризики в процесі реалізації стратегії та відшкодування всіх чи частини збитків за рахунок створених страховою організацією грошових фондів. Цей метод нівелювання ризику доречно

застосовувати в тому випадку, коли ймовірність реалізації ризику невисока, проте може призвести до значних втрат.

Нестрахове передавання ризику – передавання ризику третій особі, тобто передавання діяльності, пов'язаної з ризиком, або фінансової відповідальності за втрати, зумовлені ним.

3. Запобігання ризику передбачає такі заходи: здобуття додаткової інформації, витіснення ризику.

Здобуття додаткової інформації – збільшення витрат ресурсів та часу на отримання додаткової інформації про чинники зовнішнього та внутрішнього середовищ, які пов'язані з реалізацією стратегії, яка дозволяє знизити ризик та зменшити можливі збитки.

Витіснення ризику – виконання дій щодо реалізації стратегії з одночасним активним впливом підприємства на джерела ризику.

Отже, використання вищезазначених методів нівелювання ризику залежно від створеної ситуації щодо реалізації стратегії дасть можливість підприємствам мінімізувати ризики та сприятиме досягненню бажаного результату.

Список літератури

1. Закон України “Про інформацію” № 2657-XII від 02.10.1992 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
2. Закон України «Про охоронну діяльність» №4616-VI від 22.03.2012 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
3. Постанова КМУ від 18.11.2015 року №960 «Про затвердження ліцензійних умов, які визначають організаційні, кадрові та технологічні вимоги провадження охоронної діяльності» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
4. Гапоненко В. Ф. Экономическая безопасность предприятий. Подходы и принципы / В. Ф. Гапоненко, А. Л. Беспалько, А. С. Власков. – М. : Изд-во «Ось-89», 2007. – 208 с.
5. Гончаренко Л. П. Управление безопасностью : учеб. пособ. / Л. П. Гончаренко. – М. : КНОРУС, 2010. – 272 с.
6. Довбня С. Б. Діагностика рівня економічної безпеки підприємства / С. Б. Довбня, Н. Ю. Гічова // Фінанси підприємств. – 2008. – № 4. – С. 88–97.
7. Долженков О. Ф. Особливості гарантування економічної безпеки підприємницької діяльності в ринкових умовах : монографія / О. Ф. Долженков, Ж. О. Жуковська, О. М. Головченко. – Одеса : ОЮІ ХНУВС, 2007. – 208 с.
8. Донець Л. І. Економічна безпека підприємства : навч. посіб. [для студ. вищ. навч. закл.] / Л. І. Донець, Н. В. Ващенко. – К. : Центр уч. л-ри, 2008. – 240 с.
9. Економічна безпека підприємств, організацій та установ : навч. посіб. / [В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін.]. – К. : Правова єдність, 2009. – 544 с.
10. Заїнчковський А. О. Економічна безпека підприємства : навч. посіб. [для студ. вищ. навч. закл.] / А. О. Заїнчковський, Т. М. Іванюта. – К. : Центр уч. л-ри, 2009. – 256 с.
11. Зацеркляний М. М. Основи економічної безпеки : навч. посіб. / М. М. Зацеркляний, О. Ф. Мельников. – К. : КНТ, 2009. – 337 с.
12. Ильяшенко С. Н. Составляющие экономической безопасности предприятия и подходы к их оценке / С. Н. Ильяшенко // Актуальні проблеми економіки. – 2003. – № 3. – С. 12–19.
13. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. / М. І. Камлик. – К. : Атіка, 2005. – 432 с.
14. Картузов Є. П. Визначення фінансової безпеки підприємства: поняття, зміст, значення і функціональні аспекти / Є. П. Картузов // Актуальні проблеми економіки. – 2012. – № 8 (134). – С. 172–181.
15. Кіндрацька Г. І. Стратегічний менеджмент : навч. посіб. / Кіндрацька Г. І. – [2-ге вид., переробл. і доповн.]. – Л. : В-во Львівської політехніки, 2010. – 406 с.
16. Ковальов Д. Економічна безпека підприємства / Д. Ковальов, Т. Сухорукова // Економіка України. – 1998. – № 10. – С.48–52.

17. Ковальов Д. Кількісна оцінка рівня економічної безпеки підприємства / Д. Ковальов, І. Плєтникова // Економіка України. – 2001. – № 4. – С. 35–40.
18. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения : монографія / А. В. Козаченко, В. П. Пономарев, А. Н. Ляшенко. – К. : Либра, 2003. – 280 с.
19. Куркін М. В. Контроль та захист економічної безпеки діяльності підприємств : навч. посіб. / Куркін М. В., Понікаров В. Д., Назаренко Д. В. – Х. ; ФОП Павленко О. Г.; ВД «ІНЖЕК», 2010. – 300 с.
20. Моделювання економічної безпеки: держава, регіон, підприємство : монографія / [Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. та ін.] ; за ред. Гейця В. М. – Х. : ВД «ІНЖЕК», 2006. – 240 с.
21. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства : навч. посіб. / І. П. Мойсеєнко, О. М. Марченко. – Львів : ЛДУВС, 2011. – 380 с.
22. Нємцов В. Д. Стратегічний менеджмент : навч. посіб. [для студ. вищ. навч. закл.] / В. Д. Нємцов, Л. С. Довгань. – К. : ЕксОб, 2004. – 560 с.
23. Омелянович Л. О. Економічна безпека торговельного підприємства : монографія / Л. О. Омелянович, Г. Є. Долматова. – Донецьк : ДонДУЕТ, 2005. – 195 с.
24. Орлик О. В. Концептуальні основи стратегії забезпечення фінансово-економічної безпеки підприємства / О. В. Орлик // Сталий розвиток економіки. – 2016. – № 1(30). – С. 67–73.
25. Основи економічної безпеки : підруч. / О. М. Бандурка, В. Є. Духов, К. Я. Петрова, І. М. Черняков. – Київ : Вид-во нац. ун-ту внутр. справ, 2003. – 236 с.
26. Основы экономической безопасности (Государство, регион, предприятие, личность) / [под ред. Е. А. Олейникова]. – М. : ЗАО «Бизнес-школа «Интел-Синтез», 1997. – 288 с.
27. Подольчак Н. Ю. Організація та управління системою фінансово-економічної безпеки підприємства / Н. Ю. Подольчак, В. Я. Карковська. – Львів : Вид-во НУ «Львівська політехніка», 2014. – 268 с.
28. Система економічної безпеки: держава, регіон, підприємство / монографія в 3 т. Т. 1 / [Г. В. Козаченко, О. М. Ляшенко, Ю. С. Погорелов та ін.] ; за заг. ред. Г. В. Козаченко. – Луганськ : Елтон-2, 2010. – 282 с.
29. Фоміна М. В. Проблеми економічно безпечного розвитку підприємства: теорія і практика : монографія / М. В. Фоміна. – Донецьк : ДонДУЕТ, 2005. – 140 с.
30. Франчук В. І. Основи економічної безпеки : навч. посіб. / Франчук В. І. – Львів : «Каменяр», 2008. – 203 с.

Основна література для студентів

1. Економічна безпека підприємств, організацій та установ : навч. посіб. / [В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін.]. – К. : Правова єдність, 2009. – 544 с.
2. Заїнчковський А. О. Економічна безпека підприємства : навч. посіб. [для студ. вищ. навч. закл.] / А. О. Заїнчковський, Т. М. Іванюта. – К. : Центр уч. л-ри, 2009. – 256 с.
3. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. / М. І. Камлик. – К. : Атіка, 2005. – 432 с.
4. Куркін М. В. Контроль та захист економічної безпеки діяльності підприємств : навч. посіб. / М. В. Куркін, В. Д. Понікаров, Д. В. Назаренко. – Х. ; ФОП Павленко О. Г.; ВД «ІНЖЕК», 2010. – 300 с.
5. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства : навч. посіб. / І. П. Мойсеєнко, О. М. Марченко. – Львів : Львів. держ. ун-т вн. справ , 2011. – 380 с.
6. Подольчак Н. Ю. Організація та управління системою фінансово-економічної безпеки підприємства / Н. Ю. Подольчак, В. Я. Карковська. – Львів : Вид-во НУ «Львівська політехніка», 2014. – 268 с.
7. Управління фінансово-економічною безпекою : навч. посіб. / [Кириченко О. А., Лаптєв С. М., Пригунов П. Я., Захаров О. І. та ін.]. – К. : Дорадо-Друк, 2010. – 480 с.
8. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / [Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В.] ; [за ред. Т. Г. Васильціва]. – Львів : ВИДАВНИЦТВО, 2012. – 386 с.

Додаткова література для студентів

1. Господарський кодекс України від 21.10.2004 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
2. Кримінальний кодекс України №2341-ІІІ від 05.04.2001 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
3. Цивільний кодекс України № 435-IV від 16.01.2003 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
4. Андрощук Г. А. Экономическая безопасность предприятия: защита комерческой тайны : монография / Г. А. Андрощук, П. П. Крайнев. – К. : Ін Юре, 2000. – 398 с.
5. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия : монография / В. А. Игнатьев. – Старый Оскол : ООО «ТНТ», 2005. – 448 с.
6. Кузнецов О. О. Захист інформації та економічна безпека підприємства : монографія / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Х. : ХНЕУ, 2008. – 360 с.
7. Логвиненко М. І. Організація і управління майновою та особистою безпекою підприємця : навч. посіб. / М. І. Логвиненко, А. М. Кривошеєв. – Суми : Видавець Наталуха А.С., 2012. – 176 с.

8. Садердинов А. А. Информационная безопасность предприятия : учеб. пособ. / Садердинов А. А., Трайнев В. А., Федулов А. А. – М. : ИТК «Дашков и К°», 2005. – 336 с.
9. Скорук О. В. Економіко-математичне моделювання у реалізації стратегії економічної безпеки підприємства / О. В. Скорук // Науковий вісник Херсонського державного університету. Серія «Економічні науки». – 2016. – № 16/2016. – С. 70–72.
10. Скорук О. В. Реалізація стратегії економічної безпеки підприємства [Електронний ресурс] / О. В. Скорук // Глобальні та національні проблеми економіки. – 2016. – Вип. 11. – С. 498–503. – Режим доступу до журналу : http://global-national.in.ua/issue-11-2016.
11. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2. – Т.2. – С. 32–35.

Короткий термінологічний словник

Безпека	– це відсутність загрози, збереженість, надійність, тобто відсутність будь-яких загроз особі, суспільству і державі (об'єктам безпеки) (за тлумачним словником В.Даля)
Безпека	– стан захищеності життєво важливих інтересів особи, суспільства, організації від потенційно і реально існуючих загроз або відсутність таких загроз
Економічна загроза підприємства	– реальна негативна дія чинників зовнішнього та внутрішнього середовищ, за якої відбуваються небажані зміни стану фінансово-економічної безпеки
Економічна небезпека підприємства	– деструктивний вплив негативних чинників на діяльність підприємства, що може призвести до його занепаду чи банкрутства
Економічний ризик підприємства	– можливість настання негативних подій, явищ, процесів чи несприятливих умов зовнішнього та внутрішнього середовищ, що можуть призвести до непередбачуваних негативних наслідків у процесі діяльності підприємства, до зниження фінансово-економічної безпеки
Загрози інтелектуально-кадровій безпеці підприємства	– існуючі або потенційні суперечності, що ускладнюють або унеможливлюють реалізацію пріоритетних інтересів за рахунок використання інтелектуально-кадрового ресурсу
Інтелектуально-кадрова безпека	– це здатність підприємства запобігати ризикам і загрозам організації праці, безпосередньо персоналу, його трудовому та інтелектуальному потенціалу, трудовим відносинам в цілому
Інтереси підприємства	– усвідомлені, матеріалізовані та конкретизовані керівництвом потреби підприємства (збільшення обсягу продажу продукції, завоювання ринкової ніші, покращення іміджу підприємства тощо)
Інформаційна безпека підприємства	– це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні
Комерційна таємниця	– інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою і не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію (згідно зі ст. 505 ЦК України)
Лояльність персоналу	– це доброзичливе, коректне, щире ставлення до керівництва, працівників, інших осіб, їх дій, до підприємства в цілому; свідоме виконання працівниками своєї роботи відповідно до цілей і завдань в інтересах підприємства, а також дотримання норм, правил і зобов'язань відносно підприємства, керівництва, працівників та інших суб'єктів взаємодії
Майнові права інтелектуальної власності на комерційну таємницю	– право на використання комерційної таємниці; – виключне право дозволяти використання комерційної таємниці; – виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці; – інші майнові права інтелектуальної власності, встановлені законом (ст. 506 Цивільного кодексу)

Механізм забезпечення фінансово-економічної безпеки	– це сукупність законодавчих актів, правових норм, рушійних мотивів та стимулів, методів, засобів та заходів для ефективного функціонування системи фінансово-економічної безпеки підприємства
Механізм реалізації стратегії фінансово-економічної безпеки	– це сукупність методів та інструментів, властивих стратегічному управлінню підприємством, які використовуються для реалізації функцій механізму в умовах динамічних змін зовнішнього та внутрішнього середовищ функціонування підприємства
Моніторинг реалізації стратегії фінансово-економічної безпеки	– це безперервний процес збору, обробки й аналізу інформації про перебіг реалізації стратегії, аналіз відхилень у реалізації стратегії та їх причин, розроблення програм дій на нівелювання негативних відхилень
Надійність персоналу (працівників)	– властивість людини зберігати здатність здійснювати професійну діяльність у повному обсязі з необхідною якістю протягом необхідного проміжку часу, в тому числі в екстремальних ситуаціях
Ознаки комерційної таємниці	– інформація, що становить комерційну таємницю має комерційну цінність; – інформація, що становить комерційну таємницю, не відома іншим особам та відсутній вільний доступ до неї на законних підставах; – вжито заходів для охорони конфіденційної інформації
Організація управління системою фінансово-економічної безпеки підприємства	– формування його організаційної структури (визначення складу суб'єктів управління та їхніх взаємозв'язків) та розподіл завдань, повноважень, відповідальності між окремими ланками управління
Політико-правова безпека	– складова фінансово-економічної безпеки, яка полягає у правовому забезпеченні діяльності підприємства і дотриманні чинного законодавства
Реалізація стратегії фінансово-економічної безпеки	– сукупність управлінських дій, які пов'язані з послідовним виконанням усіх етапів стратегічного плану, розподілом обов'язків, відповідальності, створенням необхідного ресурсного, нормативно-правового, інформаційного та організаційного забезпечення, необхідною координацією зусиль усіх підрозділів підприємства
Ризики реалізації стратегії фінансово-економічної безпеки підприємства	– це ймовірність того, що стратегічні дії, передбачені процесом реалізації, не забезпечать позитивного результату або й взагалі призведуть до негативних наслідків
Ринкова складова фінансово-економічної безпеки підприємства	– це захист від неефективно обраної моделі поведінки на ринку, помилок у товарній збутовій політиці, політиці ціноутворення, виготовлення неконкурентоспроможної продукції

Силова безпека підприємства	– характеризує захищеність інтересів підприємства від негативних фізичних впливів. Вона включає: а) забезпечення фізичної безпеки (життя і здоров'я) працівників та керівника підприємства; б) забезпечення захисту майна підприємства від негативних впливів, які можуть призвести до втрати цього майна або зниження його вартості; в) забезпечення силових аспектів інформаційної безпеки підприємства.
Система фінансово-економічної безпеки підприємства	– це організована сукупність засобів, методів, організаційно-управлінських, режимних, технічних, профілактичних та інших заходів, спрямованих на реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх негативних чинників і досягнення цілей діяльності
Служба фінансово-економічної безпеки підприємства	– це штатний структурний підрозділ підприємства, який підпорядковується безпосередньо його керівникові (власнику) і організовує у взаємодії з іншими структурними підрозділами (а також за необхідності, органами державної влади та управління, іншими зовнішніми суб'єктами) розроблення, реалізацію та контроль виконання заходів щодо захисту життєво важливих інтересів підприємства від зовнішніх і внутрішніх загроз
Стратегія фінансово-економічної безпеки підприємства	– це обґрунтована система послідовних дій і заходів, орієнтованих на досягнення поставленої мети, спосіб досягнення встановлених цілей забезпечення фінансово-економічної безпеки з урахуванням тенденції зміни її рівня
Суб'єкт охоронної діяльності	– суб'єкт господарювання будь-якої форми власності, створений та зареєстрований на території України, що здійснює охоронну діяльність на підставі отриманої у встановленому порядку ліцензії
Суб'єкти системи фінансово-економічної безпеки	– ті особи, підрозділи, служби, органи, установи, які безпосередньо займаються забезпеченням безпеки
Техніко-технологічна безпека	– це складова фінансово-економічної безпеки, пріоритетним завданням якої є захист від негативних чинників з метою створення та найбільш ефективного використання технічної бази та технологічних процесів для забезпечення високого рівня конкурентоспроможності підприємства
Фінансова безпека підприємства	– це здатність підприємства ефективно і стабільно здійснювати свою господарську, в т.ч. й фінансову діяльність, шляхом використання сукупності взаємопов'язаних діагностичних, інструментальних та контрольних заходів фінансового характеру, які повинні оптимізувати використання фінансових ресурсів, забезпечити належний їх рівень та нівелювати вплив ризиків внутрішнього та зовнішнього середовищ
Фінансово-економічна безпека підприємства	– стан захищеності життєво важливих інтересів підприємства від різноманітних внутрішніх та зовнішніх негативних чинників, що гарантує найбільш ефективне використання корпоративних ресурсів підприємства для забезпечення стабільного функціонування та динамічного розвитку
Функціональні складові фінансово-економічної безпеки підприємства	– це сукупність основних напрямів його фінансово-економічної безпеки, кожна з яких характеризується власним змістом, набором функціональних критеріїв і способом забезпечення

Навчальне видання

Скорук Олена Володимирівна

Фінансово-економічна безпека виробничого підприємства

Конспект лекцій

Друкується в авторській редакції

Підп. до друку 2017 р. Формат 60х84/16
Папір офс. Гарн. Times New Roman. Ум. друк. арк. 1,3.
Обл.-вид.арк. 1,0. накладом 50 прим.
Друк ПП «Поліграфія»