20
РОКІВ

ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Львівський державний університет внутрішніх справ

Наталія Шевченко
Марта Копитко

Менеджмент безпеки організації

Навчальний посібник

Львів
2025

УДК 658.012.8:005.934
Ш 37

Рекомендовано до друку та розміщення в електронних сервісах ЛьвДУВС
Вченою радою Львівського державного університету внутрішніх справ
(протокол від 25 листопада 2025 року № 5)

Р е ц е н з е н т и:

АЛЬКЕМА Віктор Григорович – доктор економічних наук, професор
(Університет економіки та права «КРОК»);

МИСЬКІВ Галина Василівна – доктор економічних наук, професор
(Національний університет «Львівська політехніка»).

Шевченко Н. В., Копитко М. І.

Ш 37 Менеджмент безпеки організації : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2025. 324 с.

ISBN 978-617-511-436-0

Розглянуто та охарактеризовано економічну, кадрову, інформаційну, екологічну, кредитну та фінансову безпеку організації. Визначено механізми їх забезпечення в системі управління організаціями. Висвітлено актуальні питання сутності, видів і напрямів управління безпековими аспектами діяльності сучасних організацій.

Для здобувачів вищої освіти економічних спеціальностей, аспірантів, викладачів, практичних працівників підприємств, установ та організацій, а також керівників, які враховують безпекові аспекти у процесі прийняття управлінських рішень.

The economic, personnel, information, environmental, credit, and financial security of an organization are considered and characterized. Mechanisms for ensuring them in the organizational management system are identified. Current issues concerning the essence, types, and directions of managing the security aspects of modern organizations are highlighted.

The manual is intended for students of economic specialties, graduate students, teachers, practitioners of enterprises, institutions, and organizations, as well as managers who take security aspects into account in the process of making management decisions.

УДК 658.012.8:005.934

ISBN 978-617-511-436-0

ЗМІСТ

ПЕРЕДМОВА....9

ТЕМА 1
ТЕОРЕТИЧНІ ОСНОВИ МЕНЕДЖМЕНТУ БЕЗПЕКИ ОРГАНІЗАЦІЇ....11

1.1. Сутність понять «безпека», «безпека організації» та «менеджмент безпеки організації»....11
1.2. Принципи, суб'єкти, об'єкти, функції менеджменту безпеки організації....19
1.3. Основні завдання забезпечення безпеки організації....26
1.4. Основи управління економічною безпекою організації....29
Питання для самоконтролю....34
Тестові завдання....35

ТЕМА 2
ФОРМУВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ БЕЗПЕКИ ОРГАНІЗАЦІЇ....37

2.1. Сутність системи менеджменту безпеки організації....37
2.2. Етапи формування системи менеджменту безпеки....44
2.3. Напрями та методи оцінки безпеки організації....48
Питання для самоконтролю....57
Тестові завдання....58
Практичні завдання....60

ТЕМА 3
УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ....62

3.1. Сутність управління фінансовою безпекою організації....62
3.2. Методичні підходи до оцінки фінансового стану та її показники....69
3.3. Інформаційне забезпечення фінансової безпеки підприємства....77
3.4. Чинники забезпечення фінансової безпеки організації....80
Питання для самоконтролю....85
Тестові завдання....86
Практичні завдання....87

ТЕМА 4
МЕНЕДЖМЕНТ КРЕДИТНОЇ БЕЗПЕКИ.....89

4.1. Складові та сутність управління кредитною безпекою організації.....89
4.2. Види кредитних загроз та управління ними.....97
4.3. Оцінка рівня кредитної безпеки банківських установ.....103
4.4. Оцінка рівня кредитоспроможності позичальника в системі фінансово-кредитної безпеки.....106
Питання для самоконтролю.....112
Тестові завдання.....113
Практичні завдання.....114

ТЕМА 5
УПРАВЛІННЯ ІНВЕСТИЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ.....117

5.1. Сутність та складові інвестиційної безпеки.....117
5.2. Емісійна та дивідендна політика в системі інвестиційної безпеки.....123
5.3. Напрями оцінки інвестиційної безпеки організації.....128
5.4. Роль фінансових посередників у забезпеченні інвестиційної безпеки організації.....132
Питання для самоконтролю.....136
Тестові завдання.....137
Практичні завдання.....139

ТЕМА 6
СИСТЕМА КОРПОРАТИВНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ.....141

6.1. Сутність, функції та принципи корпоративної безпеки.....141
6.2. Рівні корпоративної безпеки організації.....146
6.3. Фактори впливу на корпоративну безпеку організації.....150
6.4. Структура системи корпоративної безпеки організації.....157
Питання для самоконтролю.....164
Тестові завдання.....164
Практичні завдання.....166

ТЕМА 7
МЕНЕДЖМЕНТ КАДРОВОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ.....168

7.1. Сутність кадрової безпеки організації та її аспекти.....168
7.2. Складові управління кадровою безпекою організації.....178
7.3. Напрями збереження кадрової безпеки: вітчизняний та світовий досвід.....185

Питання для самоконтролю.....191
Тестові завдання.....191
Практичні завдання.....193

ТЕМА 8
ІНФОРМАЦІЙНА БЕЗПЕКА В СТРУКТУРІ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ.....195

8.1. Сутність інформаційної безпеки організації.....195
8.2. Види і принципи інформаційної безпеки.....201
8.3. Джерела загроз інформаційній безпеці організації.....207
8.4. Напрями запобігання інформаційним ризикам в організації та управління ними.....213
Питання для самоконтролю.....221
Тестові завдання.....222
Практичні завдання.....224

ТЕМА 9
МЕНЕДЖМЕНТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ.....226

9.1. Сутність екологічної безпеки та її місце в системі корпоративної безпеки.....226
9.2. Складові системи екологічної безпеки організації.....233
9.3. Інструменти та стратегія менеджменту екологічної безпеки.....239
Питання для самоконтролю.....244
Тестові завдання.....244
Практичні завдання.....246

ТЕМА 10
ОЦІНКА ЕФЕКТИВНОСТІ МЕНЕДЖМЕНТУ БЕЗПЕКИ ОРГАНІЗАЦІЇ.....248

10.1. Сутність оцінки ефективності менеджменту безпеки організації.....248
10.2. Методи, підходи та інструменти оцінки ефективності менеджменту безпеки організації.....253
10.3. Напрями удосконалення системи оцінки ефективності менеджменту безпеки організації.....259
Питання для самоконтролю.....264
Тестові завдання.....264
Практичні завдання.....266

ТЕМА 11
ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ БЕЗПЕКИ ОРГАНІЗАЦІЇ.....268
11.1. Нормативно-правова база забезпечення безпеки організацій.....268
11.2. Організаційна структура управління безпекою та її правове регламентування.....273
Питання для самоконтролю.....277
Тестові завдання.....278

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....281

ДОДАТКИ.....290

ПЕРЕДМОВА

У сучасних умовах глобалізації, цифровізації та загострення конкурентної боротьби особливого значення набуває забезпечення комплексної безпеки організації. Ефективна діяльність підприємств, установ, організацій неможлива без належного управління ризиками, загрозами та небезпеками, що можуть впливати на їхню стабільність, фінансову стійкість і конкурентоспроможність. Саме тому формування системи менеджменту безпеки організації стає однією з базових умов стратегічного розвитку бізнесу.

З огляду на динамічність зовнішнього середовища та внутрішні ускладнення функціонування підприємств, неабияк важливо нині здійснити визначення теоретичних основ та практичних інструментів управління безпекою. Це, зокрема, передбачає аналіз ризиків, розробку політики безпеки, забезпечення фінансової стійкості, захист ресурсів і персоналу, створення антикризових програм і системи реагування на надзвичайні ситуації.

Навчальний посібник «Менеджмент безпеки організації» підготовлено відповідно до вимог програми обов'язкової навчальної дисципліни для здобувачів вищої освіти ступеня «бакалавр» освітньо-професійної програми «Менеджмент та безпека бізнесу». Структура посібника передбачає подання таких матеріалів: теоретичні основи менеджменту безпеки організації та формування його системи (теми 1 і 2), управління фінансовою безпекою (тема 3), вивчення особливостей менеджменту кредитної та інвестиційної безпеки (теми 4 і 5), дослідження системи корпоративної і кадрової безпеки організації (теми 6 і 7), визначення системи інформаційної безпеки в структурі діяльності підприємства (тема 8) та екологічної безпеки (тема 9), а також оцінка ефективності менеджменту безпеки організації (тема 10) та організаційно-правове забезпечення системи безпеки організації (тема 11).

Метою викладання дисципліни «Менеджмент безпеки організації» є формування у здобувачів вищої освіти системи теоретичних знань і практичних навичок

щодо управління безпековими аспектами діяльності сучасних організацій, опанування методів ідентифікації ризиків, розробки заходів протидії загрозам, а також уміння приймати ефективні управлінські рішення в умовах невизначеності.

За результатами роботи з матеріалом, поданим у навчальному посібнику, користувачі зможуть:

– ознайомитися з основними поняттями та визначеннями у сфері менеджменту безпеки організації;

– розкрити сутність, функції та принципи управління безпекою на підприємствах, в організаціях;

– оволодіти методами аналізу ризиків і загроз економічній, інформаційній, кредитній, інвестиційній, кадровій та іншим підсистемам організацій;

– визначити напрями формування комплексної системи безпеки;

– навчитися застосовувати інструменти прогнозування, планування та контролю у сфері безпеки;

– розробляти антикризові стратегії та програми забезпечення стабільного розвитку підприємства;

– приймати управлінські рішення з урахуванням безпекових факторів.

Важливою перевагою навчального посібника «Менеджмент безпеки організації» є подання матеріалів у доступній формі, з використанням схем, таблиць та визначень основних понять, термінів. Питання для самоконтролю, тестові та практичні завдання після кожної теми сприятимуть закріпленню знань і формуванню практичних умінь.

Видання буде корисним для здобувачів вищої освіти економічних та управлінських спеціальностей, викладачів, аспірантів, керівників і фахівців підприємств, установ, організацій, які у своїй діяльності стикаються з необхідністю управління безпековими аспектами.

ТЕМА 1
ТЕОРЕТИЧНІ ОСНОВИ МЕНЕДЖМЕНТУ БЕЗПЕКИ ОРГАНІЗАЦІЇ

1.1. Сутність понять «безпека», «безпека організації» та «менеджмент безпеки організації»

1.2. Принципи, суб'єкти, об'єкти, функції менеджменту безпеки організації

1.3. Основні завдання забезпечення безпеки організації

1.4. Основи управління економічною безпекою організації

Основні поняття і терміни: безпека, безпека організації, менеджмент, менеджмент безпеки організації, управління, підприємство, організація, економічна безпека, фактори впливу, загрози, ризики, небезпека, ризик-менеджмент, ризикове середовище, чинники впливу.

1.1. Сутність понять «безпека», «безпека організації» та «менеджмент безпеки організації»

У сучасних умовах глобальних змін, цифрової трансформації та високої конкуренції питання комплексної безпеки організацій виходить на перший план. Жодне підприємство не може ефективно функціонувати без налагодженого процесу управління ризиками та загрозами, які здатні вплинути на його фінансову стійкість, репутацію та стратегічний розвиток. Побудова дієвої системи менеджменту безпеки забезпечує захист ресурсів, стабільність бізнес-процесів та підвищує рівень конкурентоспроможності організації на ринку.

Зростаюча складність зовнішніх та внутрішніх чинників діяльності підприємств вимагає глибокого розуміння теоретичних засад і практичних механізмів управління безпекою. Це передбачає проведення оцінки ризиків, розроблення політики безпеки, створення ефективних програм протидії загрозам, підтримання інформаційної та фінансової стійкості,

а також впровадження антикризових стратегій та заходів оперативного реагування на непередбачувані ситуації.

У сучасній економічній літературі існує значна кількість трактувань поняття «безпека» (табл. 1.1).

Таблиця 1.1

Підходи до трактування поняття «безпека»

Автор (джерело)	**Визначення поняття**
1	*2*
Г. Назарова, А. Дем'яненко	Безпека – це стан, у якому система або суб'єкт перебувають у захищеності від реальних чи потенційних загроз, що забезпечує збереження їх функцій і життєво важливих інтересів.
В. Тихий	Безпека – це суб'єктивне та об'єктивне відчуття людини, що створює умови відсутності небезпеки, тобто коли для особи або об'єкта не існують загрози, що можуть завдати шкоди.
О. Павленко	Безпека – це здатність соціальної або правової системи забезпечувати захищеність основних засад суспільного устрою та державного ладу від зовнішніх і внутрішніх загроз.
Б. Бузан	Безпека – це властивість об'єкта або процесу зберігати функціональність у середовищі зовнішніх та внутрішніх викликів, підтримуючи баланс між ризиками та ресурсами наявних засобів захисту.
В. Тихий	Безпека – це стан захищеності людини, суспільства чи держави, який передбачає мінімізацію загроз і можливостей матеріальної або нематеріальної шкоди.
М. Степаненко	Безпека – це комплекс соціально-правових, організаційних та управлінських заходів, що мають на меті попередження, виявлення і нейтралізацію загроз, здатних порушити функціонування систем або забезпечення їх сталого розвитку.
Н. Пряхіна	Безпека – це стан, у якому збережено основні характеристики і параметри системи, що дозволяє їй адаптуватись до змін зовнішнього середовища без втрат функціональності.
С. Гордієнко	Безпека – це стан захищеності конкретного соціального об'єкта (особи, суспільства, держави), коли встановлено певні гарантії проти негативного зовнішнього чи внутрішнього впливу.
І. Корж	Безпека – це відсутність загроз або небезпеки, яка б могла порушити нормальний стан або функціонування об'єкта, або коли існують такі загрози – наявні засоби їх усунення або мінімізації.

Завершення табл. 1.1

1	*2*
В. Дуга	Безпека – це стан стабільності або динамічної рівноваги системи, за якого ключові її параметри підтримуються в допустимих межах попри дію зовнішніх чи внутрішніх факторів.
С. Верещак	Безпека – це стан, коли для суб'єкта або об'єкта не існує загрози і збережено життєво важливі умови для нормальної діяльності, розвитку чи функціонування.

Отже, **безпека** – це стан захищеності особи, суспільства або організації від внутрішніх і зовнішніх загроз, який забезпечує стабільне функціонування, розвиток і збереження життєво важливих інтересів. У контексті діяльності підприємства безпека охоплює комплекс організаційних, технічних, правових і соціально-економічних заходів, спрямованих на мінімізацію ризиків, запобігання збиткам і підтримання стабільності бізнес-процесів.

Ризик відображає невизначеність зовнішнього і внутрішнього середовища, а також необхідність прийняття управлінських рішень, спрямованих на ідентифікацію, оцінювання, попередження чи використання потенційних загроз та шансів для забезпечення стабільного розвитку системи.

Безпека у широкому значенні трактується як відсутність небезпек, стан надійності та збереження цілісності. Термін «убезпечувати» означає здійснювати заходи для запобігання загрозам та створювати умови, які унеможливлюють виникнення небезпечних ситуацій.

У буквальному сенсі безпека розуміється як повна відсутність будь-яких ризиків або загроз. Проте у реальному середовищі досягти абсолютної безпеки практично неможливо, оскільки зовнішні та внутрішні фактори постійно змінюються. Саме тому сучасне тлумачення цього поняття виходить за межі простої відсутності небезпеки та включає активні заходи зі захисту, збереження стабільності й адаптації до змін (рис. 1.1).

На ринку поняття безпеки охоплює не лише фізичний чи інформаційний захист, але й комплекс економічних механізмів, що забезпечують стійкість підприємства

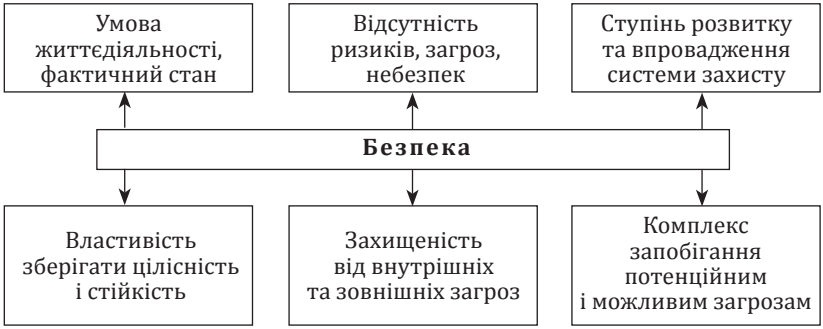


Рис. 1.1. Напрями трактування поняття «безпека»

до конкурентних викликів, фінансових коливань і правових змін. Безпека підприємства у ринкових умовах означає його здатність ефективно функціонувати, захищати ресурси та підтримувати конкурентоспроможність навіть за наявності загроз та невизначеності.

Під **безпекою підприємства** слід розуміти не лише стан його стабільної та безперебійної діяльності, але й здатність ефективно функціонувати в умовах змін зовнішнього та внутрішнього середовища. Це означає, що підприємство мусить підтримувати виконання стратегічних і тактичних програм розвитку, забезпечувати фінансову стійкість, отримувати запланований прибуток, а також протистояти дестабілізуючим чинникам – економічним, політичним, технологічним, соціальним і природним. Безпека підприємства включає захист ресурсів, інформації, репутації та конкурентних позицій на ринку, формування адаптивної стратегії управління ризиками та підвищення стійкості до кризових ситуацій. Основними складовими безпеки організації є:

1. Об'єкти безпеки:

– майнові ресурси (будівлі, обладнання, транспорт, запаси);

– фінансові активи (капітал, інвестиції, грошові потоки);

– інформаційні ресурси (дані, ноу-хау, комерційна таємниця);

– людські ресурси (персонал, управлінські кадри);

– ділова репутація та імідж організації.

2. Пов’язані суб’єкти безпеки:

– власники та керівництво підприємства;

– підрозділи служби безпеки, відділи кадрів, фінансові департаменти;

– державні органи контролю та правоохоронні структури;

– партнери, підрядники та клієнти;

– громадські організації та ЗМІ (як фактори впливу).

3. Нормативно-правове забезпечення:

– закони та підзаконні акти, що регулюють економічну, трудову, інформаційну та екологічну безпеку;

– галузеві стандарти та корпоративні регламенти;

– міжнародні угоди та норми у сфері захисту інформації, прав людини, екології.

4. Фізичний і технічний захист:

– охоронні системи (відеоспостереження, сигналізація, контроль доступу);

– захист від пожеж, аварій та техногенних катастроф;

– системи резервного живлення та відновлення даних.

5. Організаційно-управлінські механізми:

– система менеджменту безпеки (планування, моніторинг, контроль ризиків);

– розробка стратегій антикризового управління та планів реагування на надзвичайні ситуації;

– навчання персоналу та інструктажі з безпеки.

6. Соціально-психологічні аспекти:

– формування корпоративної культури довіри та відповідальності;

– профілактика внутрішніх конфліктів та саботажу;

– програми мотивації та утримання ключових кадрів.

7. Інформаційно-аналітичне забезпечення:

– системи збору та аналізу даних про потенційні загрози;

– моніторинг ринку, конкурентів і змін у законодавстві;

– використання сучасних технологій кіберзахисту.

Через визначення сутності та особливостей понять «безпека», «безпека організації» можна визначити «менеджмент безпеки організації» як цілеспрямовану та систематичну діяльність керівництва і відповідних підрозділів, спрямовану на забезпечення стабільного функціонування підприємства, захист його ресурсів, персоналу, інформації та репутації

від внутрішніх і зовнішніх загроз. Це процес планування, організації, контролю та координації заходів безпеки, який враховує можливі ризики, зміни ринкового середовища та правові вимоги. Менеджмент безпеки включає ідентифікацію небезпек, оцінку рівня ризиків, розробку превентивних стратегій та оперативне реагування на кризові ситуації.

У ширшому значенні **менеджмент безпеки організації** – це невід'ємна частина загальної системи управління, що інтегрує фінансову, інформаційну, кадрову, екологічну, технічну та правову складові захисту. Він передбачає не лише нейтралізацію загроз, а й формування корпоративної культури відповідальності, використання інноваційних інструментів захисту, партнерство з державними та приватними структурами у сфері безпеки. Такий підхід дає можливість організації підтримувати конкурентоспроможність, ефективно функціонувати на ринку та забезпечувати довгострокову стійкість у динамічному та ризиковому бізнес-середовищі.

Також менеджмент безпеки організації можна визначати з позиції управлінського процесу, з точки зору ризик-менеджменту, як елемент корпоративної стратегії (рис. 1.2).

Загалом **менеджмент безпеки організації** можна розглядати як сукупність елементів та напрямів, заходів власників підприємства та працівників, що використовуються для зменшення впливу внутрішніх і зовнішніх негативних факторів на економіко-фінансовий стан організації, її функціонування та розвиток.

Мета забезпечення безпеки організації полягає у всебічному захисті від можливих і реальних загроз, зниження або усунення яких дозволяє суб'єкту господарювання стабільно та ефективно функціонувати навіть у мінливих умовах зовнішнього і внутрішнього середовища. Для досягнення цього важливо забезпечити безпеку за багатьма напрямами, кожен з яких має власне значення і завдання.

До структури менеджменту безпеки організації включають різні види безпеки, які мають свої особливості та по-різному впливають на діяльність і розвиток організації. Основними є:

1. Економічна безпека (включаючи комерційну) – здатність організації підтримувати стійке економічне становище,

Рис. 1.2. Підходи до визначення менеджменту безпеки організації

зберігати ринкову позицію та забезпечувати захист від недобросовісної конкуренції чи економічного шантажу.

2. Фінансова безпека – контроль над грошовими потоками, платоспроможністю та кредитоспроможністю компанії, що дозволяє уникати кризових ситуацій, дефіциту ресурсів і фінансових ризиків.

3. Науково-технічна безпека – збереження та розвиток власних технологій, захист ноу-хау, запобігання витоку інноваційних рішень і технічних секретів, а також використання сучасних технологій для зниження ризиків.

4. Інформаційна безпека – забезпечення конфіденційності, цілісності та доступності корпоративної інформації, захист від кібератак, промислового шпигунства та несанкціонованого доступу до даних.

5. Кадрова безпека – формування надійної кадрової політики, захист від внутрішніх загроз, таких як витік інформації чи зловживання, підбір кваліфікованих працівників і створення мотиваційних механізмів для збереження ключових спеціалістів.

6. Фізична безпека – захист матеріальних активів, приміщень, обладнання та персоналу від злочинних посягань, аварій, пожеж, стихійних лих чи інших фізичних загроз.

7. Правова безпека – дотримання законодавства, захист інтересів підприємства в правовому полі, попередження судових спорів та ризиків, пов'язаних із порушенням нормативно-правових актів.

8. Інвестиційна безпека – збереження та ефективне використання вкладених коштів, захист від ризиків, що можуть вплинути на повернення інвестицій або їхню прибутковість.

9. Соціальна безпека – підтримання сприятливого соціально-психологічного клімату в колективі, запобігання конфліктам, страйкам чи протестам, забезпечення належних умов праці та розвитку персоналу.

10. Екологічна безпека – дотримання природоохоронного законодавства, мінімізація шкідливого впливу на довкілля та впровадження технологій сталого розвитку.

11. Політична та правова стабільність – оцінка та врахування впливу політичних процесів і змін законодавства на діяльність підприємства, адаптація стратегії бізнесу до умов зовнішнього середовища.

12. Репутаційна безпека – формування позитивного іміджу компанії, управління публічними комунікаціями та попередження ситуацій, які можуть зашкодити діловій репутації.

13. Техногенна та промислова безпека – попередження аварій на виробництві, дотримання норм техніки безпеки, нагляд за станом обладнання та виробничих процесів.

14. Кібербезпека – захист інформаційних систем, мереж і цифрових ресурсів підприємства від несанкціонованого доступу, кіберзлочинів, шкідливого програмного забезпечення

та витоків даних. Кібербезпека включає впровадження надійних політик управління доступом, регулярне оновлення програмного забезпечення, резервне копіювання даних і підвищення обізнаності персоналу щодо кіберзагроз.

1.2. Принципи, суб'єкти, об'єкти, функції менеджменту безпеки організації

Принципи забезпечення економічної безпеки підприємства становлять систему концептуальних положень та управлінських орієнтирів, спрямованих на цілісний захист суб'єкта господарювання від зовнішніх та внутрішніх загроз, що можуть негативно вплинути на його фінансову стійкість, конкурентоспроможність і стабільність розвитку. Вони визначають методологічну основу для формування ефективної політики безпеки та вибору адекватних інструментів управління ризиками. До них можна віднести:

1. **Системність.** Забезпечення економічної безпеки має здійснюватися як комплексна, взаємопов'язана система, що охоплює всі ключові сфери діяльності підприємства: фінансово-економічну, виробничо-технологічну, кадрову, інформаційну, екологічну та репутаційну. Такий підхід допомагає узгоджено враховувати взаємозалежність окремих складових і запобігати фрагментарним або неефективним заходам.

2. **Превентивність.** Пріоритет надається попередженню ризиків та загроз, а не лише їх ліквідації. Система економічної безпеки повинна забезпечувати своєчасне виявлення потенційних небезпек шляхом проведення регулярного моніторингу середовища, прогнозування ризиків і впровадження профілактичних механізмів мінімізації можливих збитків.

3. **Безперервність.** Підтримання економічної безпеки не може бути епізодичним; воно має здійснюватися постійно, навіть за умов стабільної діяльності чи відсутності очевидних загроз. Це означає регулярне оновлення політик безпеки, постійний аналіз ризиків і коригування планів відповідно до змін економічних, політичних та соціальних факторів.

4. **Адаптивність.** Підприємство мусить володіти високою здатністю до гнучкого реагування на динамічні зміни у зовнішньому середовищі – від появи нових технологій

до непередбачуваних економічних чи політичних криз. Оперативна адаптація забезпечує збереження конкурентних переваг і мінімізацію негативних наслідків.

5. **Економічна доцільність.** Заходи із забезпечення економічної безпеки повинні бути фінансово обґрунтованими. Витрати на впровадження захисних механізмів мають відповідати можливим ризикам та очікуваним результатам, що дозволяє зберегти баланс між фінансовою стійкістю та рівнем захищеності підприємства.

6. **Комплексність.** Система безпеки повинна враховувати різноманітність загроз – від фінансових і виробничих ризиків до іміджевих та правових. Це передбачає інтеграцію організаційних, технічних, правових, інформаційних та управлінських заходів, задіюваних узгоджено.

7. **Легітимність.** Усі дії, спрямовані на забезпечення економічної безпеки, мають здійснюватися відповідно до чинного законодавства, корпоративних стандартів та етичних норм. Дотримання цього принципу захищає підприємство від юридичних санкцій та підтримує його позитивну репутацію на ринку.

8. **Конфіденційність.** Важливо забезпечувати надійний захист стратегічно значущої інформації, комерційної таємниці, інноваційних розробок і фінансових даних від несанкціонованого доступу або розголошення, оскільки такі витоки можуть призвести до серйозних економічних втрат.

9. **Контроль та моніторинг.** Систематичний контроль за внутрішніми процесами та зовнішнім середовищем, а також регулярний моніторинг стану економічної безпеки дають змогу вчасно ідентифікувати нові ризики та оперативно приймати коригувальні управлінські рішення.

10. **Інноваційність.** Підприємство має активно застосовувати новітні технології, сучасні аналітичні інструменти й передові управлінські практики для підвищення ефективності системи безпеки. Інноваційний підхід дозволяє не лише нейтралізувати актуальні загрози, а й випереджати потенційні виклики у майбутньому.

Суб'єкти менеджменту безпеки організацій – це особи або групи, які приймають рішення, контролюють і відповідають за впровадження заходів з безпеки в організації. До основних суб'єктів належать: власники, керівники різних рівнів,

спеціалісти з безпеки, службовці відділів інформаційної, фізичної, фінансової та кадрової безпеки, а також зовнішні консультанти та регуляторні органи, суб'єкти що здійснюють співпрацю з організацією. Ключовою функцією суб'єктів є організація, координація та контроль заходів, спрямованих на забезпечення захисту організації від потенційних загроз, а їхні завдання в процесі забезпечення менеджменту безпеки наведено в табл. 1.2.

Таблиця 1.2

Суб'єкти та їхні завдання під час забезпечення менеджменту безпеки організації

Суб'єкти	Завдання, пов'язані зі забезпеченням менеджменту безпеки
1	*2*
Власники та акціонери організації	Визначення стратегічних пріоритетів безпеки, формування ресурсної бази для захисту активів, затвердження політики безпеки та контроль за її виконанням.
Вищий керівний склад (дирекція, топменеджери)	Розробка та впровадження політики економічної, інформаційної та фізичної безпеки; інтеграція безпекових заходів у загальну стратегію розвитку підприємства; організація процесів оцінювання та мінімізації ризиків.
Служба безпеки організації	Моніторинг загроз, організація заходів з охорони об'єктів і персоналу, проведення аналітичної роботи щодо ризиків, управління кризовими ситуаціями, координація взаємодії з правоохоронними структурами.
Фінансовий відділ та бухгалтерія	Запобігання фінансовим шахрайствам, забезпечення прозорості фінансових потоків, контроль за дотриманням бюджетної дисципліни, аналіз ризиків інвестицій та угод.
Юридичний відділ	Правове забезпечення діяльності організації, мінімізація юридичних ризиків, підготовка та перевірка договорів, контроль дотримання норм законодавства, захист інтересів підприємства у судах.
ІТ-відділ та спеціалісти з кіберзахисту	Розробка і впровадження заходів інформаційної та кібербезпеки, захист корпоративних даних і мереж, управління доступом, проведення аудитів інформаційної інфраструктури.
Керівники відділів та працівники	Впровадження безпекових політик на рівні підрозділів, контроль дотримання норм і процедур безпеки працівниками, звітування про ризики та інциденти. Дотримання внутрішніх правил і політик безпеки, своєчасне інформування керівництва про потенційні загрози чи порушення, участь у навчаннях та тренінгах.

Завершення табл. 1.2

1	*2*
Профспілкові організації або представники колективу	Захист трудових прав працівників, участь у розробці політики соціальної та кадрової безпеки, сприяння формуванню безпечних умов праці.
Контролюючі органи та державні інституції	Нагляд за дотриманням норм законодавства, проведення перевірок щодо екологічної, технічної, пожежної та фінансової безпеки, надання рекомендацій і санкцій у разі порушень.
Правоохоронні та спеціальні служби	Протидія кримінальним загрозам, проведення розслідувань правопорушень, охорона об'єктів підвищеного ризику, забезпечення громадського порядку.
Постачальники та бізнес-партнери	Забезпечення надійності постачання ресурсів, дотримання договірних умов і стандартів безпеки, уникнення ризиків, пов'язаних із недобросовісною діяльністю.
Клієнти та споживачі	Зворотний зв'язок щодо якості продукції чи послуг, участь у підтримці репутаційної безпеки організації шляхом довіри до бренду та дотримання контрактних зобов'язань.
Аудиторські та консалтингові компанії	Незалежна оцінка стану безпеки, аудит фінансових та управлінських процесів, рекомендації щодо удосконалення політик безпеки.

Об'єкти менеджменту безпеки організації – це всі елементи, ресурси, процеси та цінності підприємства, що потребують захисту для стабільного функціонування та розвитку (рис. 1.3). При цьому об'єкти можуть змінюватися залежно від організаційної структури організації, що досліджується, як об'єкти безпеки, та цілей, які ставлять перед собою суб'єкти.

Управління цими об'єктами передбачає комплекс заходів: систематичний моніторинг загроз, оцінювання ризиків та пріоритетів захисту, розробку внутрішніх регламентів і політик безпеки, застосування технічних, організаційних та правових механізмів захисту, впровадження систем контролю доступу та резервування ресурсів, а також регулярне навчання персоналу. Ефективне управління об'єктами безпеки передбачає інтеграцію захисних заходів у загальну стратегію підприємства, використання превентивних підходів та гнучке реагування на зміни в зовнішньому та внутрішньому середовищі, що дозволяє зберігати стабільність і конкурентоспроможність організації.

Рис. 1.3. Головні об'єкти менеджменту безпеки організації

Функції менеджменту безпеки організації включають комплекс заходів і дій, спрямованих на забезпечення захисту підприємства від різних загроз. Основними функціями є:

1. Аналіз та оцінка ризиків, яка полягає у виявлені потенційних загроз, оцінюванні впливу на діяльність організації, ідентифікацію ризиків, аналіз імовірності їх виникнення та оцінку можливих наслідків для фінансової, інформаційної, фізичної та кадрової безпеки.

2. Функція планування безпеки передбачає структурування і координацію роботи підрозділів безпеки, розподіл відповідальності та ресурсів, впровадження необхідних інструментів і технологій для забезпечення ефективного функціонування системи безпеки.

3. Функція організації системи безпеки включає комплексне структурування та чітку координацію діяльності всіх підрозділів і відповідальних осіб, які залучені до забезпечення захисту підприємства, включаючи розподіл повноважень, обов'язків та відповідальності між учасниками процесу, раціональне використання та ефективний розподіл фінансових, матеріальних і людських ресурсів,

а також впровадження сучасних інструментів, технологій та управлінських механізмів, завдяки яким можливо створити узгоджену, гнучку та результативну систему безпеки, здатну оперативно реагувати на загрози та підтримувати стабільність функціонування організації.

4. Моніторинг і контроль – проведення постійного контроль та моніторингу за виконанням заходів з безпеки та моніторинг внутрішніх і зовнішніх змін, що можуть вплинути на захищеність організації. Завданням цієї функції є виявлення нових ризиків, оцінка ефективності заходів безпеки та їх своєчасне коригування.

5. Функція реагування на загрози передбачає оперативне реагування на виявлені ризики або факти порушення безпеки, включаючи усунення наслідків інцидентів, локалізацію загроз і мінімізацію втрат. Функція включає реалізацію кризових планів і відновлення нормального функціонування організації після інцидентів.

6. Оцінка ефективності системи безпеки шляхом вимірювання результативності впроваджених заходів з безпеки, аналіз їхньої дієвості та економічної доцільності, а також визначення можливих покращень для підвищення рівня захисту.

7. Аналітична функція у менеджменті безпеки організації полягає у систематичному та всебічному зборі, ретельній обробці й поглибленій оцінці різноманітної інформації про зовнішнє та внутрішнє середовище підприємства, що включає аналіз ринкових тенденцій, фінансових показників, правових умов, соціально-економічних факторів і технічних характеристик діяльності, з метою своєчасного виявлення потенційних слабких місць, критичних точок та ймовірних ризиків, які можуть негативно вплинути на стабільність і безпечність функціонування організації.

8. Захисна функція передбачає цілеспрямоване та послідовне впровадження комплексу практичних заходів, спрямованих на забезпечення фізичної охорони об'єктів підприємства, захист важливої та конфіденційної інформації від несанкціонованого доступу чи витоку, дотримання правових норм та стандартів з метою мінімізації юридичних ризиків, збереження фінансової стабільності шляхом контролю

за ресурсами та запобігання шахрайству, а також підтримку кадрової безпеки через формування надійного персоналу, підвищення його лояльності та попередження можливих внутрішніх загроз.

9. Ресурсна функція полягає у своєчасному та комплексному забезпеченні всіх напрямів діяльності системи безпеки необхідними фінансовими коштами, матеріальними засобами, кваліфікованими кадрами та сучасними технологічними ресурсами, що дозволяє гарантувати безперебійне функціонування механізмів захисту, ефективне реагування на можливі ризики та підтримання належного рівня безпеки навіть у кризових ситуаціях.

10. Правова функція передбачає постійний моніторинг і дотримання вимог чинного законодавства, нормативно-правових актів та внутрішніх регламентів підприємства, а також забезпечення правового супроводу заходів безпеки з метою захисту законних прав, інтересів та репутації організації, попередження юридичних ризиків і уникнення можливих санкцій чи претензій з боку державних органів та партнерів.

11. Інноваційна функція означає систематичне впровадження новітніх технологій, сучасних методів управління ризиками, передових підходів та практик у сфері безпеки, що дозволяє підвищувати ефективність та надійність захисту організації, адаптувати систему безпеки до динамічних змін зовнішнього середовища, а також забезпечувати конкурентоспроможність та стійкість підприємства у довгостроковій перспективі.

12. Відновлювальна функція у менеджменті безпеки організації передбачає комплекс заходів, спрямованих на оперативне та ефективне відновлення стабільної діяльності підприємства після виникнення надзвичайних ситуацій, інцидентів, кризових подій або зовнішніх та внутрішніх загроз, включаючи оцінку масштабів завданої шкоди, мобілізацію необхідних ресурсів, координацію дій відповідальних підрозділів, впровадження тимчасових і постійних рішень для усунення наслідків порушень, а також розробку та реалізацію стратегій, які дозволять уникнути повторення подібних подій у майбутньому та підвищити стійкість організації.

1.3. Основні завдання забезпечення безпеки організації

У суспільній свідомості й досі зберігаються стійкі стереотипи, що асоціюють поняття «забезпечення безпеки» виключно з державними інтересами та діяльністю спеціалізованих урядових структур. Натомість у чинному законодавстві під безпекою розуміється стан захищеності життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз, що свідчить про пріоритетність прав та інтересів особистості.

Одним із таких інтересів визнається підприємницька діяльність, яка може здійснюватися як індивідуально, так і шляхом участі у створенні та функціонуванні юридичних осіб. Отож забезпечення безпеки підприємства слід розглядати як комплексну управлінську діяльність, спрямовану на захист матеріальних, фінансових та людських ресурсів від потенційних і реальних загроз, а також на виявлення та усунення причин, що можуть їх зумовлювати. Основною метою менеджменту безпеки організації є гарантування стабільності функціонування, збереження майна та захист працівників шляхом реалізації превентивних, аналітичних і захисних заходів у мінливому зовнішньому та внутрішньому середовищі.

Головним елементом, на який опирається система формування завдань безпеки організації та її менеджменту, є негативні фактори зовнішнього та внутрішнього середовища (рис. 1.4).

Основні завдання забезпечення безпеки організації спрямовані на захист її ресурсів, стабільність діяльності та мінімізацію негативних впливів. До ключових **завдань безпеки організації** належать:

1. Ідентифікація загроз, їх оцінка за рівнем впливу на окремі види діяльності та фінансово-економічний стан організації загалом. Процес забезпечення безпеки організації починається з комплексного виявлення внутрішніх та зовнішніх ризиків, здатних впливати на стабільність її діяльності. Це включає систематичний моніторинг економічного середовища, політичної ситуації, конкурентного ринку і технологічних змін, а також внутрішніх аспектів,

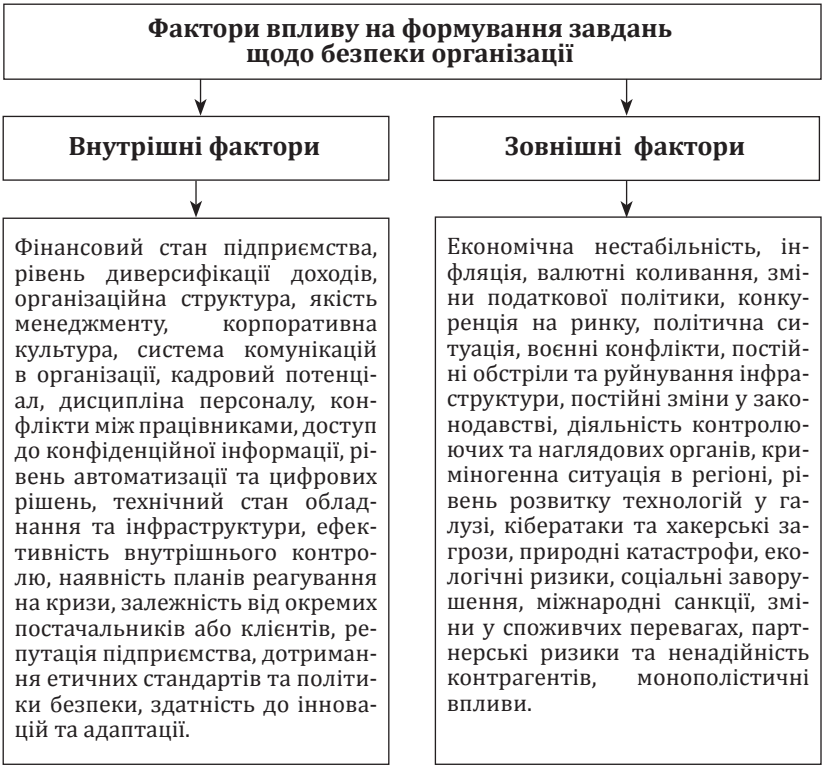


Рис. 1.4. Чинники, що здійснюють вплив на формування основних завдань щодо безпеки підприємства

таких як кадровий потенціал, фінансова дисципліна, стан інфраструктури й корпоративна культура. Оцінка загроз передбачає визначення ймовірності їх реалізації та масштабів можливих наслідків для фінансових, матеріальних, інформаційних і людських ресурсів, що дозволяє сформувати обґрунтовану пріоритетність заходів реагування.

2. Створення та впровадження стратегії безпеки, яка буде розроблена на короткостроковий та довгостроковий період, враховуватиме специфіку діяльності та кадрову політику. На основі результатів аналізу загроз формується багаторівнева стратегія безпеки, яка розробляється як складова частина загальної стратегії управління організацією.

Така стратегія має включати політики, стандарти, процедури, інструменти та організаційні рішення, спрямовані на запобігання ризикам, мінімізацію ймовірності кризових подій та зменшення їхніх негативних наслідків. Її впровадження передбачає координацію роботи різних структурних підрозділів, оптимальний розподіл ресурсів та використання сучасних технологічних рішень.

3. Формування системи захисту інформаційних та матеріальних ресурсів, а також ключових активів підприємства, що забезпечують його прибутковість. Це стосується не лише матеріальних цінностей (будівель, обладнання, готової продукції), а й нематеріальних – інформаційних систем, комерційних таємниць, баз даних і технологічних ноу-хау. Для цього застосовуються як фізичні методи (системи відеоспостереження, контроль доступу, охорона), так і організаційно-правові та технічні заходи (резервне копіювання даних, використання шифрування, розмежування прав доступу, договори про нерозголошення інформації).

4. Управління кризами через створення попереднього планування дій у надзвичайних обставинах. Завданням організації є створення системи управління кризами, яка передбачає розроблення детальних планів реагування на різні види критичних подій: збої у виробничих процесах, кібератаки, стихійні лиха, техногенні аварії чи внутрішні конфлікти. Важливо також забезпечити оперативне відновлення функціонування організації після криз, мінімізуючи репутаційні та фінансові втрати.

5. Підвищення рівня обізнаності та підготовки персоналу, а також визначення ролі керівників і власників організації, ієрархічний розподіл обов'язків та напрямів управління. Людський фактор є однією з найуразливіших ланок системи безпеки, тому особливу увагу слід приділяти навчальним і виховним заходам. До основних завдань належить організація регулярних тренінгів, семінарів та практичних занять із питань інформаційної, фінансової, правової та фізичної безпеки, а також проведення симуляцій кризових ситуацій. Такі заходи формують у працівників відповідальне ставлення до питань безпеки, підвищують їхню готовність

до швидкого та ефективного реагування на потенційні загрози, зменшують імовірність помилок та порушень, які можуть призвести до збитків чи репутаційних ризиків.

1.4. Основи управління економічною безпекою організації

Економічна безпека підприємства – це стан захищеності його фінансово-господарської діяльності, матеріальних, інформаційних та інтелектуальних ресурсів від зовнішніх і внутрішніх загроз, який забезпечує стабільність функціонування, здатність до розвитку, конкурентоспроможність і досягнення стратегічних цілей у мінливому ринковому середовищі. Такий стан передбачає раціональне використання ресурсів, ефективне управління ризиками, своєчасне виявлення та нейтралізацію потенційних небезпек, а також формування адаптивних механізмів реагування на економічні, політичні, правові та технологічні виклики.

Управління економічною безпекою підприємства – це цілеспрямована та системна діяльність керівництва і відповідних структурних підрозділів, скерована на виявлення, оцінювання та нейтралізацію внутрішніх і зовнішніх загроз, які можуть негативно вплинути на фінансово-господарську стабільність, конкурентоспроможність і стратегічний розвиток організації. Воно передбачає планування, організацію, координацію та контроль заходів, що забезпечують раціональне використання ресурсів, захист активів та інформації, підтримання стабільного функціонування у змінному ринковому середовищі та створення умов для довгострокового економічного зростання підприємства (рис. 1.5).

Сучасні підприємства функціонують у складному, динамічному та часто непередбачуваному зовнішньому середовищі, що супроводжується постійним зростанням кількості потенційних загроз і ризиків у господарській діяльності. Такі умови зумовлюють необхідність формування в межах загальної системи менеджменту окремої спеціалізованої підсистеми – системи управління економічною безпекою підприємства. Ця система покликана забезпечити стабільність функціонування суб'єкта господарювання, захист його ресур-

Рис. 1.5. Класифікація напрямів управління економічною безпекою

сів, конкурентоспроможність і здатність до розвитку навіть за умов нестабільності та кризових явищ.

У вузькому трактуванні система управління економічною безпекою підприємства охоплює сукупність органів управління, структурних підрозділів та окремих виконавців, наділених чітко визначеними повноваженнями й відповідальністю за виконання покладених функцій. До її складу входять також методи та інструменти управлінського

впливу, за допомогою яких здійснюється захист економічних інтересів та підтримується стійкість підприємства.

У широкому розумінні **система управління економічною безпекою підприємства** є комплексною організаційно-управлінською конструкцією, що включає:

– організаційну структуру – формалізоване відображення складу, взаємозв'язків і підпорядкованості всіх елементів і рівнів управління безпекою, що забезпечує чіткий розподіл повноважень і каналів комунікації;

– суб'єкти управління (управлінський персонал) – керівники, спеціалісти й працівники, які безпосередньо реалізують функції управління або створюють умови для їх ефективного виконання; до цього кола можуть входити як внутрішні підрозділи, так і зовнішні консультанти чи підрядники;

– механізм управління – сукупність інструментів, методів, принципів і процедур, спрямованих на підготовку, ухвалення та реалізацію управлінських рішень, що забезпечують економічну стійкість та захист інтересів підприємства;

– об'єкти управління – конкретні напрями діяльності або ресурси, які потребують захисту та регулювання: фінансові потоки, матеріальні активи, виробничі процеси, інформаційні ресурси, людський капітал та інші елементи, від яких залежить ефективність діяльності організації;

– функції управління – спеціалізовані види управлінської діяльності (планування, організація, контроль, моніторинг, координація, аналіз і регулювання), що відображають послідовність та напрямки цілеспрямованого впливу суб'єктів управління на об'єкти;

– процес управління – безперервна взаємодія суб'єктів та об'єктів управління, яка здійснюється через застосування визначених методів та інструментів для досягнення стратегічних і тактичних цілей економічної безпеки.

Система економічної безпеки підприємства формується та розвивається відповідно до обраної політики та стратегії безпеки. Політика безпеки виступає як концептуальна основа, що визначає погляди, принципи, правила та комплекс заходів у сфері безпеки, спрямованих на створення стабільного середовища для ведення бізнесу, підвищення його конкурентоспроможності та захисту від ризиків.

Стратегія безпеки деталізує цю політику, перетворюючи її на систему практичних рішень і довгострокових пріоритетів, які забезпечують ефективне функціонування підприємства навіть за умов турбулентності зовнішнього та внутрішнього середовища.

У процесі управління економічною безпекою вітчизняні підприємства можуть використовувати одну із трьох моделей. Перша модель «Захисного бар'єру» (реактивна модель) (табл. 1.3) спирається на захист активів та усунення недоліків і є найбільш поширеною на практиці.

Таблиця 1.3

Характеристика моделі «Захисного бар'єру»

Характеристика	Опис
Сутність	Розглядає економічну безпеку як незалежну, допоміжну функцію, спрямовану виключно на захист існуючих активів та усунення наслідків уже реалізованих загроз.
Основний інструмент	Фізична охорона, системи контролю доступу, базове страхування, внутрішній аудит після події.
Головний недолік	Реактивний характер управління. Нездатність запобігати кризам, а лише мінімізувати їхні наслідки. Відсутність інтеграції в стратегічне планування.
Актуальність	Підходить для малих підприємств з обмеженими ресурсами або для початкового етапу формування системи економічної безпеки (ЕБ).

Другу модель «Інтерактивного ризик-менеджменту» (проактивну модель) відображено в табл. 1.4.

Таблиця 1.4

Характеристика моделі «Інтерактивного ризик-менеджменту»

Характеристика	Опис
1	*2*
Сутність	Економічна безпека повністю інтегрована в загальну корпоративну систему управління ризиками (ERM). ЕБ розглядається як інструмент підтримки стратегічних цілей.
Основний інструмент	Методології стандарту ISO 31000 (Ризик-менеджмент), регулярна ідентифікація та кількісна оцінка ризиків, розробка превентивних заходів.

Завершення табл. 1.4

1	*2*
Головний недолік	Вимагає значних інвестицій у створення інтегрованої IT-інфраструктури та високої кваліфікації персоналу. Може бути бюрократизованою.
Актуальність	Стандарт для середніх і великих компаній, які прагнуть оптимізувати співвідношення «ризик/дохід» та забезпечити стійкість (Resilience) бізнесу.

І третя модель «Стратегічного розвитку» (ціннісно-орієнтована модель) використовується, коли організації (підприємства) намагаються розширити власну діяльність шляхом формування нових підрозділів (відділень) або виходу на новий ринок і зосереджені саме на аналізі нових можливих загроз (табл. 1.5).

Таблиця 1.5

Характеристика моделі «Стратегічного розвитку»

Характеристика	**Опис**
Сутність	Економічна безпека розглядається як стратегічний ресурс (або конкурентна перевага). Управління ЕБ спрямовано не тільки на захист, але й на створення вартості (*Value Creation*).
Основний інструмент	Баланс між ризиком та інноваціями, використання ЕБ для обґрунтування інвестиційних рішень (наприклад, оцінка безпеки нового ринку), прогнозування загроз із використанням Big Data.
Головний недолік	Висока складність і залежність від точності стратегічного прогнозування. Потребує найвищого рівня інтеграції ЕБ у процес прийняття рішень на рівні Ради директорів.
Актуальність	Рекомендована для інноваційних компаній, лідерів галузі, що працюють у висококонкурентному або швидкозмінному середовищі.

Менеджмент безпеки організації відіграє центральну роль у забезпеченні безперебійної та ефективної діяльності підприємства, особливо в умовах значних і непередбачуваних ризиків. Його основна функція полягає у створенні комплексної системи захисту, яка охоплює не лише фізичні активи та інформаційні ресурси, але й стратегічні, фінансові

та репутаційні аспекти діяльності. Ефективний менеджмент безпеки дає змогу підприємству проактивно ідентифікувати потенційні загрози, такі як кібератаки, операційні збої чи зміни в законодавстві, і розробити превентивні заходи. Це забезпечує стійкість (Resilience) бізнес-процесів, мінімізуючи ймовірність критичних простоїв і фінансових втрат, що напряму впливає на виконання виробничих планів та збереження конкурентних переваг.

Система менеджменту безпеки є важливим інструментом для підтримки довіри всіх зацікавлених сторін. Гарантуючи захист даних клієнтів, фінансової інформації та дотримання міжнародних стандартів, вона зміцнює репутацію організації як надійного партнера і гравця на ринку. Крім того, інвестиції в безпеку розглядаються не як витрати, а як стратегічна інвестиція, що дозволяє підприємству приймати більш обґрунтовані та ризикові рішення, відкриваючи нові можливості для зростання. Таким чином, менеджмент безпеки перетворюється з простої функції захисту на критичний елемент управління (Governance), який забезпечує не лише виживання, але й довгостроковий сталий розвиток організації.

Питання для самоконтролю

1. Розкрийте сутність поняття економічної безпеки підприємства та поясніть, чому воно є ключовим у сучасному менеджменті.
2. Які основні внутрішні та зовнішні фактори впливають на формування завдань економічної безпеки організації?
3. Охарактеризуйте складові системи управління економічною безпекою підприємства у вузькому та широкому розумінні.
4. Які принципи забезпечення економічної безпеки підприємства вважаються фундаментальними та як вони застосовуються на практиці?
5. Назвіть та охарактеризуйте основні види безпеки організації (економічна, фінансова, інформаційна тощо) та їхню роль у стабільності бізнесу.
6. Поясніть функції менеджменту безпеки організації та розкрийте їх значення для ефективної роботи підприємства.
7. Чому інтеграція системи економічної безпеки в загальну стратегію розвитку підприємства є необхідною?

8. Яким чином кадровий потенціал і корпоративна культура впливають на рівень економічної безпеки?

9. Розкрийте зміст поняття «політика та стратегія безпеки» і поясніть їхній взаємозв'язок.

10. Які сучасні виклики і тенденції впливають на підходи до управління економічною безпекою підприємств?

Тестові завдання

1. Який головний зміст економічної безпеки підприємства?

а) Виключно захист фінансових ресурсів;

б) стан стабільності діяльності, що гарантує захист ресурсів та інтересів від загроз;

в) виконання державних нормативів безпеки;

г) лише організація фізичного захисту.

2. Яка складова не належить до системи економічної безпеки в широкому розумінні?

а) Організаційна структура управління;

б) суб'єкти управління, які визначають рівень впливу факторів;

в) механізм управління;

г) додаткові виробничі площі підприємства.

3. Принцип превентивності у менеджменті безпеки означає:

а) реагування на загрози після їх настання;

б) створення системи безпеки без ресурсного забезпечення;

в) попередження ризиків та їх раннє виявлення до настання негативних наслідків;

г) впровадження інновацій незалежно від їхньої ефективності.

4. Що є головною метою політики безпеки підприємства?

а) Формальне виконання інструкцій і нормативів;

б) створення сприятливого середовища для реалізації цілей бізнесу шляхом захисту ресурсів і інтересів;

в) лише мінімізація витрат на охоронні заходи;

г) виключно протидія зовнішнім конкурентам.

5. До зовнішніх факторів, що впливають на економічну безпеку, відносять:

а) рівень компетентності керівників;

б) політичну нестабільність, зміни законодавства, ринкову конкуренцію;

в) низьку корпоративну культуру та комунікації;

г) невдале планування бюджету.

6. Який елемент належить до механізму управління економічною безпекою?

а) Фінансові активи підприємства;

б) методи, інструменти та процедури впливу на процес прийняття рішень;

в) окремі підрозділи виробництва;

г) ступінь автоматизації облікових процесів.

7. Інтеграція безпекової стратегії у загальну стратегію розвитку підприємства дає можливість:

а) уникнути необхідності зовнішнього аудиту;

б) узгодити заходи безпеки з бізнес-цілями та оптимізувати ресурси;

в) зменшити обсяг кадрових витрат;

г) звузити сферу відповідальності менеджерів.

8. До видів безпеки, які забезпечують стабільність підприємства, відноситься:

а) лише фінансова безпека;

б) економічна, правова, кадрова, інформаційна, фізична, інвестиційна та інші;

в) тільки соціальна та екологічна;

г) лише захист комерційної таємниці.

9. Яка функція менеджменту безпеки передбачає захист від загроз шляхом застосування прямих заходів фізичного, інформаційного та правового характеру?

а) Відновлювальна функція;

б) аналітична функція;

в) захисна функція;

г) інноваційна функція.

10. Чому кадровий потенціал є критичним фактором економічної безпеки?

а) Кадри визначають лише витрати на зарплату;

б) від рівня підготовки персоналу залежить ефективність виявлення та нейтралізації загроз;

в) працівники впливають виключно на фінансовий контроль;

г) кадровий потенціал не має значення для безпеки організації.

ТЕМА 2

ФОРМУВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ БЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1. Сутність системи менеджменту безпеки організації
2.2. Етапи формування системи менеджменту безпеки
2.3. Напрями та методи оцінки безпеки організації

Основні поняття і терміни: безпека, безпека організації, менеджмент, менеджмент безпеки організації, ризики, небезпека, система безпеки, заходи захисту, потенціал безпеки, керівні органи, моніторинг ризиків.

2.1. Сутність системи менеджменту безпеки організації

Сутність системи менеджменту безпеки в діяльності організації полягає у створенні та підтримці цілісного, організованого та адаптивного механізму, який забезпечує збереження ресурсів, стабільність функціонування та захист стратегічних інтересів підприємства в умовах постійних змін і ризиків. Вона включає розробку політик безпеки, формування організаційної структури, визначення відповідальності та повноважень, а також застосування методів, інструментів технологій для попередження, виявлення та нейтралізації загроз.

Ця система інтегрує управлінські, правові, фінансові, кадрові та інформаційні заходи, поєднує превентивні та реагувальні дії, забезпечує ефективну взаємодію всіх підрозділів організації та створює умови для безперервності бізнес-процесів. Її сутність також виражається у здатності швидко адаптуватися до динамічного зовнішнього середовища, мінімізувати ризики та підтримувати конкурентоспроможність, водночас формуючи культуру безпеки серед персоналу й забезпечуючи дотримання етичних і правових норм.

Систему менеджменту безпеки організації можна розглядати з позиції комплексної структури управління, як сукупність елементів, що становлять загальну систему,

і як організаційно-управлінський механізм, проте в загальному вони формують одну багатоструктуровану складову, яка забезпечує зниження, запобігання або уникнення ризиків, що виникають у процесі діяльності організації, її розвитку та розширення.

Система менеджменту безпеки організації – це комплексна структура, яка охоплює процеси, заходи та інструменти, спрямовані на забезпечення захисту організації від внутрішніх та зовнішніх загроз, що можуть впливати на її стабільність, ефективність та конкурентоспроможність. Вона є невід'ємною частиною загального управління підприємством і спрямована на запобігання, виявлення, мінімізацію та усунення ризиків, що виникають у різних сферах діяльності.

Система менеджменту безпеки організації – це сукупність взаємопов'язаних принципів, методів, ресурсів і управлінських рішень, спрямованих на збереження цілісності ресурсів, безперервність бізнес-процесів та дотримання правових і етичних норм у діяльності підприємства. Вона інтегрує заходи превентивного та реагувального характеру, забезпечуючи здатність організації адаптуватися до змін зовнішнього середовища, нейтралізувати ризики та підтримувати стабільність розвитку.

Система менеджменту безпеки організації – це організаційно-управлінський механізм, що поєднує політику безпеки, структури управління, кадровий потенціал, технологічні та правові інструменти для гарантування захищеності стратегічних і операційних інтересів підприємства. Вона функціонує як частина загальної системи менеджменту, формує комплексну відповідь на потенційні загрози та забезпечує конкурентоспроможність і довгострокову життєздатність організації.

Складові системи менеджменту безпеки організації охоплюють взаємопов'язані елементи, які разом формують цілісний механізм захисту підприємства від ризиків і загроз. До основних складових можна віднести: принципи управління безпекою, методи та інструменти, ресурсне забезпечення, організаційні рішення та процеси, суб'єкти і об'єкти управління, потенціал безпеки, нормативно-правову базу, інформаційно-аналітичне забезпечення, культуру безпеки, моніторинг та контроль (рис. 2.1).

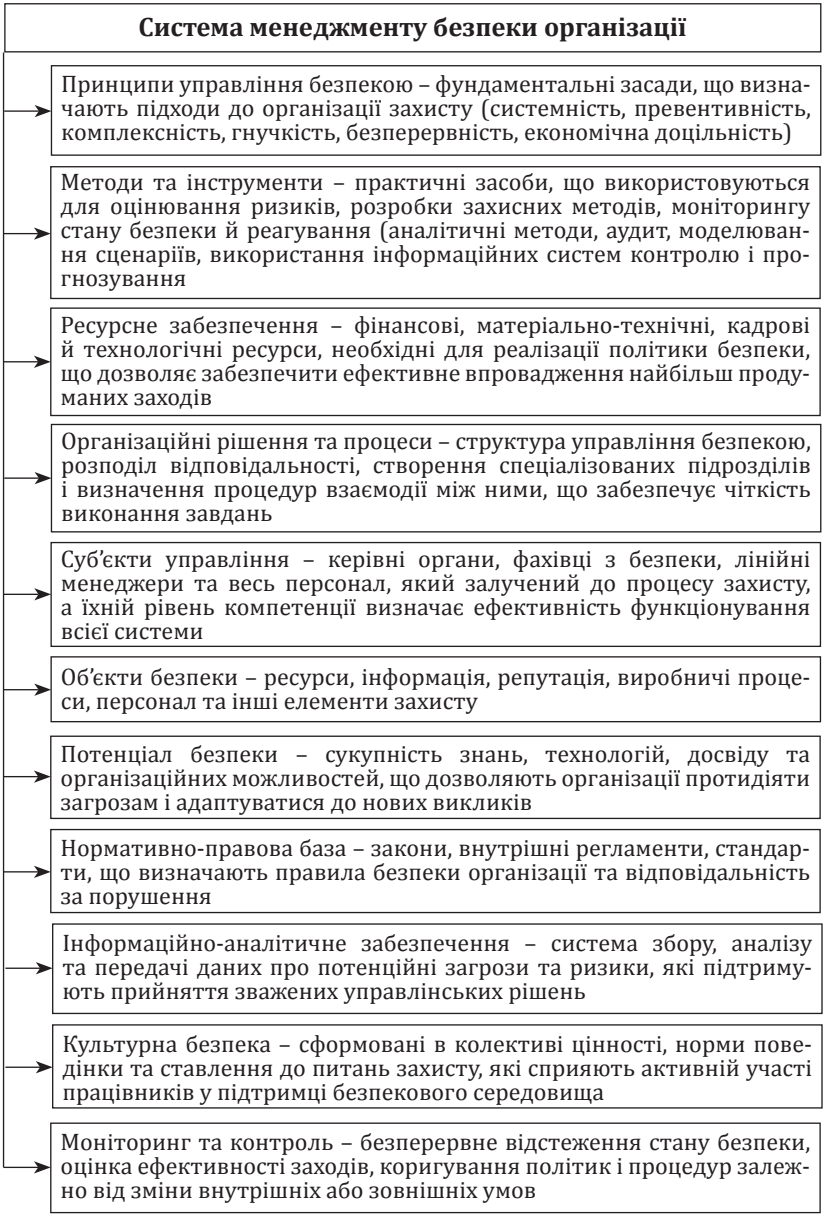


Рис. 2.1. Основні складові системи менеджменту безпеки організації

Дотримання принципів у системі менеджменту безпеки організації становить фундамент для формування цілісної та ефективної політики захисту. Принципи визначають логіку прийняття рішень, узгоджують дії всіх підрозділів та забезпечують прозорість процесів управління ризиками. Вони допомагають підтримувати баланс між економічною ефективністю та рівнем безпеки, що особливо важливо у складних і змінних умовах ринку. Виконання цих принципів підвищує стійкість організації, зміцнює довіру з боку партнерів і мінімізує негативні наслідки можливих загроз. Основними принципами системи менеджменту безпеки організації є перелічені та охарактеризовані вище (в темі 1) принципи системності, превентивності, безперервності, адаптивності, економічної доцільності, комплексності, легітимності, конфіденційності, контролю і моніторингу, інноваційності.

Методи та ***інструменти*** системи менеджменту безпеки охоплюють широкий спектр практичних засобів, які забезпечують комплексний підхід до виявлення, оцінювання та нейтралізації ризиків. До них належать: аналітичні методи (SWOT- та PEST-аналіз, порівняльний і статистичний аналіз), аудит безпеки та перевірки відповідності стандартам, моделювання можливих сценаріїв розвитку кризових подій, використання інформаційних систем контролю, прогнозування та автоматизованих систем моніторингу. Також застосовують методи управління ризиками (ідентифікація, оцінка, диверсифікація та мінімізація ризиків), інструменти фінансового аналізу, технології кіберзахисту та системи раннього попередження. Сукупне використання цих засобів дозволяє своєчасно реагувати на загрози та забезпечувати стабільність діяльності організації.

Ресурсне забезпечення системи менеджменту безпеки організації є ключовим елементом, який визначає спроможність підприємства впроваджувати ефективні заходи захисту та підтримувати стабільність у довгостроковій перспективі. Воно охоплює не лише фінансові ресурси, необхідні для фінансування програм безпеки, а й матеріально-технічні засоби, які забезпечують практичну реалізацію захисних заходів, а також кадровий потенціал, відповідальний за планування, організацію та контроль безпекових процесів.

Правильний розподіл і раціональне використання цих ресурсів допомагають оптимізувати витрати, мінімізувати ризики та підвищити загальну ефективність управління безпекою.

Крім того, важливо враховувати технологічну складову, що охоплює сучасні інструменти моніторингу, системи управління ризиками, інформаційні технології та програмне забезпечення для аналітики та контролю. Забезпечення підприємства актуальними технологіями та інноваційними рішеннями дає змогу не лише своєчасно виявляти потенційні загрози, але й оперативно реагувати на них, зберігаючи конкурентоспроможність у складних умовах зовнішнього середовища.

До елементів ресурсного забезпечення належать:

– фінансові ресурси – бюджети для реалізації програм безпеки, страхування ризиків, резервні фонди;

– матеріально-технічні ресурси – обладнання для охорони, системи відеоспостереження, сигналізації, захисні споруди;

– кадрові ресурси – фахівці з безпеки, менеджери, консультанти, навчений персонал;

– технологічні ресурси – інформаційні системи, програмне забезпечення для моніторингу та аналізу ризиків, інноваційні рішення для підвищення рівня безпеки;

– організаційно-методичні ресурси – стандарти, методики, регламенти та інструкції, що визначають порядок використання ресурсів і реалізації заходів безпеки.

Організаційні рішення та процеси у сфері безпеки організації є основним елементом системи управління, що забезпечує ефективну реалізацію стратегічних та тактичних заходів захисту. Вони формують структуру управління безпекою, визначають зони відповідальності, створюють спеціалізовані підрозділи а також встановлюють процедури взаємодії між ними. Метою прийняття таких рішень є:

– чітке розмежування обов'язків серед керівного та виконавчого складу;

– своєчасне та ефективне реагування на загрози та інтенданти;

– оптимізація ресурсів для забезпечення безпеки;

– підвищення надійності та передбачуваності дій у критичних ситуаціях;

– створення внутрішньої культури безпеки, де кожен співробітник знає свої обов'язки та завдання.

Організаційні рішення і процеси забезпечують системність, структурованість і контрольованість безпекових заходів у будь-якій організації. Їх класифікацію наведено на рис. 2.2.

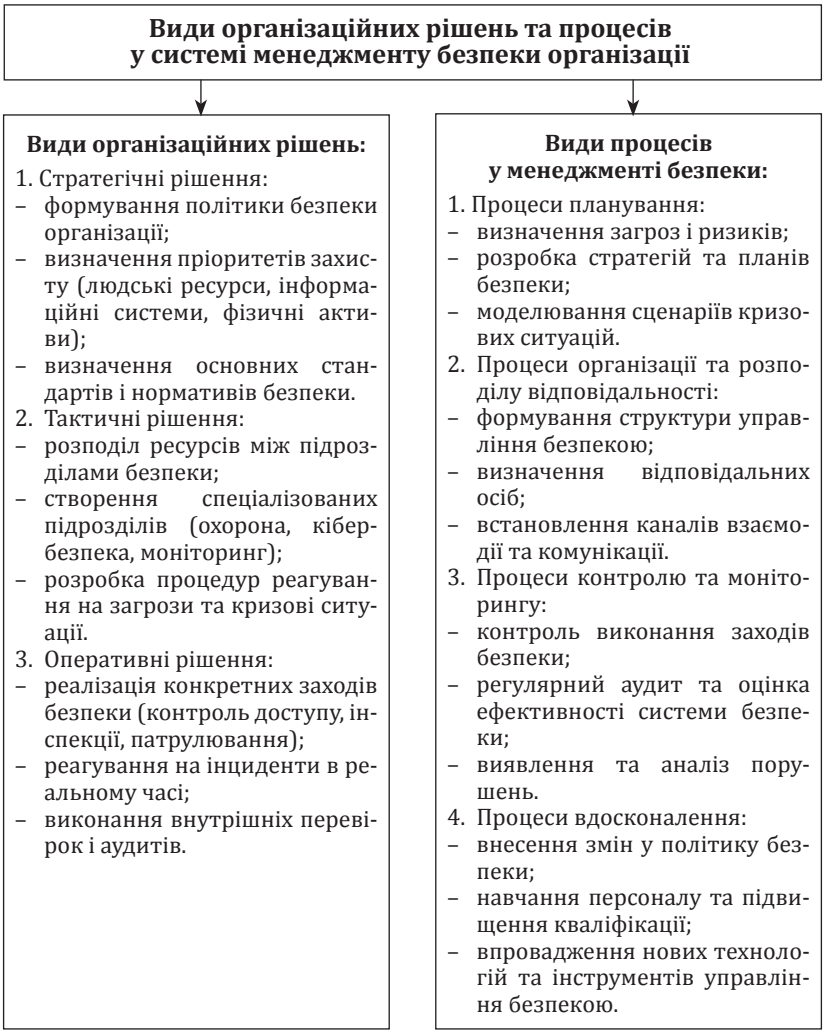


Рис. 2.2. Види організаційних рішень та процесів

Суб'єктами системи менеджменту організаційної безпеки є власники підприємства, вищий менеджмент, керівники структурних підрозділів, служби безпеки, працівники підприємства, державні органи контролю та нагляду, правоохоронні органи, партнери, постачальники, інвестори, підрядники. Об'єктами системи менеджменту організаційної безпеки є майно підприємства, фінансові ресурси, інформаційні ресурси, персонал, технології та ноу-хау, виробничі процеси, комерційні інтереси, ділова репутація, стратегічні цілі, корпоративна культура, екологічна безпека, правові відносини, клієнтська база (див. тему 1).

Потенціал безпеки являє собою інтегральну характеристику організації, яка поєднує наявні знання, сучасні технології, практичний досвід та організаційні спроможності, спрямовані на забезпечення стійкості функціонування та розвитку. Він відображає готовність підприємства вчасно ідентифікувати загрози, адекватно на них реагувати та забезпечувати адаптацію до нових умов зовнішнього середовища. Сформований потенціал безпеки створює основу для побудови дієвої системи захисту економічних, інформаційних та виробничих інтересів організації, а також визначає її здатність до інноваційного оновлення та підтримання конкурентоспроможності навіть за умов підвищеної ризикованості середовища.

Культурна безпека організації ґрунтується на системі спільних цінностей, норм і правил поведінки, що формуються у трудовому колективі та визначають позицію працівників щодо питань захисту і відповідального ставлення до ресурсів та процесів. Вона забезпечує створення атмосфери довіри, взаємної підтримки та усвідомленого дотримання безпекових вимог, що мінімізує ризики, пов'язані з людським фактором. Високий рівень культурної безпеки сприяє активній участі персоналу у виявленні загроз, їх попередженні та реалізації захисних заходів, перетворюючи безпеку на невід'ємний елемент корпоративної культури та щоденної діяльності організації.

Моніторинг та контроль системі менеджменту безпеки забезпечують не лише виявлення відхилень у поточному стані захисту, а й своєчасне реагування на них через адаптацію управлінських рішень, що дозволяє підтримувати

стабільність та мінімізувати ризики. Основними цілями моніторингу та контролю є:

– своєчасне виявлення внутрішніх і зовнішніх загроз;
– оцінка результативності реалізованих заходів безпеки;
– виявлення слабких місць у системі захисту;
– оперативне коригування політик, процедур та ресурсного забезпечення;
– підтримання відповідності діяльності організації нормативним і законодавчим вимогам;
– забезпечення прозорості та підзвітності у сфері безпеки.

2.2. Етапи формування системи менеджменту безпеки

Для сучасних підприємств та організацій формування чітких етапів системи менеджменту є ключовою умовою для забезпечення комплексного та системного підходу до захисту та формування ефективної стратегії безпеки. Чіткі етапи дозволяють узгодити стратегію і практичні дії, забезпечивши послідовність від виявлення загроз до контролю результатів і коригування заходів. Завдяки цьому підприємство отримує можливість своєчасно реагувати на ризики, раціонально використовувати ресурси та підтримувати стабільність у мінливому середовищі. Назагал можна виділити сім основних етапів процесу формування системи безпеки організації:

1. Перший етап – на якому проводиться аналіз поточного стану безпеки організації. Це включає виявлення основних загроз, вразливостей, ризиків та аналіз існуючих засобів захисту. Використовуються методи аудиту безпеки, SWOT-аналізу та інших інструментів оцінки ризиків для отримання чіткого уявлення про наявну ситуацію. Ретельний аналіз дає змогу сформувати обґрунтовану базу для прийняття подальших управлінських рішень у сфері безпеки.

2. Другий етап – визначення об'єктів та суб'єктів безпеки. Після аналізу слід з'ясувати, які ресурси організації потребують захисту (об'єкти безпеки), а також хто відповідатиме за реалізацію заходів безпеки (суб'єкти безпеки). Це можуть бути фізичні активи, інформаційні ресурси, персонал,

фінансові активи тощо. Чітке розмежування об'єктів і суб'єктів допомагає уникнути дублювання функцій і підвищує ефективність управління.

3. Третій етап передбачає розробку політики безпеки, яка буде мати короткостроковий або довгостроковий характер. На цьому етапі формується загальна політика безпеки організації, яка визначає стратегічні цілі, принципи та правила управління безпекою. Політика має бути документально оформлена і затверджена керівництвом організації, а також вона слугує базою для розробки детальних процедур і заходів з безпеки. Важливо, щоб політика відповідала специфіці діяльності підприємства та враховувала чинні нормативно-правові вимоги.

4. Четвертий етап – планування заходів безпеки, які включають визначення конкретних кроків, необхідних для реалізації політики безпеки організації. Це можуть бути технічні, організаційні, кадрові та інші заходи, що спрямовані на зменшення ризиків та підвищення рівня захищеності. Планування передбачає також визначення ресурсів, відповідальних осіб і терміни виконання. Якісне планування дає змогу уникнути зайвих витрат і забезпечити оптимальний розподіл ресурсів.

5. П'ятий етап – реалізація заходів безпеки через впровадження їх у діяльність, або виконання певних функціональних елементів (контроль, аудит чи аналіз). Це може включати встановлення технічних засобів захисту, проведення навчань для персоналу, оновлення процедур і політик тощо. Реалізація повинна бути систематичною та відповідати затвердженим планам. Основним аспектом є контрольованість процесу впровадження для досягнення очікуваних результатів.

6. Шостий етап пов'язаний із моніторингом та контролем і є критично важливими для забезпечення ефективності системи менеджменту безпеки. Це включає регулярне спостереження за виконанням заходів з безпеки, оцінку ефективності впроваджених засобів захисту, а також своєчасне виявлення і реагування на нові загрози. Системний моніторинг допомагає оперативно адаптувати політику та заходи безпеки до змін у зовнішньому та внутрішньому середовищі.

7. Сьомий, завершальний, етап – оцінка ефективності системи безпеки та внесення коректив. Проводиться аналіз результатів, досягнутих у сфері безпеки, визначаються слабкі місця та можливості для покращення. За потреби політики, процедури і заходи з безпеки коригуються для підвищення їхньої ефективності. Цей етап формує основу для постійного розвитку системи безпеки та забезпечує її відповідність сучасним викликам.

Розглянемо основні цілі, які повинні досягатися на кожному етапі з метою забезпечення ефективної системи менеджменту безпеки організації, враховуючи сучасний стан економіки і ризиків, що впливають на діяльність організацій (табл. 2.1).

Різні суб'єкти системи менеджменту безпеки можуть бути залучені до виконання окремих етапів, залежно від їхніх функцій, компетенцій та відповідальності. Так, аналітичні підрозділи забезпечують оцінку ризиків, технічні служби відповідають за реалізацію захисних заходів, а керівництво визначає політику та стратегічні пріоритети безпеки. Водночас основна роль у забезпеченні цілісності й ефективності всієї системи належить керівництву організації, яке координує дії всіх учасників та приймає ключові управлінські рішення.

При цьому в процесі формування та реалізації етапів системи менеджменту безпеки доцільно дотримуватися таких принципів-правил, як:

– системність та комплексність підходу до управління ризиками;

– пріоритет превентивних заходів над реактивними;

– адаптивність системи безпеки до змін зовнішнього та внутрішнього середовища;

– витрати на безпеку мають бути співмірними з потенційними ризиками та збитками;

– відповідальність і чіткий розподіл повноважень між суб'єктами безпеки;

– безперервність моніторингу та вдосконалення механізмів захисту;

– прозорість та документальне закріплення прийнятих рішень і процедур.

Таблиця 2.1

Цілі етапів формування системи безпеки організації

Етап формування системи безпеки організації	Основні цілі
Дослідження можливостей ефективного розміщення емісії акцій, яка планується (Етап I: Аналіз та планування)	Всебічна оцінка внутрішнього та зовнішнього середовища, ідентифікація критичних активів, аналіз існуючих вразливостей, визначення стратегічних пріоритетів захисту.
Визначення цілей емісії (Етап II: Визначення цілей безпеки)	Чітке формулювання бажаного рівня захищеності (наприклад, цільовий рівень толерантності до ризику), узгодження цілей безпеки зі загальною місією та стратегією підприємства.
Визначення обсягу емісії (Етап III: Оцінка та ресурсне забезпечення)	Розрахунок необхідного бюджету та обсягу ресурсів (кадрових, технічних) для реалізації системи безпеки, обґрунтування інвестицій у захисні механізми.
Визначення номіналу, видів і кількості емітованих акцій (Етап IV: Проєктування системи)	Розробка детальної архітектури системи безпеки, вибір конкретних засобів захисту (технічних, організаційних, правових), формалізація політик та процедур.
Оцінка вартості акціонерного капіталу, який залучається (Етап V: Впровадження та аудит)	Практичне розгортання захисних механізмів, інтеграція підсистем безпеки в операційну діяльність, проведення внутрішнього аудиту для перевірки відповідності встановленим стандартам.
Визначення ефективних форм андеррайтингу (Етап VI: Моніторинг та вдосконалення)	Встановлення системи постійного контролю за рівнем загроз, регулярний перегляд та оновлення політик безпеки, забезпечення безперервного навчання персоналу, підтримка культури безпеки.
Етап VII: Забезпечення безперервності та організаційної стійкості (Resilience)	Розробка та тестування планів відновлення після катастроф (DRP) та забезпечення безперервності бізнесу (BCP); регулярне проведення аудиту та перевірки на проникнення (penetration testing)

Це дозволяє забезпечити узгодженість дій усіх учасників процесу та підвищити ефективність функціонування системи загалом.

2.3. Напрями та методи оцінки безпеки організації

Оцінка безпеки організації є ключовим інструментом, що дозволяє визначити поточний стан захищеності її ресурсів, процесів і персоналу. Вона передбачає виявлення вразливостей, ідентифікацію потенційних загроз і визначення рівня готовності до їх подолання. Такий аналіз створює основу для формування обґрунтованих управлінських рішень у сфері безпеки та допомагає з'ясувати, які напрями потребують першочергового зміцнення.

Важливість оцінки полягає також у забезпеченні стабільності та стійкості функціонування підприємства. Завдяки своєчасній і якісній діагностиці безпеки можна уникати значних фінансових втрат, зберігати репутацію та підвищувати конкурентоспроможність на ринку. Крім того, вона сприяє формуванню довіри з боку партнерів, клієнтів і державних органів, що особливо актуально в умовах зростаючої складності бізнес-середовища.

Оцінка безпеки виконує роль стратегічного орієнтира в розвитку організації, оскільки дає змогу прогнозувати можливі ризики та адаптувати систему захисту до нових викликів. Вона забезпечує ефективне використання ресурсів, допомагає оптимізувати структуру заходів безпеки та формує основу для безперервного вдосконалення системи менеджменту. В результаті підприємство отримує не лише інструмент контролю, а й механізм розвитку, що інтегрує безпеку у загальну стратегію діяльності.

Визначення сутності оцінки безпеки організації полягає у комплексному та систематичному процесі кількісного та якісного аналізу поточного стану захищеності життєво важливих інтересів підприємства від цілого спектру внутрішніх і зовнішніх загроз. Цей процес охоплює не просто інвентаризацію наявних систем захисту, а й виявлення вразливостей, розрахунок імовірності настання ризикових подій

та оцінку їх потенційного збитку для фінансових, операційних, кадрових та репутаційних активів. Кінцева мета оцінки безпеки полягає у встановленні фактичного рівня захищеності порівняно з бажаним (цільовим) рівнем і наданні керівництву обґрунтованих рекомендацій із оптимізації інвестицій у заходи безпеки, забезпечуючи адекватність захисних механізмів існуючим загрозам.

Напрями оцінки безпеки організації охоплюють ключові сфери її функціонування та дозволяють комплексно визначити рівень захищеності організації на різних рівнях, а саме:

– фінансова безпека – аналіз платоспроможності, ліквідності, стійкості фінансових потоків та здатності протистояти зовнішнім економічним загрозам;

– інформаційна безпека – перевірка захищеності даних, IT-інфраструктури, корпоративних комунікацій та механізмів кіберзахисту;

– кадрова безпека – оцінка професійного рівня персоналу, його лояльності, кваліфікації, а також ризиків, пов'язаних із внутрішніми загрозами чи плинністю кадрів;

– матеріально-технічна безпека – визначення рівня захисту виробничих потужностей, обладнання, будівель та іншої матеріальної бази;

– правова безпека – оцінка дотримання чинного законодавства, наявності правових ризиків, захисту інтересів у контрактах та угодах;

– екологічна безпека – аналіз відповідності діяльності екологічним стандартам та оцінка впливу на навколишнє середовище;

– репутаційна безпека – моніторинг іміджу організації у суспільстві, ЗМІ та серед партнерів, а також ризиків, що можуть зашкодити довірі до бренду.

Важливим елементом системи ефективного управління економічною безпекою підприємства є вибір та застосування методів оцінки рівня економічної безпеки, які можна класифікувати за трьома групами: фінансові; комплексні; методи, що враховують вплив загроз (рис. 2.3).

Враховуючи значну кількість та різноманітність сучасних підходів до оцінювання економічної безпеки підприємства, їх доцільно систематизувати за основними цілями

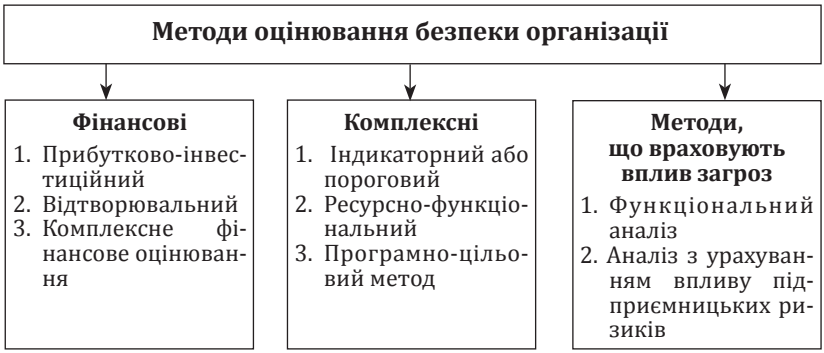


Рис. 2.3. Комплекс методів оцінки безпеки організації

аналізу та рівнями проведення оцінки. Така класифікація дає змогу більш чітко визначити інструменти, що застосовуються у практиці управління безпекою, а також адаптувати їх до специфіки діяльності конкретної організації (табл. 2.2).

Групування методів за критерієм мети дає змогу розділити їх на ті, що спрямовані на виявлення рівня поточної безпеки, прогнозування її стану в майбутньому, або на визначення резервів для зміцнення захисного потенціалу підприємства. У свою чергу, класифікація за рівнями проведення оцінки відображає можливість застосування методів на макро-, мезочи мікрорівні, завдяки чому можна враховувати як загальнодержавні тенденції, так і специфічні умови функціонування окремих підприємств.

Така структуризація забезпечує системність підходу до аналізу безпеки, сприяє вибору найбільш ефективних інструментів для прийняття управлінських рішень і підвищує точність прогнозів щодо розвитку потенційних загроз.

Алгоритм інтегральної діагностики рівня економічної безпеки підприємства включає низку послідовних кроків. Спершу формується ієрархічна система інтегральної оцінки, яка забезпечує упорядкування всіх елементів аналізу. Далі складаються матриці переваг показників, що дозволяє визначити їх відносну значущість та пріоритетність у загальній системі оцінювання. Наступним етапом є встановлення вагових коефіцієнтів для ключових індикаторів, після чого обираються показники, які відображають окремі складові

Таблиця 2.2

Методи оцінки безпеки організації та їх характеристика

Методи оцінки	Основні ознаки методу	Недоліки методу
Індикаторний	Суть методу полягає у відстеженні динаміки показників, що характеризують стан безпеки підприємства, та їхньому зіставленні з нормативними, референтними чи галузевими орієнтирами. Він дає можливість виявити відхилення у роботі підприємства та оцінити рівень його стійкості.	Відсутність єдиних критеріїв для різних галузей, складність визначення меж допустимих відхилень показників, недостатня точність у врахуванні впливу зовнішнього та внутрішнього середовища.
Функціонально-ресурсний	Метод базується на оцінці окремих елементів системи економічної безпеки, які можуть групуватися за функціональними завданнями (фінансова, інформаційна, кадрова безпека тощо) або за ресурсною складовою (матеріальні, інформаційні, фінансові ресурси). Такий підхід дозволяє простежити роль кожного елементу в загальній системі захисту.	Виникають труднощі при формалізації функціональних та ресурсних характеристик на рівні окремого підприємства, що знижує об'єктивність оцінки.
Економіко-математичне забезпечення	Метод заснований на застосуванні математичних моделей, що описують поведінку системи економічної безпеки в умовах невизначеності та прогнозованого впливу внутрішніх і зовнішніх чинників. Дозволяє будувати сценарії розвитку та оцінювати потенційні ризики.	Труднощі з побудовою моделей через потребу в реальних статистичних даних, а також проблеми формалізації ресурсних і функціональних складових у різних організаціях.

безпеки (фінансову, інформаційну, кадрову, правову, технічну та інші). Паралельно визначаються коефіцієнти значимості кожної функціональної складової, а завершальним кроком виступає розрахунок інтегрального індикатора, що відображає загальний рівень економічної безпеки підприємства.

Стратегія економічної безпеки організації являє собою сукупність довгострокових управлінських рішень, спрямованих на протидію негативним впливам внутрішнього та зовнішнього середовища. Вона визначає ключові напрями розвитку системи управління безпекою та закріплює пріоритети у сфері захисту інтересів підприємства.

Оцінювання рівня безпеки є важливим елементом управлінської практики, оскільки воно допомагає виявити критичні вразливості, оцінити масштаби потенційних ризиків і своєчасно запровадити заходи задля їх мінімізації. Для цього застосовуються різні **методичні підходи**, вибір яких залежить від характеру можливих загроз, особливостей діяльності та об'єктів, що потребують захисту:

1. Метод SWOT-аналізу. SWOT-аналіз є універсальним інструментом стратегічного планування, що дозволяє оцінити сильні та слабкі сторони організації, а також зовнішні можливості й загрози. Його використання допомагає сформувати ефективну стратегію розвитку та мінімізувати ризики. Розшифровка аналізу подана на рисунку 2.4.

SWOT-аналіз застосовується підприємствами та організаціями різного масштабу – від невеликих фірм до транснаціональних корпорацій. Його використовують у різних сферах діяльності, зокрема під час створення нових продуктів, виходу на нові ринки, а також у процесах управління змінами чи оцінки потенційних ризиків. Ефективність цього методу

	КОРИСНО для досягнення цілей	ШКОДИТЬ, впливає на діяльність та стан
ВНУТРІШНІ властивості організації	СИЛЬНІ СТОРОНИ (*Strengths*) – оцінка внутрішніх ресурсів і можливостей, які підвищують рівень безпеки	СЛАБКОСТІ (*Weaknesses*) – виявлення внутрішніх вразливостей, які можуть загрожувати організації
ЗОВНІШНІ властивості оточення	МОЖЛИВОСТІ (*Opportunities*) – зовнішні фактори, які можна використовувати для підвищення рівня безпеки	ЗАГРОЗИ (*Threats*) – зовнішні фактори, які можуть негативно вплинути на безпеку організації

Рис. 2.4. Характеристика SWOT-аналізу

залежить від конкретних умов та характеру проблем, які необхідно вирішити. Найбільшу цінність SWOT-аналіз має у ситуаціях динамічних змін на ринку або при розробці нових стратегічних ініціатив, натомість у стабільному середовищі його роль може бути менш суттєвою.

Завдяки універсальності цей інструмент адаптується до різних сфер бізнесу. Наприклад, у високотехнологічних секторах, де швидко відбуваються інновації та оновлення технологій, SWOT-аналіз дозволяє гнучко реагувати на зміни та визначати перспективні напрями розвитку. Тимчасом у більш традиційних галузях його доцільно застосовувати для вдосконалення існуючих процесів, підвищення ефективності та пошуку резервів для оптимізації. Таким чином, результативність використання методу безпосередньо пов'язана з особливостями ринкового середовища та галузевими умовами.

Аналогічні методи для аналізу діяльності та планування діяльності організації, їх опис, переваги та недоліки наведено в додатку А.

2. Метод оцінки ризиків (*Risk Assessment*) – включає ідентифікацію, аналіз і оцінку ризиків, які можуть впливати на організацію. За допомогою цього методу оцінюється ймовірність виникнення ризиків та їхній можливий вплив на діяльність підприємства. Метод оцінки ризиків передбачає систематичний процес виявлення потенційних загроз, їх класифікацію та подальший аналіз можливих наслідків для організації. Він охоплює кілька ключових етапів: ідентифікацію ризиків, аналіз їхніх джерел і причин, визначення ймовірності настання ризикових подій та вимірювання рівня їхнього впливу на бізнес-процеси. Особлива увага приділяється не лише зовнішнім факторам (ринковим, політичним, правовим), а й внутрішнім (операційним, кадровим, фінансовим). У кількісній оцінці часто використовується базова формула визначення рівня ризику:

$$R = P \times I, \tag{2.1}$$

де R – рівень ризику, P – ймовірність настання події, I – інтенсивність або масштаб можливих збитків.

Застосування такої моделі допомагає встановити пріоритетність ризиків, розробити план їх попередження

та мінімізації, а також ефективно розподілити ресурси організації. Метод оцінки ризиків є фундаментальним інструментом у сфері управління безпекою та стратегічного планування, оскільки дає змогу знизити невизначеність і підвищити стійкість підприємства в умовах змінного середовища.

3. Аудит безпеки (*Security Audit*) – це комплексна оцінка діючих заходів, політик і процедур безпеки з метою перевірки їхньої ефективності та відповідності встановленим стандартам і нормативним вимогам. Він може проводитися як внутрішніми силами, так і зовнішніми незалежними експертами.

У процесі аудиту аналізуються такі складові: система контролю доступу до приміщень і ресурсів, рівень захисту інформаційних систем, збереження конфіденційних даних, кадрові процедури та політика управління персоналом, відповідність технічних засобів охорони вимогам, а також готовність до реагування на інциденти. Результати аудиту дають змогу виявити слабкі місця, оцінити рівень ризиків та сформувати рекомендації щодо їх усунення.

4. Аналіз загроз та вразливостей (*Threat and Vulnerability Analysis*) – це метод оцінки безпеки, спрямований на виявлення слабких місць організації та факторів, що можуть бути використані для порушення її стабільності. Його головна мета полягає у своєчасному визначенні потенційних точок ризику, які здатні призвести до втрати ресурсів, витоку інформації чи зниження ефективності бізнес-процесів.

Процес аналізу включає декілька етапів: ідентифікацію можливих загроз (наприклад, кібернапади, несанкціонований доступ, технічні збої, внутрішні порушення), дослідження слабких сторін у системах захисту, визначення ймовірності використання цих вразливостей та оцінку можливих наслідків. Для проведення аналізу застосовуються як експертні методи, так і спеціалізовані програмні інструменти: сканери вразливостей IT-інфраструктури, системи тестування проникнення (penetration testing), а також інструменти моделювання загроз. Результати аналізу дають змогу організації не лише усунути виявлені недоліки, але й сформувати превентивні заходи, розробити оновлені політики безпеки, посилити контроль доступу, модернізувати технічні

засоби захисту та підвищити готовність персоналу до реагування на кризові ситуації.

5. Метод сценаріїв (*Scenario Analysis*) – це інструмент оцінювання та управління ризиками, який ґрунтується на моделюванні можливих варіантів розвитку подій у майбутньому. Його сутність полягає у створенні декількох сценаріїв, що враховують різні поєднання загроз, невизначеностей та факторів впливу на організацію. Такий підхід допомагає визначити потенційні ризики, спрогнозувати їхні наслідки й розробити ефективні стратегії реагування. Метод широко використовується в системі менеджменту безпеки для підготовки до кризових ситуацій, стратегічного планування та підвищення стійкості підприємства. Основні етапи застосування методу сценаріїв представлено на рисунку 2.5.

6. Індикативний метод оцінки економічної безпеки ґрунтується на аналізі динаміки ключових показників діяльності підприємства та їх відповідності нормативним чи референтним значенням. Він дозволяє визначити відхилення від встановлених критеріїв і виявити загрози як внутрішнього, так і зовнішнього середовища. Основною перевагою цього підходу є його наочність і можливість швидкої діагностики рівня безпеки, хоча він потребує узгоджених стандартів для точності оцінювання.

7. Матричний метод оцінки ризиків полягає у визначенні рівня ризику через поєднання двох ключових параметрів: ймовірності настання події та ступеня її наслідків для організації. Для цього будується матриця ризиків, де по горизонталі відображається шкала ймовірності (низька, середня, висока), а по вертикалі – масштаб наслідків (незначні, середні, критичні). Поєднання цих двох показників дозволяє віднести ризик до певної категорії: прийнятний, керований або критичний, що вимагає негайного реагування.

8. Метод експертних оцінок ґрунтується на залученні фахівців, які мають відповідні знання та практичний досвід у сфері безпеки чи управління ризиками, для формування якісної або кількісної оцінки стану безпеки. Суть методу полягає у зборі, узагальненні та систематизації думок експертів щодо ймовірності настання подій, можливих наслідків чи ефективності заходів протидії.

Рис. 2.5. Перелік основних етапів
застосування методу сценаріїв

Зазвичай використовуються такі інструменти, як анкетування, інтерв'ю, метод Делфі або колективні дискусії.

Основна перевага цього підходу – можливість залучити професійний досвід та інтуїцію спеціалістів у ситуаціях, де відсутні точні статистичні дані чи складно застосувати математичні моделі. Водночас недоліком є суб'єктивність оцінок, що може призвести до розбіжностей у результатах. Отже, метод експертних оцінок працює за таким планом:

1. Вибираємо об'єкт для експертної оцінки.
2. Вибираємо параметри для порівняння.
3. Визначаємо вагу кожного параметра.
4. Задаємо порівняльну шкалу.
5. Порівнюємо.

За допомогою таблиці виражаємо оцінки експертів (їх число залежить від вибору самого підприємства, оцінка також може бути від 1–100 балів) (табл. 2.3).

Таблиця 2.3

Таблиця заповнення методом експертних оцінок

Експерт	Показник 1	Показник 2	Показник 3	Показник 4	Показник 5	Сума
Експерт 1	бали	бали	бали	бали	бали	=
Експерт 2	бали	бали	бали	бали	бали	=
Експерт 3	бали	бали	бали	бали	бали	=

9. Метод бенчмаркінгу передбачає систематичне порівняння рівня безпеки організації з провідними стандартами, найкращими практиками галузі або показниками конкурентів. Такий підхід дозволяє визначити відставання у впроваджених заходах, виявити слабкі сторони та знайти напрямки для вдосконалення системи захисту. Бенчмаркінг допомагає адаптувати успішні рішення інших компаній, підвищити ефективність використання ресурсів і забезпечити відповідність сучасним вимогам безпеки. В підсумку організація отримує можливість не лише підвищити власний рівень захищеності, а й зміцнити конкурентні переваги на ринку.

Питання для самоконтролю

1. У чому полягає сутність оцінки економічної безпеки організації та чому вона є важливою для розвитку підприємства?
2. Які є основні напрями оцінки безпеки організації?
3. У чому полягають переваги та недоліки індикаторного методу оцінки економічної безпеки?
4. На яких засадах ґрунтується функціонально-ресурсний підхід до оцінки безпеки підприємства?
5. Які є особливості використання економіко-математичного забезпечення для оцінки рівня економічної безпеки?
6. У чому полягає алгоритм інтегральної оцінки рівня економічної безпеки підприємства?

7. Які принципи та завдання враховуються під час SWOT-аналізу?

8. У чому полягає сутність методу оцінки ризиків і які основні етапи його застосування?

9. Які завдання виконуються в межах аудиту безпеки, аналізу загроз та вразливостей?

10. У чому полягає значення методів сценарного аналізу, експертних оцінок та бенчмаркінгу для підвищення рівня безпеки організації?

Тестові завдання

1. Що є головною метою оцінки економічної безпеки організації?

а) Виявлення конкурентів на ринку;

б) визначення рівня фінансової стабільності та захищеності від загроз;

в) підвищення продуктивності праці персоналу;

г) зменшення кількості виробничих витрат.

2. У чому полягає сутність індикаторного методу оцінки безпеки?

а) У порівнянні результатів з кращими практиками інших підприємств;

б) у використанні набору показників та їх порівнянні з нормативними чи референтними значеннями;

в) у проведенні анкетування та експертних інтерв'ю;

г) у прогнозуванні можливих сценаріїв розвитку подій.

3. Який недолік має функціонально-ресурсний підхід до оцінки безпеки?

а) Висока складність обчислень та побудови моделей;

б) недостатня аргументація при формалізації функціональних і ресурсних складових на окремих підприємствах;

в) залежність результатів від суб'єктивних оцінок експертів;

г) надмірна кількість індикаторів для аналізу.

4. Що є основою економіко-математичного підходу до оцінки безпеки?

а) Використання анкет і соціологічних методів;

б) проєктування моделей поведінки економічної системи в умовах прогнозованого впливу зовнішніх і внутрішніх факторів;

в) виключно порівняння показників прибутковості та рентабельності;

г) проведення спеціалізованих експертних опитувань.

5. Який етап входить до алгоритму інтегральної оцінки безпеки підприємства?

а) Підбір спеціалізованих консультантів;

б) побудова ієрархічної структури оцінювання показників економічної безпеки;

в) проведення маркетингових досліджень ринку;

г) аналіз конкурентних переваг у галузі.

6. У чому полягає цінність SWOT-аналізу для організації?

а) У збиранні статистики щодо виробництва;

б) у визначенні сильних і слабких сторін, а також можливостей і загроз в умовах змін ринку;

в) у формуванні фінансової звітності та балансів;

г) у забезпеченні відповідності міжнародним стандартам.

7. Що передбачає метод оцінки ризиків (Risk Assessment)?

а) Виключно перевірку систем безпеки підприємства;

б) ідентифікацію, аналіз і кількісне оцінювання можливих ризиків з розрахунком їх ймовірності та впливу;

в) оцінку відповідності законодавчим нормам;

г) визначення сильних сторін персоналу організації.

8. Який аспект найчастіше перевіряється під час аудиту безпеки?

а) Рівень інноваційності продукції підприємства;

б) поточний стан політик, процедур і технічних засобів безпеки та їх відповідність стандартам;

в) взаємодія підприємства з конкурентами на ринку;

г) загальний рівень прибутковості бізнесу.

9. Метою аналізу загроз і вразливостей є:

а) пошук інвесторів для розвитку підприємства;

б) виявлення слабких місць систем захисту, які можуть бути використані для здійснення атак або несанкціонованого доступу;

в) формування кадрової політики та підбір персоналу;

г) зниження виробничих витрат на енергоносії.

10. У чому криється сутність бенчмаркінгу при оцінці безпеки організації?

а) У зборі конфіденційної інформації конкурентів;

б) у порівнянні власних показників безпеки з найкращими галузевими практиками або результатами інших підприємств;

в) у проведенні соціологічних опитувань персоналу;

г) у створенні інноваційних технологій захисту.

Практичні завдання

Завдання 1.

Підприємство «Техноромакс» займається виробництвом електронних компонентів і активно виходить на нові зарубіжні ринки. За минулий рік компанія зіткнулася з низкою проблем:

1. Під час аудиту було виявлено серйозні вразливості в ІТ-системах, що створюють ризик витоку конфіденційної інформації.
2. Через зростання конкуренції та тиск постачальників збільшилися фінансові ризики, а рентабельність скоротилася майже на 15%.
3. На підприємстві почастішали випадки порушення трудової дисципліни: конфлікти між відділами, зростання кількості прогулів та зниження мотивації персоналу.
4. Ринок, на який планується вихід, має нестабільне законодавче середовище, що посилює правові ризики.
5. Керівництво доручило службі економічної безпеки провести оцінку стану підприємства, визначити ключові загрози та розробити заходи щодо мінімізації ризиків.

1. На основі наведеної ситуації складіть SWOT-аналіз безпеки підприємства, виділивши сильні та слабкі сторони, можливості та загрози.

2. Розробіть три сценарії розвитку подій (оптимістичний, песимістичний та базовий) і коротко опишіть наслідки для діяльності компанії за кожним із них.

3. Запропонуйте комплекс заходів з підвищення рівня економічної безпеки «Техноромакс», розподіливши їх за сферами: інформаційна, фінансова, кадрова та правова.

Завдання 2.

Фінансова установа «Ексель» планує впровадити нову систему онлайн-банкінгу для клієнтів. Під час підготовки було виявлено:

– застаріле програмне забезпечення на частині серверів;
– відсутність двофакторної аутентифікації для користувачів;
– високий рівень довіри до сторонніх підрядників, які мають доступ до внутрішніх систем.

1. Визначте основні загрози та вразливості у цій ситуації.

2. Запропонуйте методи оцінки ризиків, які доцільно використати для аналізу проблеми.

3. Сформулюйте три ключові рекомендації для підвищення рівня інформаційної та кадрової безпеки банку.

Завдання 3.

Виробниче підприємство «Таско», що спеціалізується на хімічній продукції, розглядає три можливі сценарії розвитку:

Сценарій А: Розширення ринку збуту шляхом експорту в інші країни.

Сценарій В: Впровадження нових технологій автоматизації виробництва.

Сценарій С: Оптимізація витрат і скорочення частини персоналу.

Проте існують ризики: посилення екологічного контролю, загроза кіберзламів систем управління виробництвом, можливі страйки працівників.

1. Визначте фактори ризику для кожного сценарію.

2. Опишіть, як метод сценарного аналізу допоможе оцінити ймовірність та наслідки цих ризиків.

3. Запропонуйте варіанти дій, які дозволять мінімізувати негативні наслідки обраного сценарію.

ТЕМА 3
УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

3.1. Сутність управління фінансовою безпекою організації
3.2. Методичні підходи до оцінки фінансового стану та її показники
3.3. Інформаційне забезпечення фінансової безпеки підприємства
3.4. Чинники забезпечення фінансової безпеки організації

Основні поняття і терміни: фінансова безпека, управління фінансовою безпекою, фінансові показники, фінансові ризики, ліквідність, платоспроможність, прибутковість, заборгованість, грошові потоки, ризик банкрутства, фінансові інструменти, грошові потоки.

3.1. Сутність управління фінансовою безпекою організації

Фінансова безпека організації є ключовим елементом її економічної стабільності та конкурентоспроможності. Вона відображає здатність підприємства ефективно формувати, розподіляти та використовувати фінансові ресурси, протистояти внутрішнім і зовнішнім загрозам, а також забезпечувати стале зростання в умовах ринкової невизначеності. Наявність належного рівня фінансової безпеки сприяє підвищенню довіри інвесторів і партнерів, гарантує виконання зобов'язань перед кредиторами та державою, а також знижує ризик банкрутства. Таким чином, фінансова безпека виступає основою стабільного фінансово-економічного стану підприємства та передумовою його довгострокового розвитку.

У сучасних економічних джерелах немає єдиного підходу до трактування поняття «фінансова безпека». Так, на думку О. Барановського, фінансова безпека підприємства може розглядатися як стан забезпеченості організації необхідними фінансовими ресурсами, які дають змогу задовольняти її потреби та виконувати взяті зобов'язання.

Вона передбачає підтримання збалансованості та стійкості до внутрішніх і зовнішніх деструктивних чинників, здатність протидіяти фінансовому тиску ззовні, а також створює умови для збереження фінансової стабільності, ефективного функціонування та сталого економічного розвитку.

Згідно з І. Бланком, фінансова безпека підприємства може тлумачитись як якісно та кількісно визначений рівень його фінансового стану, який гарантує надійний захист ключових та збалансованих фінансових інтересів від наявних і можливих загроз як внутрішнього, так і зовнішнього походження. Її параметри формуються відповідно до фінансової стратегії та концепції підприємства, забезпечуючи необхідні умови для стабільного розвитку та підтримки стійкого зростання як у короткостроковій, так і в довгостроковій перспективі.

О. Ареф'єва та Т. Кузенко фінансову безпеку підприємства розглядають як стан найбільш раціонального та результативного використання корпоративних ресурсів, що проявляється у досягненні оптимальних показників прибутковості та рентабельності діяльності, ефективності управління, правильного розподілу й застосування основних і оборотних активів. Вона також відображається у збалансованій структурі капіталу, стабільності виплат за цінними паперами та ринковій вартості корпоративних прав, яка виступає інтегральним індикатором поточного фінансово-господарського стану та перспектив подальшого розвитку підприємства як у технологічному, так і у фінансовому вимірі.

Г. Шиназі трактує фінансову безпеку підприємства як здатність підтримувати та розвивати економічні процеси корпорації, ефективно управляти ризиками її діяльності та мінімізувати можливі негативні наслідки. Він зазначає, що «важливою особливістю цієї категорії є її безперервність у часі: фінансова безпека не зникає, а лише трансформується залежно від змін у системі фінансів та взаємодії її складових елементів».

Отже, фінансова безпека організації – це такий стан її фінансової системи, за якого забезпечується стійкість та збалансованість грошових потоків, достатність фінансових ресурсів для виконання поточних і стратегічних зобов'язань, здатність протидіяти внутрішнім і зовнішнім ризикам,

а також створюються умови для стабільного функціонування та довгострокового економічного розвитку.

Управління фінансовою безпекою організації виступає одним із визначальних чинників її стабільної роботи та подальшого розвитку. Фінансова безпека засвідчує можливість підприємства підтримувати рівновагу у фінансовій сфері, не зважаючи на зовнішні чи внутрішні виклики. Основним завданням управління фінансовою безпекою є мінімізація ризиків, що здатні негативно вплинути на бізнес-процеси компанії, а також забезпечення її готовності діяти ефективно в умовах економічної турбулентності та ринкової непередбачуваності.

Серед головних елементів управління фінансовою безпекою слід виділити контроль і регулювання грошових потоків, оптимізацію витрат, роботу з дебіторською заборгованістю, реалізацію інвестиційних стратегій та захист капіталу від впливу зовнішніх факторів, зокрема кризових явищ чи правових змін. Важливими інструментами виступають фінансовий аналіз, ризик-прогнозування, страхування фінансових операцій, а також створення резервних фондів. Це формує стійкість підприємства до ймовірних фінансових загроз і забезпечує безперервність обігу коштів.

Система управління фінансовою безпекою вимагає постійного моніторингу стану компанії, що включає оцінку ключових фінансових показників, серед яких ліквідність, прибутковість та здатність до виконання зобов'язань. Такий підхід дозволяє своєчасно виявляти проблемні аспекти та приймати рішення щодо їх усунення. Водночас стратегічне фінансове планування дає змогу не лише реагувати на виклики, але й наперед формувати сприятливі умови для уникнення ризиків.

Управління фінансовою безпекою є комплексним процесом, який охоплює як оперативні заходи з контролю ресурсів, так і довготривалі стратегії зміцнення фінансової стійкості підприємства. Для його ефективності потрібен інтегрований підхід, що поєднує планування, управління ризиками та розробку надійних механізмів, спрямованих на захист бізнесу від можливих фінансових загроз.

З іншого боку, **управління фінансовою безпекою організації** – це цілеспрямований комплекс організаційних, методичних та управлінських заходів, який має на меті забезпечити стабільність фінансової системи, захист фінансових інтересів від потенційних внутрішніх і зовнішніх загроз, зменшення фінансових ризиків та створення передумов для сталого зростання компанії. Цей процес передбачає впровадження систем контролю, аналітику, стратегічне та операційне планування, адаптацію до змін зовнішнього середовища та прийняття превентивних рішень.

Об'єктом управління фінансовою безпекою організації є її фінансові ресурси, які включають активи, пасиви, грошові потоки, капітал, інвестиції та інші фінансові показники. Це також охоплює всі аспекти, пов'язані з їхньою ефективністю використання, збереженням та захистом від можливих внутрішніх і зовнішніх загроз. Управління фінансовими ресурсами спрямоване на забезпечення стабільної діяльності організації, незалежно від економічної нестабільності або ризиків на ринку.

Окрім фінансових ресурсів, до **об'єктів управління фінансовою безпекою** відносяться зобов'язання компанії, включаючи кредиторську та дебіторську заборгованість, інвестиційні проєкти, а також операції, що можуть створювати фінансові ризики. Сюди також входять питання ліквідності, платоспроможності та прибутковості, які впливають на фінансову стійкість організації.

Суб'єктами управління фінансовою безпекою організації є ті особи або органи, що беруть участь у процесах контролю, аналізу та захисту фінансових ресурсів підприємства (рис. 3.1).

Фінансова безпека відіграє вирішальну роль у діяльності організації, оскільки вона є фундаментом її економічної стійкості та незалежності. Суть цієї ролі полягає у забезпеченні такого стану фінансових ресурсів підприємства, який гарантує його здатність ефективно реалізовувати свої стратегічні цілі, зберігати платоспроможність та фінансову рівновагу в умовах внутрішніх і зовнішніх загроз. Фінансова безпека дає змогу компанії не лише мінімізувати ризики банкрутства чи фінансових втрат, але й підтримувати необхідний рівень

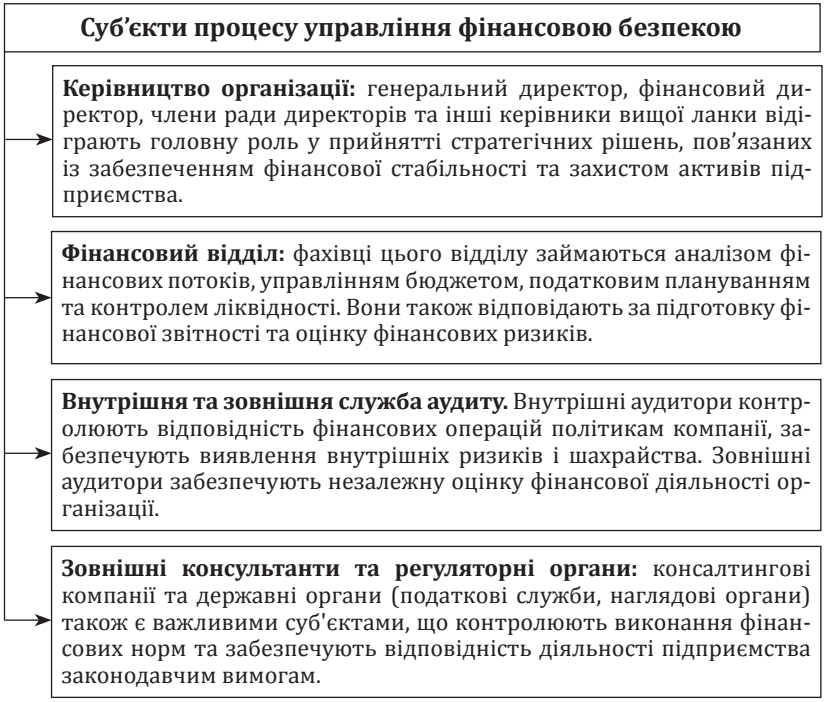


Рис. 3.1. Суб'єкти управління фінансовою безпекою організації

ліквідності для безперебійного функціонування, своєчасного виконання зобов'язань перед кредиторами, партнерами та державою, а також для фінансування операційних і капітальних витрат.

Крім того, фінансова безпека виконує функцію стратегічного ресурсу, дозволяючи організації приймати обґрунтовані інвестиційні рішення та використовувати сприятливі ринкові можливості. Вона забезпечує захист фінансових потоків від незаконного привласнення, шахрайства та нецільового використання, що підвищує довіру інвесторів і партнерів. Ефективне управління фінансовою безпекою також передбачає постійний моніторинг фінансових показників, прогнозування потенційних загроз (наприклад, валютних, кредитних чи інфляційних ризиків) та розробку механізмів

їх нейтралізації. Це перетворює фінансову безпеку з простої захисної функції на активний інструмент управління, який сприяє стійкому розвитку та зростанню конкурентоспроможності підприємства в довгостроковій перспективі.

До основних умов, **що забезпечують управління фінансовою безпекою організації,** можна віднести:

– гармонійне узгодження фінансових інтересів підприємства з інтересами його працівників, партнерів і зовнішнього середовища;

– створення стійкої та гнучкої фінансової системи, здатної протистояти внутрішнім і зовнішнім загрозам та підтримувати реалізацію стратегічних і тактичних завдань;

– збалансоване використання фінансових інструментів і технологій, які забезпечують ефективне управління ресурсами;

– постійний розвиток та адаптацію фінансової системи підприємства до змін ринкових умов і економічних викликів;

– наявність достатніх резервів і страхових механізмів, що підвищують здатність компанії протистояти кризовим явищам.

Функціональні цілі управління фінансовою безпекою організації включають:

– забезпечення фінансової стійкості, незалежності та максимальної ефективності діяльності;

– підтримку технологічної самостійності та посилення конкурентних переваг у використанні технічного потенціалу;

– підвищення результативності системи управління та оптимізацію бізнес-процесів;

– розвиток людського капіталу шляхом підвищення професійного рівня та кваліфікації персоналу;

– створення надійної системи правового захисту всіх аспектів фінансово-господарської діяльності;

– формування довгострокової стратегії інноваційного та інвестиційного розвитку, яка зміцнює фінансову стабільність у майбутньому.

Основні інструменти, які забезпечують процес ефективного управління фінансовою безпекою підприємства, подано на рис. 3.2.

Рис. 3.2. Перелік інструментів управління фінансовою безпекою

У процесі реалізації системи управління фінансовою безпекою підприємства, установи та організації розробляють стратегію управління фінансовою безпекою. Стратегія управління фінансовою безпекою є складовою загальної стратегії розвитку підприємства, оскільки визначає ключові напрями, джерела та об'єкти фінансування, а також формує основу для стабільності та стійкого зростання. Вона забезпечує узгодженість фінансових рішень із цілями організації, сприяє ефективному використанню ресурсів і дозволяє завчасно реагувати на зміни у зовнішньому середовищі. Вибір стратегії залежить від рівня фінансової безпеки підприємства, який визначається через аналіз фінансового стану, ідентифікацію ризиків та оцінку інтегральних показників.

Процес розроблення стратегії управління фінансовою безпекою складається з кількох ключових етапів. Спочатку визначаються довгострокові та короткострокові цілі, які формують основу майбутньої політики безпеки. Наступним кроком є комплексний аналіз зовнішнього середовища, що включає дослідження економічної ситуації, тенденцій фінансового ринку, динаміки законодавчих змін та впливу конкурентів. Паралельно проводиться внутрішня

діагностика, коли оцінюється фінансовий стан підприємства, його стійкість до ризиків, ефективність управління активами й зобов'язаннями, а також рівень ліквідності та платоспроможності. На основі цього формується перелік можливих загроз і визначаються фактори, які впливають на стабільність та розвиток організації.

Далі відбувається формування стратегічних альтернатив, тобто опрацювання кількох можливих сценаріїв управління фінансовою безпекою. Кожна альтернатива оцінюється за критеріями ефективності, ризиковості та відповідності ресурсним можливостям підприємства. Вибір оптимальної стратегії здійснюється з урахуванням реального рівня фінансової безпеки та прогнозованих змін у внутрішньому і зовнішньому середовищі. Після цього розробляється стратегічний портфель, що поєднує як довгострокові напрями (інвестиційна політика, диверсифікація фінансових потоків), так і короткотермінові заходи (захист грошових коштів, оптимізація витрат, створення резервів). Тож стратегічне планування є не лише механізмом адаптації підприємства до змін, а й інструментом проактивного формування умов для підвищення фінансової стійкості.

Завершальним етапом є контроль за виконанням стратегічних завдань і своєчасне внесення змін у разі відхилень фактичних результатів від запланованих. Таким чином, стратегія управління фінансовою безпекою охоплює комплекс взаємопов'язаних етапів – від постановки цілей і аналізу середовища до планування, реалізації та контролю – і виступає основою для підтримання фінансової стабільності та довгострокового розвитку організації.

3.2. Методичні підходи до оцінки фінансового стану та її показники

Оцінка фінансової безпеки організації в сучасних умовах є ключовим елементом управління стабільністю та конкурентоспроможністю підприємства. Вона надає змогу визначити рівень захищеності фінансових ресурсів, виявити слабкі місця у функціонуванні та спрогнозувати можливі ризики, що здатні негативно вплинути на діяльність.

Завдяки системній оцінці підприємство отримує інструмент для своєчасного ухвалення управлінських рішень, адаптації до змін зовнішнього середовища, мінімізації впливу кризових ситуацій і забезпечення збалансованого розвитку. У сучасній економіці, що характеризується нестабільністю та високим рівнем ризиків, така оцінка стає не лише засобом контролю, а й важливим стратегічним орієнтиром для збереження фінансової стійкості та довгострокового розвитку.

Етапи оцінки фінансової безпеки організації відтворено на рис. 3.3.

Організації здійснюють оцінку фінансової безпеки для того, щоб своєчасно визначати рівень захищеності власних ресурсів, виявляти потенційні ризики та загрози і приймати управлінські рішення, спрямовані на їх мінімізацію. Завдяки такій оцінці можна контролювати фінансову стійкість, ефективно розподіляти ресурси, забезпечувати стабільність у кризових умовах і підвищувати конкурентоспроможність.

Основними цілями оцінки фінансової безпеки організації є:

– визначення фактичного рівня фінансової стійкості та надійності;

– виявлення внутрішніх і зовнішніх ризиків, що можуть вплинути на діяльність;

– порівняння фінансових показників із нормативними та галузевими стандартами;

– прогнозування можливих сценаріїв розвитку та підготовка до них;

– формування рекомендацій для підвищення ефективності управління фінансами;

– створення основи для стратегічного планування й довгострокового розвитку підприємства.

Для оцінки фінансової безпеки використовують різні **методи**, які залежать від об'єкта оцінки, цілей та показників, які важливі для суб'єкта оцінки; проте основними вважаються такі:

1. Оціночні фінансові коефіцієнти (індикаторний підхід). Найпростіший і найбільш поширений підхід – це набір фінансових коефіцієнтів, які дають оперативну картину ліквідності, платоспроможності, рентабельності

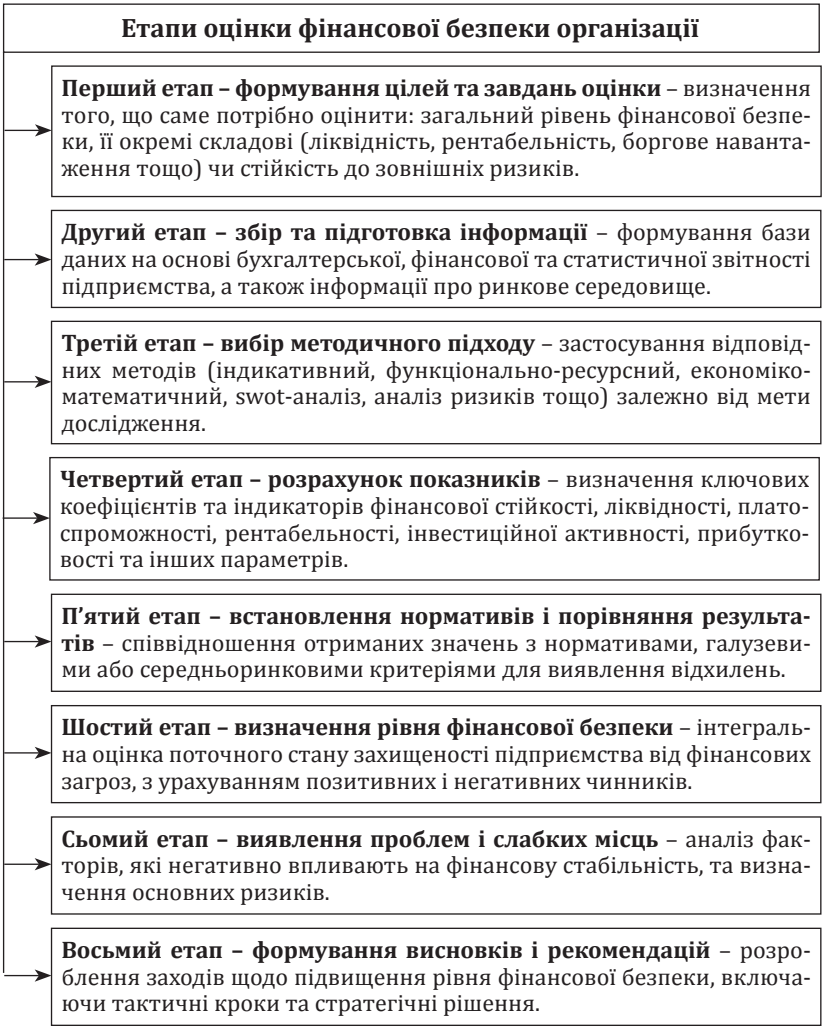


Рис. 3.3. Головні етапи оцінки фінансової безпеки організації

та фінансового важеля. Для кожного коефіцієнта подається формула і коротка інтерпретація. Такий підхід вважається базовим, оскільки допомагає швидко виявити сильні та слабкі сторони фінансового стану підприємства

й порівняти їх з нормативними чи галузевими орієнтирами. Крім того, використання системи коефіцієнтів створює підґрунтя для подальшого глибшого аналізу і застосування складніших методів оцінки фінансової безпеки.

Поточний коефіцієнт (*Current ratio*):

$$Current\ ratio = \frac{Current\ assets}{Current\ liabilities}. \quad (3.1)$$

Показує здатність погасити короткострокові зобов'язання за рахунок оборотних активів.

Швидкий коефіцієнт (*Quick / Acid-test*):

$$Quick\ ratio = \frac{Current\ asset - Inventories}{Current\ liabilities}. \quad (3.2)$$

Консервативніша міра короткострокової платоспроможності.

Коефіцієнт заборгованості (*Debt-to-Assets* або *Debt-to-Equity*):

$$Debt/Assets = \frac{Total\ liabilities}{Total\ assets},\ Debt/Equity = \frac{Total\ liabilities}{Equity}. \quad (3.3)$$

Оцінює фінансовий важіль і залежність від позикового капіталу.

Покриття відсотків (*Interest coverage*):

$$Interest\ coverage = \frac{EBIT}{Interest\ expense}. \quad (3.4)$$

Відображає здатність генерувати прибуток для обслуговування боргу.

Рентабельність активів (*ROA*) / рентабельність власного капіталу (*ROE*):

$$ROA = \frac{Net\ income}{Total\ assets},\ ROE = \frac{Net\ income}{Equity}. \quad (3.5)$$

Показники прибутковості, що важливі для довгострокової стійкості.

2. Матричні (*R = P × I*) та ризик-матриці. Матричний метод оцінки ризиків ґрунтується на поєднанні двох ключових параметрів: ймовірності виникнення події (*P*)

та можливого впливу її наслідків (*I*). За допомогою простої формули розраховується інтегральний рівень ризику, що дозволяє класифікувати його як низький, середній чи високий. Для зручності використовується ризик-матриця, де по горизонталі відображається ймовірність, а по вертикалі – масштаб можливих наслідків, що створює наочну систему для ухвалення управлінських рішень. Такий підхід допомагає організації визначати пріоритетність заходів безпеки, концентрувати ресурси на найбільш критичних загрозах та ефективніше планувати заходи з їх нейтралізації. Класичний підхід для ранжування ризиків: поєднання ймовірності настання (*P*) і ступеня негативних наслідків (*I* – *impact*).

Базова формула:

$$R = P \times I, \tag{3.6}$$

де *P* оцінюється в умовних одиницях (наприклад, 0…1 або 1…5), а *I* – за шкалою збитків; отримане *R* класифікують як низький/середній/високий ризик у матриці 3×3 або 5×5. Цей метод зручний для прийняття рішень про пріоритетність заходів.

3. Інтегральний (композитний) індекс (зважена сума нормалізованих індикаторів). Інтегральний (композитний) індекс застосовується для комплексної оцінки фінансової безпеки шляхом узагальнення кількох показників у єдиний індикатор. Для цього всі показники попередньо нормалізуються (приводяться до єдиної шкали), після чого зважуються відповідно до їхньої значущості та підсумовуються. Отримане значення інтегрального індексу дає змогу сформувати об'єктивну картину рівня фінансової безпеки організації та порівняти її з нормативними або середньогалузевими орієнтирами. Багато методик формують один інтегральний показник фінансової безпеки як зважену суму нормалізованих індикаторів. Загальна формула (компонентна інтеграція):

$$I_{integral} = \sum_{i=1}^{n} w_i \times \tilde{x_i}, \tag{3.7}$$

де $\tilde{x}_i$ – нормалізований (відношення до референту або нормативу) показник *i*-тої групи (ліквідність, платоспроможність, рентабельність, оборотність і т. д.), а w_i – ваговий коефіцієнт,

що відображає значимість компонента. Нормалізацію та ваги зазвичай визначають експертно або за допомогою статистичних методів (наприклад, факторного аналізу або методу аналітичної ієрархії).

4. Altman *Z-Score* (модель прогнозування банкрутства). Модель *Altman Z-Score* є одним із найвідоміших методів прогнозування ймовірності банкрутства підприємства. Вона була розроблена американським економістом Едвардом Альтманом у 1968 році та ґрунтується на поєднанні кількох фінансових коефіцієнтів, які інтегруються в єдиний показник. Ця модель дає можливість оцінити фінансовий стан компанії, враховуючи ліквідність, прибутковість, ефективність використання активів та структуру капіталу.

Значення *Z-Score* інтерпретується так: високий показник свідчить про фінансову стійкість і низький ризик неплатоспроможності, натомість низьке значення сигналізує про підвищену ймовірність банкрутства. У практиці управління фінансовою безпекою цей метод відіграє важливу роль, адже допомагає не лише виявити слабкі місця у фінансовій системі підприємства, а й своєчасно впровадити коригувальні заходи.

З точки зору оцінки фінансової безпеки, *Altman Z-Score* виступає дієвим інструментом ранньої діагностики кризових ситуацій. Використання цього підходу надає змогу організаціям:

– прогнозувати фінансові ризики;

– визначати рівень надійності і стабільності компанії;

– приймати стратегічні рішення щодо реструктуризації боргів, інвестицій та оптимізації витрат;

– формувати політику управління ризиками та посилювати довіру інвесторів.

Отже, *Altman Z-Score* можна розглядати як один із ключових методів у системі моніторингу фінансової безпеки, що дозволяє знизити ризик несподіваних фінансових криз і забезпечити довгострокову стабільність організації. Широковідома модель для оцінки ризику фінансового колапсу – комбінація п'яти фінансових коефіцієнтів з вагами:

$$Z = 1/2 \times A + 1.4 \times B + 3.3 \times C + 0.6 \times D + 1.0 \times E, \qquad (3.8)$$

де

$$A = \frac{Working\ capital}{Total\ assets}, \tag{3.9}$$

$$B = \frac{Retained\ earnings}{Total\ assets}, \tag{3.10}$$

$$C = \frac{EBIT}{Total\ assets}, \tag{3.11}$$

$$D = \frac{Market\ value\ of\ equity}{Total\ liabilities}, \tag{3.12}$$

$$E = \frac{Sales}{Total\ assets}. \tag{3.13}$$

Низькі значення Z сигналізують про високий ризик банкрутства (у класичному варіанті пороги: $Z < 1.8$ – висока небезпека; $Z > 3.0$ – низький ризик). Модель має варіанти, адаптовані для приватних компаній та неманufактурних підприємств. Інший варіант обчислення, враховуючи показники балансу, поданий у додатку В.

5. Скорингові / бінарні показники (наприклад, ***Piotroski F-score***). Метод полягає в нарахуванні балів за виконання набору фінансових критеріїв (кожна умова = 1 або 0), а сумарна оцінка відображає силу фінансового стану. Сума таких балів дозволяє швидко визначити рівень фінансової стійкості організації, виявити потенційні ризики та оцінити перспективи розвитку. Приклад (*Piotroski F-score*): 9 критеріїв, підсумок F від 0 до 9:

$$F = \sum_{k=1}^{9} s_k,\ s_k \in \{0,1\}. \tag{3.14}$$

Критерії охоплюють прибутковість, зміну *leverage*/*liquidity* та операційну ефективність. Високі значення свідчать про міцність фінансового стану.

6. Методи експертної оцінки та *Delphi* (якісно-кількісні підходи). Коли даних мало або вони неоднорідні, використовують опитування групи експертів, зведення думок і побудову ваг/рейтингу. Результат може бути виражений як нормалізована експертна інтегральна оцінка або як вхід у модель інтегрального індексу. Часто застосовують узгодження ваг (*AHP*) або *Delphi* для мінімізації суб'єктивності.

7. Фазі-/нечіткі (*fuzzy*) підходи і моделі нечіткої логіки. Нечіткі системи дозволяють працювати з нечіткими

входами (наприклад, «висока ліквідність», «середній ризик») і через правила-основи отримувати більш гнучкі інтегральні оцінки. Вони корисні, коли потрібно агрегувати якісні експертні судження з кількісними даними. Формально результат обчислюють через нечіткі множини та операції дефазифікації.

8. Сценарні та моделювальні підходи (*simulation / econometric models*). Використовуються для прогнозування і «стрес-тестування» фінансової стійкості при різних макро- і мікросценаріях (зміни процентних ставок, падіння продажу, втрата важливого партнера). Методи включають регресійні моделі, *VAR*, *Monte-Carlo* симуляції; результат – розподіл можливих сценаріїв і ймовірностей суттєвого погіршення.

9. Комбіновані методики для інтегральної діагностики (практичні алгоритми). У науковій практиці часто комбінують індикаторний підхід, експертні ваги і модельну нормалізацію:

– обрати набір індикаторів;

– нормалізувати значення (наприклад, методом *min-max*);

– визначити ваги (експертно або статистично);

– обчислити інтегральний індекс;

– класифікувати рівень безпеки за порогами.

Формула:

$$\tilde{x}_i = \frac{x_i - x_i^{min}}{x_i^{max} - x_i^{min}}, \; I_{integral} = \sum w_i \tilde{x}_i. \qquad (3.15)$$

Цей підхід широко застосовується у змінених локальних умовах (галузеві адаптації).

Оцінка та аналіз фінансової безпеки мають ключове значення для стабільного функціонування та розвитку організації, адже вони дозволяють вчасно виявити загрози, оцінити рівень ризиків і розробити заходи для їх мінімізації. Завдяки систематичному моніторингу фінансових показників підприємство отримує можливість підтримувати ліквідність, платоспроможність та інвестиційну привабливість навіть в умовах економічної нестабільності. Таким чином, оцінка фінансової безпеки є не лише інструментом захисту від кризових ситуацій, а й засобом стратегічного планування, що забезпечує довгострокову конкурентоспроможність та фінансову стійкість бізнесу.

3.3. Інформаційне забезпечення фінансової безпеки підприємства

Інформаційне забезпечення фінансової безпеки – це організований процес формування, обробки та передачі релевантних даних і аналітики, який створює інформаційну основу для своєчасного виявлення загроз, оцінки ризиків і прийняття управлінських рішень щодо захисту фінансових інтересів підприємства. Воно включає не лише збір бухгалтерської та ринкової інформації, а й інтелектуальну обробку (моніторинг, прогнозування, ранжування ризиків) і забезпечує інформаційно-аналітичну підтримку як оперативного, так і стратегічного управління.

Основними компонентами інформаційного забезпечення фінансової безпеки є:

– база даних та інформаційні масиви (внутрішні фінансові звіти, платіжні потоки, облікові регістри, контракти);

– зовнішня аналітика (макроекономічні індикатори, галузеві огляди, ринкова розвідка, нормативно-правова інформація);

– інструменти обробки та аналізу (платформи BI, моделі прогнозування, матриці ризиків, економіко-математичні моделі);

– системи раннього попередження та моніторингу (автоматизований збір подій, порогові сповіщення, стрес-тести);

– заходи інформаційної та кібербезпеки (політики доступу, резервування, захист даних, контроль цілісності інформації);

– організаційно-процедурні елементи (регламенти збору інформації, звітність, ролі відповідальних осіб, експертні групи).

Ці складові разом утворюють функціональний комплекс, що забезпечує аналітичну підтримку фінансового менеджменту. Роль інформаційного забезпечення в системі фінансової безпеки полягає в кількох вимірах: забезпечити прозорість фінансового стану, підвищити швидкість і обґрунтованість управлінських рішень, заручитися можливістю проактивного реагування на зовнішні шоки через сценарне моделювання, а також створити технічні й організаційні

передумови для захисту конфіденційних і критичних даних. В умовах цифровізації та зростання кіберзагроз інформаційне забезпечення виступає одночасно як джерело аналітики і як перша лінія оборони проти інформаційних ризиків, що впливають на фінансову стійкість.

Фінансове забезпечення оцінки безпеки підприємства ґрунтується насамперед на використанні фінансової звітності, яка виступає основним джерелом інформації для аналізу. Фінансова звітність підприємства – це систематизований комплекс показників, визначений чинним законодавством України, що охоплює різні форми облікових документів і розкриває інформацію про фінансовий стан, результати діяльності та наявні ресурси підприємства. Вона формується за конкретний звітний період, зазвичай календарний рік, і включає записи в окремих статтях, які дозволяють отримати об'єктивні дані для подальшої аналітичної оцінки. Структура фінансової звітності подана на рис. 3.4.

Окрім традиційної фінансової звітності, до інформаційного забезпечення оцінки фінансової безпеки входять статистичні матеріали, дані внутрішнього управлінського обліку, результати аудиторських перевірок та економічні прогнози. Сукупність цих джерел дає змогу не лише оцінити поточний рівень фінансової стабільності, а й прогнозувати можливі ризики, визначати тенденції розвитку

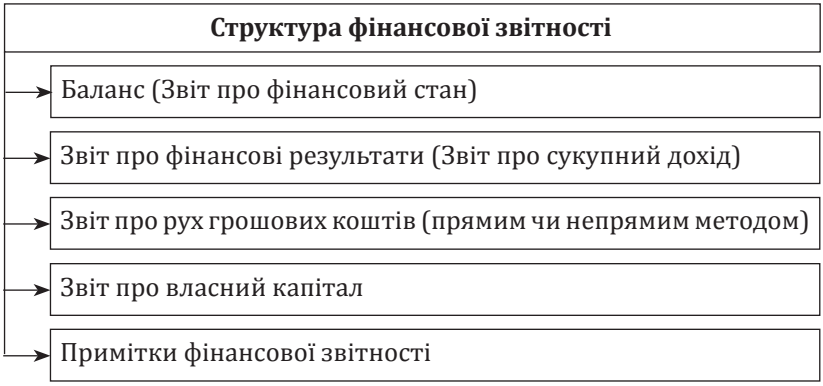


Рис. 3.4. Структура фінансової звітності підприємства, необхідна для оцінки фінансової безпеки

та своєчасно ухвалювати рішення щодо зміцнення безпеки. Таким чином, інформаційна база виступає ключовим елементом у процесі забезпечення фінансової безпеки підприємства, оскільки від її повноти та достовірності залежить точність висновків і ефективність заходів захисту.

Баланс є ключовим елементом фінансової звітності підприємства, оскільки відображає вартість усього майнового комплексу компанії, включаючи основні та оборотні засоби (активи), а також джерела їх фінансування у вигляді власного капіталу та залучених ресурсів (пасиви).

Звіт про фінансові результати (звіт про сукупний дохід) розкриває кінцеві підсумки господарської діяльності підприємства за певний період. У ньому відображаються доходи, витрати та фінансові результати, що дає змогу оцінити рівень ефективності виробничо-комерційної діяльності та прибутковість компанії.

Звіт про рух грошових коштів деталізує всі грошові надходження та витрати підприємства за напрямами діяльності впродовж року. Він структурується за трьома основними розділами:

- рух коштів від операційної діяльності;
- рух коштів від фінансової діяльності;
- рух коштів від інвестиційної діяльності.

Додатки до фінансової звітності (форма № 5) надають розширені пояснення до основних статей балансу та звіту про фінансові результати. У них містяться дані щодо нематеріальних активів, основних засобів, капітальних і фінансових інвестицій, доходів і витрат, резервів і забезпечень, запасів, дебіторської заборгованості, податку на прибуток та інших показників, які дозволяють глибше оцінити фінансово-господарський стан підприємства.

Зовнішня аналітика в системі інформаційного забезпечення фінансової безпеки організації є надзвичайно важливим елементом, адже вона дозволяє враховувати вплив середовища, яке безпосередньо не контролюється підприємством, але суттєво впливає на його діяльність. У першу чергу, сюди належать макроекономічні індикатори, які відбивають стан економіки країни (рівень інфляції, валовий внутрішній продукт, безробіття, процентні ставки тощо).

Вони визначають загальну економічну ситуацію, що формує умови функціонування будь-якого бізнесу.

Другим важливим компонентом виступають галузеві огляди, які допомагають оцінити тенденції та перспективи розвитку конкретної сфери економіки, визначити рівень конкуренції, бар'єри входу на ринок, технологічні інновації й динаміку попиту. Завдяки їм підприємство може розробляти конкурентні стратегії та уникати ризиків, пов'язаних із занепадом чи надмірною концентрацією ринку.

До зовнішньої аналітики також належить ринкова розвідка (market intelligence), що забезпечує інформацію про діяльність конкурентів, їхні фінансові результати, цінову політику, інвестиційні проєкти та інноваційні рішення. Завдяки цьому організація може прогнозувати поведінку конкурентів, адаптувати власну бізнес-модель та вчасно виявляти потенційні загрози.

Не менш значущим аспектом є нормативно-правова інформація, яка охоплює закони, підзаконні акти, регуляторні вимоги, податкове законодавство, стандарти звітності та інші правові обмеження. Її врахування дозволяє знизити юридичні ризики, уникати штрафів і санкцій, а також діяти у межах правового поля, що позитивно впливає на репутацію та фінансову стабільність підприємства.

3.4. Чинники забезпечення фінансової безпеки організації

Чинники, що визначають фінансову безпеку організації, являють собою комплекс внутрішніх і зовнішніх елементів, які впливають на її здатність підтримувати стабільний розвиток та забезпечувати належний рівень захищеності від ризиків. Вони формують основу, на якій підприємство будує свою фінансову політику та приймає стратегічні рішення. Врахування таких чинників дозволяє вчасно ідентифікувати загрози, мінімізувати їхній вплив і водночас використати наявні можливості для зміцнення фінансового стану.

До внутрішніх чинників можна віднести ефективність управління фінансовими потоками, якість організаційної структури, рівень кваліфікації персоналу, інноваційність,

конкурентоспроможність продукції, оптимізацію витрат і здатність формувати резерви для покриття непередбачуваних втрат (рис. 3.5). Важливу роль також відіграє здатність організації оперативно реагувати на зміни у внутрішньому середовищі, зокрема в управлінні ліквідністю та борговими зобов'язаннями.

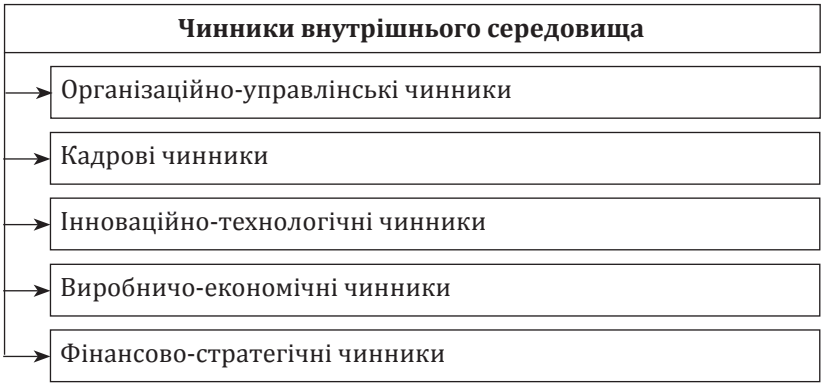


Рис. 3.5. Чинники внутрішнього середовища,
що впливають на фінансову безпеку організації

Більш детально класифікувати чинники внутрішнього середовища можна таким чином:

1. Організаційно-управлінські чинники:

– ефективність управління фінансовими потоками – наскільки якісно підприємство формує, розподіляє й використовує грошові ресурси;

– якість організаційної структури – чіткість підпорядкування, наявність спеціалізованих відділів (фінансового, планово-аналітичного, ризик-менеджменту);

– система внутрішнього контролю – наявність процедур перевірки достовірності даних, контролю витрат, управління бюджетом.

2. Кадрові чинники:

– рівень кваліфікації персоналу – компетентність фінансових менеджерів, бухгалтерів, аналітиків;

– професійний розвиток і навчання – постійне підвищення кваліфікації, освоєння нових фінансових технологій;

– корпоративна культура та відповідальність – чесність і доброчесність працівників, що впливають на зниження шахрайських дій.

3. Інноваційно-технологічні чинники:

– інноваційність – застосування сучасних методів фінансового планування, прогнозування та ризик-менеджменту;

– автоматизація процесів – використання бухгалтерських і управлінських програм, ERP-систем для прозорості даних;

– захист інформації – рівень кібербезпеки у фінансово-інформаційних системах підприємства.

4. Виробничо-економічні чинники:

– конкурентоспроможність продукції – здатність утримувати позиції на ринку, отримувати стабільний дохід;

– собівартість і структура витрат – рівень оптимізації витрат, економія ресурсів;

– рентабельність активів та капіталу – фінансова ефективність використання ресурсів.

5. Фінансово-стратегічні чинники:

– ліквідність та платоспроможність – здатність своєчасно виконувати зобов'язання;

– управління борговими зобов'язаннями – оптимальне співвідношення власного й позикового капіталу;

– формування резервів – створення фінансових «подушок безпеки» для непередбачуваних витрат;

– інвестиційна політика – здатність залучати інвестиції та ефективно ними управляти.

Вплив внутрішніх чинників напряму залежить від ефективності керівництва, власників та акціонерів управляти фінансовими ресурсами, контролювати рух грошових потоків організації, особливо вихідних, та визначати пріоритетні напрями щодо інвестування чи реінвестування власних коштів. Ключовим показником є рівень прибутковості, адже саме він визначає ефективність акумулювання, управління чи розпорядження фінансовими ресурсами, які є основним складником фінансової безпеки. До додаткових внутрішніх чинників відносяться:

– корпоративне управління та прозорість – наявність чітких правил прийняття рішень, прозорість у звітності та мінімізація конфліктів інтересів;

– система управління ризиками – здатність підприємства виявляти, аналізувати й контролювати ризики, пов'язані з фінансовою діяльністю;

– фінансова дисципліна – своєчасне виконання зобов'язань перед контрагентами, дотримання внутрішніх фінансових правил і процедур;

– рівень диверсифікації доходів – залежність підприємства від одного чи кількох джерел доходу; що вища диверсифікація – то стабільніша фінансова безпека;

– репутація та довіра партнерів – рівень ділової репутації, який впливає на можливість отримувати кредити, залучати інвестиції чи укладати контракти;

– інноваційно-кадровий потенціал – наявність внутрішніх можливостей для розвитку через інновації, професійну підготовку кадрів та корпоративну культуру, орієнтовану на стійкість і зростання.

Зовнішні чинники, що впливають на управління фінансовою безпекою вітчизняних організацій, подано на рис. 3.6.

Розглянемо детальніше класифікацію зовнішніх чинників, котрі впливають на фінансову безпеку підприємства:

1. Економічні чинники:

– макроекономічна стабільність – темпи інфляції, динаміка ВВП, безробіття, загальний стан економіки;

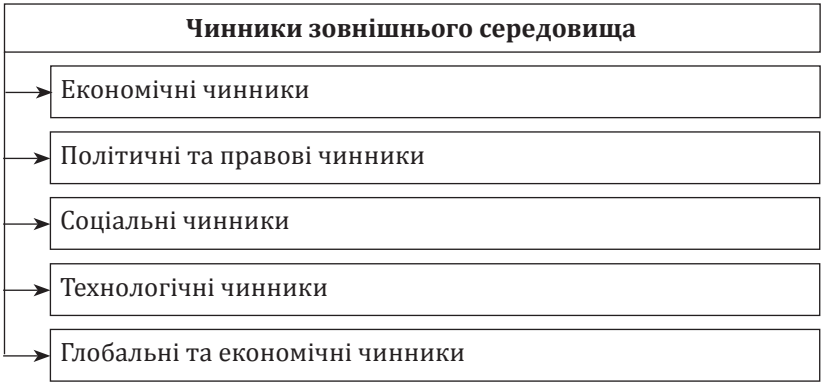


Рис. 3.6. Чинники зовнішнього середовища,
які мають вплив на фінансову безпеку організації

– доступність фінансових ресурсів – процентні ставки, вартість позикового капіталу, доступ до кредитів;

– розвиток ринку капіталу – можливість залучення інвестицій, рівень ліквідності фондового ринку;

– курсова політика – стабільність національної валюти, коливання валютних курсів.

2. Політичні та правові чинники:

– політична стабільність – ризики зміни влади, військово-політичні загрози;

– регуляторна політика – частота та непередбачуваність змін у законодавстві;

– податкове навантаження – рівень податкових ставок, пільги та податкові стимули;

– державна підтримка бізнесу – субсидії, програми розвитку, гранти.

3. Соціальні чинники:

– рівень доходів населення – купівельна спроможність та структура споживчого попиту;

– демографічна ситуація – чисельність та вікова структура населення, трудові ресурси;

– війна, постійні обстріли та руйнування інфраструктури;

– соціальна стабільність – наявність чи відсутність масових протестів, страйків.

4. Технологічні чинники:

– рівень інновацій у галузі – швидкість технологічних змін та можливість адаптації до них;

– цифровізація економіки – впровадження інформаційних систем, автоматизація фінансових процесів;

– доступ до сучасних технологій – можливість імпорту обладнання та програмного забезпечення.

5. Глобальні та екологічні чинники:

– глобальні кризи – економічні рецесії, пандемії, міжнародні фінансові потрясіння;

– міжнародні відносини – доступ до зовнішніх ринків, вплив санкцій та торговельних бар'єрів;

– екологічні ризики – природні катастрофи, кліматичні зміни, обмеження на використання ресурсів.

Внутрішні чинники мають найбільший вплив на фінансову безпеку організації, оскільки вони безпосередньо контролюються керівництвом і визначають здатність підприємства протистояти зовнішнім загрозам. На відміну від зовнішніх факторів (як-от макроекономічна нестабільність чи політичні ризики), які є некерованими, внутрішні чинники – якість управління, фінансова дисципліна та ефективність бізнес-процесів – формують внутрішній потенціал стійкості. Криза, спричинена зовнішнім шоком (наприклад, зростанням цін на сировину), переростає у фінансову катастрофу лише в тому випадку, якщо організація вже мала внутрішні проблеми, такі як неефективна структура капіталу, слабкий контроль за витратами або дефіцит ліквідності. Тобто внутрішні чинники є фундаментом фінансової безпеки: якщо цей фундамент міцний, організація може адаптуватися до зовнішніх викликів; якщо він слабкий – будь-який зовнішній вплив призводить до критичних наслідків.

Питання для самоконтролю

1. У чому полягає сутність фінансової безпеки організації та які її ключові ознаки?
2. Які основні внутрішні та зовнішні чинники впливають на фінансову безпеку підприємства?
3. Яку роль відіграє фінансова безпека в забезпеченні конкурентоспроможності організації?
4. Що включає в себе процес управління фінансовою безпекою?
5. Які існують методи оцінки рівня фінансової безпеки підприємства?
6. Яким чином фінансова звітність виступає інформаційною базою для оцінки фінансової безпеки?
7. У чому криється значення стратегічного управління фінансовою безпекою?
8. Які етапи формування та реалізації стратегії управління фінансовою безпекою можна виокремити?
9. Які інструменти найчастіше використовуються для управління фінансовою безпекою організації?
10. Чому оцінка фінансової безпеки має відмінності для різних типів організацій?

Тестові завдання

1. Що відображає фінансова безпека організації?

а) Лише рівень прибутковості підприємства;

б) стан захищеності від усіх можливих ризиків;

в) здатність підприємства зберігати стабільність за умов впливу внутрішніх і зовнішніх загроз;

г) лише виконання податкових зобов'язань.

2. Яка з наведених складових належить до управління фінансовою безпекою?

а) Управління ризиками та резервами;

б) формування корпоративної культури;

в) виключно контроль якості продукції;

г) лише забезпечення технічної безпеки.

3. Яке головне завдання оцінки фінансової безпеки підприємства?

а) Визначення кількості працівників;

б) виявлення та аналіз слабких місць у фінансовій системі;

в) оцінка рівня задоволеності клієнтів;

г) планування маркетингових заходів.

4. Які фактори належать до зовнішніх у контексті фінансової безпеки?

а) Структура управління підприємством;

б) рівень інноваційності персоналу;

в) податкова політика та валютні ризики;

г) рівень оптимізації витрат підприємства.

5. Який метод використовується для прогнозування банкрутства підприємства?

а) SWOT-аналіз;

б) Altman Z-Score;

в) PEST-аналіз;

г) Balanced Scorecard.

6. Яка роль фінансової звітності у забезпеченні фінансової безпеки?

а) Вона допомагає лише у визначенні заробітних плат;

б) слугує виключно для оподаткування;

в) є джерелом інформації для аналізу стану підприємства та прийняття управлінських рішень;

г) має значення лише для зовнішніх користувачів.

7. Яка мета стратегії управління фінансовою безпекою?

а) Максимізація прибутку в короткостроковій перспективі;

б) забезпечення виконання адміністративних завдань;

в) створення умов для стійкого розвитку підприємства та захисту його від фінансових ризиків;

г) лише зменшення податкового навантаження.

8. Який із наведених інструментів не використовується для управління фінансовою безпекою?

а) Страхування ризиків;

б) фінансовий аналіз і прогнозування;

в) створення резервних фондів;

г) підвищення культурної свідомості суспільства.

9. Чим характеризується інтегральний підхід до оцінки фінансової безпеки?

а) Використанням лише одного коефіцієнта;

б) узагальненням низки показників у єдиний індекс, який визначає рівень прибутковості організації;

в) виключно якісною оцінкою;

г) аналізом лише кадрових ризиків.

10. Чому оцінка фінансової безпеки різних організацій може відрізнятися?

а) Всі підприємства працюють за однаковою системою звітності та опрацювання фінансових показників;

б) через різний рівень кваліфікації персоналу;

в) через відмінності у розмірі, сфері діяльності, фінансових стратегіях та структурі ризиків;

г) лише через використання різних методик бухгалтерського обліку, які притаманні конкретному аналізу.

Практичні завдання

Завдання 1.

ТОВ «Альфа» працює на ринку будівельних матеріалів понад 10 років. Упродовж останніх двох років компанія зіткнулася з низкою викликів: коливання валютних курсів, зростання вартості енергоносіїв, збільшення кредитного навантаження та посилення конкуренції з боку іноземних компаній. Додатково організація має високий рівень дебіторської заборгованості, що знижує її ліквідність. Керівництво прагне зміцнити систему фінансової безпеки та забезпечити стійкість бізнесу в умовах економічної нестабільності.

1. Визначте основні внутрішні та зовнішні загрози для фінансової безпеки ТОВ «Альфа».

2. Запропонуйте управлінські рішення, які допоможуть мінімізувати виявлені ризики.

3. Сформулюйте рекомендації щодо підвищення фінансової стійкості організації в короткостроковій та довгостроковій перспективі.

Завдання 2.

АТ «ЕкоФарм» – виробник лікарських препаратів на основі рослинної сировини. Підприємство має сучасне обладнання, власну лабораторію та команду висококваліфікованих спеціалістів. Проте компанія стикається з проблемами: зростає конкуренція з боку великих міжнародних корпорацій, існують ризики підвищення цін на імпортну сировину, а також спостерігається жорстке регулювання фармацевтичного ринку. Водночас підприємство планує вийти на європейський ринок.

1. Складіть SWOT-аналіз підприємства (визначте сильні та слабкі сторони, можливості та загрози).

2. На основі аналізу визначте стратегічні напрями розвитку АТ «ЕкоФарм».

3. Поясніть, як SWOT-аналіз може бути використаний для зміцнення фінансової безпеки підприємства.

Завдання 3.

ТОВ «ЛогістикСервіс» надає послуги вантажних перевезень. Для оцінки ризику банкрутства пропонується використати модель Альтмана (*Z-score*). Відомі такі фінансові показники підприємства за рік:

Оборотні активи – 2 400 тис. грн

Загальні активи – 6 000 тис. грн

Нерозподілений прибуток – 1 200 тис. грн

Прибуток до сплати податків та відсотків – 800 тис. грн

Власний капітал – 2 000 тис. грн

Загальні зобов'язання – 4 000 тис. грн

Чистий дохід від реалізації – 7 000 тис. грн

1. Розрахуйте значення Z-score за моделлю Альтмана для цього підприємства.

2. Інтерпретуйте отриманий результат: до якої зони (безпечної, «сірої», ризикової) можна віднести підприємство.

3. Запропонуйте заходи щодо зменшення ризику фінансової нестабільності, якщо підприємство перебуває у зоні ризику.

ТЕМА 4
МЕНЕДЖМЕНТ КРЕДИТНОЇ БЕЗПЕКИ

4.1. Складові та сутність управління кредитною безпекою організації

4.2. Види кредитних загроз та управління ними

4.3. Оцінка рівня кредитної безпеки банківських установ

4.4. Оцінка рівня кредитоспроможності позичальника в системі фінансово-кредитної безпеки

Основні поняття і терміни: безпека, безпека організації, кредит, кредитна безпека, банківська установа, кредитний рейтинг, менеджмент безпеки організації, кредитоспроможність, позика, кредитний портфель, відсоток, застава, позичальник, кредитор, ризик.

4.1. Складові та сутність управління кредитною безпекою організації

Кредитна безпека (в контексті грошово-кредитної безпеки) – це така ситуація у фінансовій та кредитній системі, коли валюта залишається стабільною, кредитні ресурси доступні для суб'єктів господарської діяльності, а рівень контролю і регулювання достатній для захисту від надмірних ризиків.

Кредитна безпека – це такий стан кредитно-фінансової системи, при якому всі економічні учасники мають доступ до якісних кредитів за прийнятними умовами, що сприяє сталому функціонуванню господарської діяльності.

Якщо кредитну безпеку розглядати в контексті економічної безпеки організації, то **сутність кредитної безпеки** полягає у збереженні фінансової стабільності та захищеності організації або окремої особи під час користування кредитними ресурсами та виконання відповідних зобов'язань. Її головна мета – зменшення ймовірності виникнення ризиків, що супроводжують процес залучення позикового капіталу, а також забезпечення своєчасного і повного виконання зобов'язань перед банками чи іншими кредиторами.

Кредитна безпека охоплює комплекс дій, серед яких: оцінка кредитоспроможності позичальника, управління потенційними кредитними ризиками, раціональне використання отриманих коштів та постійний моніторинг виконання умов кредитних договорів. Вона виступає важливим елементом фінансової стратегії організації, адже дозволяє підтримувати довіру з боку кредиторів, формувати позитивну ділову репутацію та уникати кризових ситуацій, пов'язаних із борговими зобов'язаннями.

Основні елементи кредитної безпеки охоплюють кілька взаємопов'язаних аспектів.

1. Кредитоспроможність – це можливість підприємства або фізичної особи своєчасно та повністю виконувати всі взяті кредитні зобов'язання. Вона базується на стабільних доходах та ефективному управлінні фінансовими потоками, що гарантує відсутність ризику виникнення кризових ситуацій через боргове навантаження.

2. Кредитний ризик передбачає виявлення, аналіз і контроль загроз, пов'язаних із потенційними труднощами повернення боргу. Цей ризик може виникати як з боку позичальника, так і через несприятливі зміни на фінансовому чи валютному ринку.

3. Управління борговими зобов'язаннями означає застосування збалансованої політики щодо формування структури та розміру заборгованості. Грамотне управління допомагає уникнути надмірного кредитного тягаря, який може знизити фінансову стабільність і конкурентоспроможність компанії.

4. Забезпечення кредиту – це використання додаткових інструментів захисту інтересів кредитора, серед яких: застава, гарантії третіх осіб або страхування кредитних договорів. Такі механізми дозволяють зменшити ризик неповернення позикових коштів.

Крім того, система кредитної безпеки включає внутрішній контроль та аудит кредитних операцій, що забезпечує своєчасний моніторинг стану заборгованості. Використання сучасних аналітичних інструментів для прогнозування потенційних ризиків дає змогу заздалегідь реагувати на проблеми та приймати управлінські рішення для їх мінімізації.

У результаті кредитна безпека стає не лише механізмом захисту, але й важливим фактором підвищення фінансової стійкості організації.

Система кредитної безпеки організації – це цілісна сукупність принципів, методів, інструментів і механізмів, спрямованих на захист підприємства від надмірних кредитних ризиків та забезпечення його стабільної платоспроможності. Вона охоплює процеси планування, організації, контролю та регулювання кредитної діяльності, включаючи залучення, використання й обслуговування позикових ресурсів.

Основне завдання системи полягає у підтриманні оптимальної структури боргових зобов'язань, попередженні виникнення фінансових кризових ситуацій, формуванні стійкого рівня кредитоспроможності та створенні умов для довгострокового розвитку підприємства.

Ключові елементи системи кредитної безпеки, які формують механізм її ефективного управління, подані на рис. 4.1.

Цілями забезпечення достатнього рівня кредитної безпеки організації, з огляду на значну кількість факторів, є такі:

1. Забезпечення своєчасного виконання боргових зобов'язань, тобто підприємство має гарантувати регулярне та повне виконання своїх зобов'язань перед кредиторами, що створює основу для формування позитивної ділової репутації та підтримання довіри з боку фінансових установ і партнерів.

2. Мінімізація кредитних ризиків і загроз неплатоспроможності шляхом запобігання кризовим ситуаціям, які можуть виникнути через зростання боргового навантаження або несприятливі зміни на фінансовому ринку. Для цього організація застосовує інструменти управління ризиками, прогнозування та страхування.

3. Формування оптимальної структури джерел фінансування через передбачення балансу між власними й позиковими коштами, щоб уникнути залежності від зовнішнього фінансування та забезпечити стійкість навіть у разі обмеження доступу до кредитів.

4. Підвищення рівня фінансової стабільності та інвестиційної привабливості – високий рівень кредитної безпеки

Рис. 4.1. Основні елементи кредитної безпеки

сприяє стабільному розвитку компанії, зменшує ризики банкрутства та створює сприятливі умови для залучення нових інвесторів і партнерів.

5. Створення передумов для довгострокового розвитку без надмірного боргового навантаження, при цьому важливо не лише уникати перевищення критичного рівня заборгованості, а й вибудовувати стратегічну фінансову політику, яка дозволить підприємству зростати, не втрачаючи незалежності та керованості.

6. Забезпечення ефективного використання кредитних ресурсів. Необхідно, щоб позикові кошти спрямовувалися на проєкти з високим економічним ефектом, підвищення продуктивності чи модернізацію виробництва. Це дає змогу не лише обслуговувати борги, а й створювати додаткову вартість, зміцнюючи конкурентні позиції підприємства.

Дотримання належного рівня кредитної безпеки позитивно впливає на стабільність і розвиток організації, оскільки гарантує своєчасне виконання боргових зобов'язань та мінімізує ймовірність фінансових кризових ситуацій. Це дозволяє компанії ефективно використовувати позикові ресурси для інвестицій і розширення діяльності, зберігаючи при цьому фінансову незалежність та конкурентоспроможність. Крім того, високий рівень кредитної безпеки підвищує довіру з боку кредиторів, партнерів та інвесторів, що формує сприятливі умови для залучення нових джерел фінансування і забезпечує довгострокову стійкість підприємства.

Задля забезпечення достатнього рівня кредитної безпеки сучасним організаціям доцільно дотримуватися певних принципів:

– принцип своєчасності виконання зобов'язань;

– принцип диверсифікації джерел фінансування;

– принцип адекватності – співвідношення боргових зобов'язань до власного капіталу;

– принцип прозорості – ведення фінансової звітності й контролю;

– принцип обґрунтованості залучення кредитних ресурсів;

– принцип раціональної оцінки ризиків та загроз;

– принцип довіри до фінансових партнерів, клієнтів (якщо банківська чи кредитна установа).

Важливою складовою системи забезпечення кредитної безпеки є визначення кредитів (їх класифікація), які беруть участь в операційному чи фінансовому забезпеченні діяльності організації (табл. 4.1).

Отже, **управління кредитною безпекою організації** є головним елементом загальної фінансової безпеки, спрямоване на мінімізацію ризиків, пов'язаних із кредитуванням, та забезпечення стійкості підприємства у процесі залучення і використання позикових коштів. Цей процес охоплює кілька важливих етапів, які дозволяють організації ефективно планувати та контролювати кредитні операції, забезпечуючи стабільність та надійність свого фінансового стану.

Таблиця 4.1

Класифікація кредитів

Класифікаційна ознака	Перелік видів
1. За методами надання	– у разовому порядку; – відповідно до відкритої кредитної лінії; – гарантовані позички.
2. За методами погашення	– кредити, що погашаються одноразовим платежем на конкретну дату, яка вказана в кредитному договорі як строк повернення кредиту; – кредити, що погашаються з розстроченням платежів.
3. За кількістю кредиторів	– кредити, надані одним банком; – консорціумні кредити; – паралельні кредити.
4. За об'єктом кредитування	– у поточну діяльність; – в інвестиційну діяльність.
5. За забезпеченням	– забезпечені заставою (майном, майновими правами, цінними паперами); – гарантовані (банками, фінансами чи майном третьої особи); – з іншим забезпеченням (поручительство, свідоцтво страхової організації); – незабезпечені (бланкові).
6. За економічними суб'єктами-позичальниками	– кредити органам державного управління; – кредити суб'єктам господарювання; – кредити фізичним особам.
7. За валютою кредиту	– кредити в національній валюті; – кредити в іноземній валюті; – мультивалютні кредити.
8. За термінами (строками) користування	– короткострокові – до 1 року; – онкольні – кредити, погашення яких відбувається не у чітко зазначений термін, а за вимогою банку; – середньострокові –до 3 років; – довгострокові – понад 3 роки.
9. За характером процентної ставки	– кредити з фіксованою кредитною ставкою; – кредити з плаваючою кредитною ставкою.

При цьому основними етапами управління кредитною безпекою є такі:

1. Визначення цілей і завдань – встановлення стратегічних орієнтирів кредитної політики та ключових пріоритетів щодо захисту від ризиків.

2. Ідентифікація та оцінка ризиків – виявлення потенційних загроз, пов'язаних із кредитними зобов'язаннями, та визначення рівня їх впливу.

3. Формування кредитної стратегії – вибір підходів до залучення, використання і погашення позикових ресурсів, розробка правил та нормативів.

4. Реалізація заходів безпеки – впровадження механізмів контролю заборгованості, системи гарантій, резервів та страхових інструментів.

5. Моніторинг і контроль – постійне відстеження стану кредитного портфеля, оцінка ефективності застосованих заходів та коригування політики.

6. Оцінка результатів і вдосконалення – аналіз досягнутого рівня кредитної безпеки, виявлення слабких місць і розробка нових інструментів для підвищення стійкості.

Управління кредитною безпекою організації є важливим елементом фінансової безпеки, що фокусується на захисті активів та капіталу від ризиків, пов'язаних із кредитуванням та заборгованістю. Основними особливостями цього управління є превентивний характер (тобто запобігання ризикам до їх реалізації), що вимагає ретельної оцінки кредитоспроможності контрагентів, позичальників і дебіторів перед укладанням будь-яких угод. Управління включає формування чітких лімітів кредитного ризику, використання інструментів хеджування (наприклад, страхування кредитів), а також диверсифікацію кредитного портфеля для уникнення надмірної залежності від одного позичальника чи галузі. Крім того, невід'ємною частиною є постійний моніторинг фінансового стану дебіторів і ефективна робота з простроченою заборгованістю, що забезпечує безперебійне повернення коштів і підтримує ліквідність підприємства.

Основні методи управління подано в табл. 4.2.

Таблиця 4.2

Методи управління кредитною безпекою організації

Метод	Характеристика та роль у забезпеченні кредитної безпеки
Фінансовий аналіз	Передбачає оцінку фінансового стану підприємства (ліквідність, платоспроможність, рентабельність, динаміка капіталу). Дає змогу вчасно виявити слабкі сторони та спрогнозувати ризики неплатоспроможності.
Аналіз кредитоспроможності	Включає комплексну оцінку позичальників або партнерів з позицій їх здатності виконувати зобов'язання. Дозволяє знизити ризики неповернення кредитів та уникнути втрат.
Диверсифікація кредитного портфеля	Розподіл кредитних ресурсів між різними позичальниками, галузями, регіонами. Це зменшує концентрацію ризиків і підвищує стабільність фінансування.
Використання системи застав і гарантій	Забезпечення кредитів матеріальними чи фінансовими активами, гарантіями або страховими договорами. Сприяє зменшенню ризиків неповернення.
Кредитний моніторинг	Регулярне відстеження стану кредитів, діяльності позичальників та ринкових умов. Дає можливість оперативно реагувати на ознаки проблем.
Скоринг та рейтингові системи	Використання математичних моделей і балів для оцінки ризиковості клієнтів. Дозволяє стандартизувати рішення й зменшити суб'єктивність оцінок.
Страхування кредитних ризиків	Використання страхових механізмів для покриття можливих збитків у випадку дефолту позичальника. Додатково підвищує фінансову стійкість.
Стрес-тестування	Моделювання кризових сценаріїв (різке зниження доходів, девальвація, підвищення ставок) для оцінки впливу на здатність організації виконувати зобов'язання.
Комплаєнс-контроль	Дотримання внутрішніх правил, нормативних актів та банківських вимог. Забезпечує прозорість кредитних операцій та захист від шахрайства.
Інформаційно-аналітичні системи	Використання сучасних ІТ-рішень для аналізу даних, контролю руху коштів і прогнозування ризиків. Це підвищує оперативність прийняття рішень.

4.2. Види кредитних загроз та управління ними

Кредитні загрози – це сукупність потенційних ризиків і небезпек, що виникають у процесі залучення, використання чи надання позикових ресурсів та здатні негативно вплинути на фінансову стійкість і платоспроможність підприємства. Їх поява можлива як у внутрішньому середовищі самої організації (наприклад, помилки в управлінні чи низький рівень контролю), так і під впливом зовнішніх чинників (зміни на фінансовому ринку, коливання відсоткових ставок, макроекономічна нестабільність).

Усвідомлення різновидів кредитних загроз, їхньої структури та класифікаційних ознак дає можливість більш ефективно управляти кредитною безпекою організації, завчасно прогнозувати проблеми та розробляти заходи щодо зниження ймовірності їх виникнення. Далі наведено класифікацію ключових видів кредитних загроз, які найбільш істотно впливають на фінансовий стан підприємства.

Кредитні загрози – це потенційні, як явні, так і приховані, дії або впливи з боку позичальників, партнерів чи внутрішніх суб'єктів, які можуть спотворити або підірвати ефективність кредитних операцій. Вони формуються через порушення кредитної політики, неправильну оцінку фінансового стану клієнтів чи шахрайські дії та здатні призвести до вагомих втрат у фінансовому забезпеченні. Виникнення таких загроз вимагає активного прогнозування та реалізації превентивних заходів, щоб мінімізувати негативний вплив на кредитну стабільність організації.

Класифікацію кредитних загроз наведено в табл. 4.3.

Виявлення кредитних загроз у процесі здійснення фінансово-господарської діяльності є важливим процесом для ефективного і прибуткового функціонування та забезпечення загальної економічної безпеки організації. Для підприємства виявлення кредитних загроз проявляється через отримані кредити, які відображаються в балансі підприємства та надану дебіторську заборгованість. Для банківської установи – це управління кредитним портфелем фізичних

Таблиця 4.3

Класифікація кредитних загроз організації

Класифікаційна ознака	Перелік загроз
1. За джерелом виникнення	– внутрішні загрози – помилки у фінансовому менеджменті, низький рівень контролю за кредитними операціями, відсутність ефективної системи оцінки кредитоспроможності, зловживання персоналу; – зовнішні загрози – зміни в економічному середовищі, коливання валютних курсів і відсоткових ставок, фінансові кризи, нестабільність банківської системи, дії конкурентів.
2. За характером впливу	– прямі загрози – безпосередня загроза неповернення кредиту чи несвоєчасного виконання зобов'язань; – часткові загрози – впливають на один із видів кредитних (боргових) операцій; – непрямі загрози – чинники, що опосередковано знижують здатність підприємства обслуговувати борги (зменшення попиту на продукцію, погіршення інвестиційного клімату, правова невизначеність).
3. За тривалістю дії	– короткострокові – виникають у межах одного фінансового періоду (наприклад, затримки з платежами); – довгострокові – формують системні ризики, що впливають на фінансову стійкість підприємства в перспективі (накопичення боргового навантаження, залежність від зовнішніх кредиторів).
4. За можливістю прогнозування	– передбачувані – ризики, які можна оцінити завчасно за допомогою фінансового аналізу, скорингових моделей або моніторингу ринку. – непередбачувані – пов'язані з раптовими кризами, політичними чи соціальними потрясіннями, що важко піддаються прогнозуванню.
5. За масштабом впливу	– локальні загрози – впливають на окреме підприємство або невелику групу організацій; – системні загрози – охоплюють цілий сектор економіки чи банківську систему загалом (скажімо, глобальна фінансова криза).
6. За формою прояву	– фінансові – неповернення кредитів, дефіцит грошових потоків, зростання боргового навантаження; – організаційні – недосконаліть внутрішніх процедур управління боргами, відсутність моніторингу ризиків; – правові – недотримання умов кредитних договорів, зміни у законодавстві; – репутаційні – втрата довіри кредиторів, інвесторів і партнерів.

та юридичних осіб. Загальними (уніфікованими) **напрямами** виявлення кредитних ризиків є:

1. Фінансово-економічний аналіз – оцінка ключових показників фінансової стійкості підприємства (ліквідність, платоспроможність, рентабельність, оборотність активів). Дає можливість визначити слабкі місця у фінансовій діяльності та вчасно виявити ризиковані тенденції.

2. Аналіз кредитної історії та платіжної дисципліни – перевірка попереднього досвіду підприємства у виконанні боргових зобов'язань, дотримання строків розрахунків із кредиторами та постачальниками. Важливий індикатор надійності компанії.

3. Моніторинг внутрішніх бізнес-процесів – виявлення ризиків, що виникають унаслідок неефективного управління дебіторською заборгованістю, недостатнього контролю за договорами чи помилок персоналу.

4. Оцінка ринкового середовища – врахування змін у макроекономічних умовах, рівні інфляції, коливання відсоткових ставок і валютних курсів, що можуть вплинути на вартість і доступність кредитних ресурсів.

5. Аналіз галузевих ризиків – вивчення специфічних загроз для конкретної сфери діяльності підприємства (наприклад, сезонність, технологічні зміни, залежність від цін на сировину).

6. Правове та нормативне середовище – оцінка потенційних ризиків, пов'язаних зі змінами у законодавстві, податковій політиці, банківських регуляціях, які можуть ускладнити виконання кредитних договорів.

7. Використання методів прогнозування – застосування скорингових моделей, SWOT-аналізу, сценарного моделювання чи stress-testing для визначення ймовірності неплатоспроможності та оцінки потенційних наслідків ризиків.

Менеджмент кредитних ризиків – це цілеспрямований процес ідентифікації, оцінки, контролю та мінімізації ризиків, що виникають у процесі залучення чи обслуговування позикових ресурсів. Він передбачає використання фінансових, правових та організаційних інструментів для зменшення ймовірності неповернення кредитів і запобігання надмірному борговому навантаженню.

Сутність цього управління полягає у поєднанні превентивних заходів зі системним моніторингом кредитної політики підприємства, що дозволяє завчасно виявляти потенційні загрози. Завдяки цьому ефективний менеджмент кредитних ризиків забезпечує стійкість організації, її фінансову незалежність та конкурентоспроможність у довгостроковій перспективі. Основні напрями управління кредитними ризиками відображено на рис. 4.2.

Отже, управління кредитними ризиками – це важливе завдання організацій, оскільки воно безпосередньо визначає їхню фінансову стійкість, ліквідність та здатність підтримувати стабільну діяльність у динамічному ринковому середовищі. Ефективне управління кредитними ризиками дозволяє мінімізувати ймовірність неповернення боргів, оптимізувати структуру кредитного портфеля, а також уникнути надмірного боргового навантаження, що може призвести до банкрутства чи втрати інвестиційної привабливості.

Завдяки системному підходу до виявлення, оцінки та контролю кредитних ризиків організація може своєчасно реагувати на зміни у внутрішньому та зовнішньому середовищі, формувати адекватні резерви та впроваджувати механізми страхування від можливих збитків. Управління цими ризиками також сприяє зміцненню довіри з боку кредиторів, партнерів та інвесторів, що є ключовим фактором для залучення додаткових ресурсів і довгострокового розвитку бізнесу.

Кредитні ризики виявляються саме у процесі надання та отримання позикових ресурсів, як у формі короткострокових, так і довгострокових фінансових зобов'язань. Вони виникають тоді, коли одна зі сторін – кредитор чи позичальник – не може або не бажає виконати свої договірні умови, що створює загрозу втрати коштів, доходів чи ліквідності. Таким чином, кредитна безпека стосується виключно тих відносин, де є рух позикових капіталів, а її ефективне забезпечення залежить від системи управління ризиками як під час видачі кредитів, так і при їх обслуговуванні.

Типовими кредитними зобов'язаннями (кредитними коштами) сучасних організацій, які фіксуються у розділі

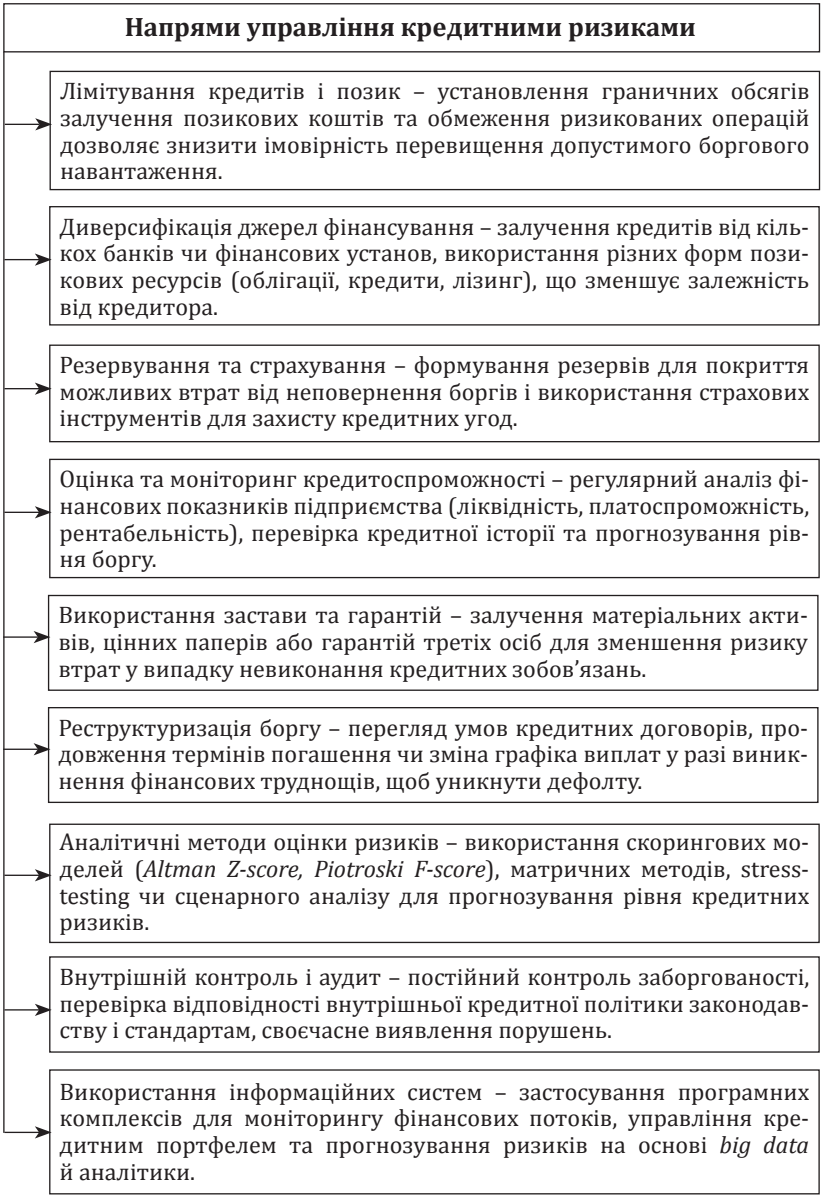


Рис. 4.2. Основні напрями управління кредитними ризиками

«Зобов'язання» (поточні або довгострокові) балансу та які вимагають постійного управління з боку підприємства, є:

– короткострокові банківські кредити та овердрафти, що підлягають погашенню протягом одного року;

– довгострокові позики (завершення погашення – понад один рік) або облігації / бондові випуски;

– зобов'язання за кредитними лініями або «ринковими» кредитами, які організація може використовувати за потреби;

– забезпечені кредити під заставу майна або активів (наприклад, іпотека, лізинг, кредити під гарантії);

– короткострокові зобов'язання – «кредиторська заборгованість» перед постачальниками, контрагентами, що формується в процесі господарської діяльності;

– поточні відсоткові зобов'язання за раніше отриманими кредитами або зобов'язаннями;

– відкладені зобов'язання (*deferred liabilities*), або контингентні зобов'язання, що можуть перерости в кредитні виплати у майбутньому;

– лізингові зобов'язання, в тому числі фінансовий лізинг, який у бухгалтерському обліку організації визнається як зобов'язання.

Зобов'язання відіграють важливу роль у діяльності підприємства, оскільки вони відображають джерела залучених фінансових ресурсів та визначають ступінь залежності компанії від кредиторів. Через кредити, позики, лізингові угоди чи відстрочені платежі підприємство отримує додаткові можливості для фінансування інвестицій, розширення виробництва або покриття поточних витрат. Таким чином, зобов'язання є своєрідним «важелем розвитку», що допомагає організації підтримувати ліквідність, навіть коли власних оборотних коштів недостатньо. Водночас надмірне боргове навантаження може створювати ризики втрати фінансової стійкості та зростання витрат на обслуговування боргу.

З іншого боку, зобов'язання виконують функцію механізму відповідальності перед зовнішніми та внутрішніми стейкхолдерами. Наявність боргових зобов'язань дисциплінує менеджмент у плануванні грошових потоків, змушує дотримуватися фінансової дисципліни та стимулює прозорість бізнес-процесів. Від своєчасного виконання зобов'язань

залежить репутація підприємства на ринку, довіра інвесторів, банків і партнерів. Отже, роль зобов'язань подвійна: вони є як інструментом розвитку і розширення можливостей підприємства, так і фактором ризику, що потребує ефективного управління та контролю.

4.3. Оцінка рівня кредитної безпеки банківських установ

Оцінка рівня кредитної безпеки – це системна процедура вимірювання стійкості банку до кредитних втрат: від якості портфеля і достатності покриття ризиків – до здатності витримати шоки без порушення нормативів капіталу та ліквідності. Вона спирається на методики внутрішнього ризик-менеджменту регуляторні стандарти (Базель, настанови ЕВА) та національні вимоги (НБУ), і завершується управлінськими рішеннями щодо лімітів, резервів, капіталу та стратегії кредитування.

Ціль оцінки кредитної безпеки банку полягає у своєчасному виявленні потенційних ризиків, які можуть негативно вплинути на його фінансову стабільність та здатність виконувати зобов'язання перед вкладниками і контрагентами. Така оцінка дозволяє банківській установі визначити реальний рівень захищеності від кредитних загроз, оцінити ефективність управління кредитним портфелем та виявити слабкі місця у політиці ризик-менеджменту. Вона також сприяє підвищенню довіри клієнтів і партнерів, формує передумови для стійкого розвитку, зниження ймовірності дефолтів та забезпечення відповідності діяльності банку нормативним вимогам і міжнародним стандартам.

Достатній рівень кредитної безпеки банку – це такий стан його кредитної діяльності, при якому установа спроможна своєчасно і повністю виконувати свої зобов'язання перед вкладниками, інвесторами та контрагентами, підтримуючи стабільність і ліквідність навіть за умов дії внутрішніх чи зовнішніх ризиків. Він передбачає оптимальне співвідношення між обсягом наданих кредитів та можливістю їх повернення, якісне управління кредитним портфелем, дотримання нормативів платоспроможності, а також ефективний

контроль за кредитними ризиками. Такий рівень забезпечує банку фінансову стійкість, підвищує його конкурентоспроможність на ринку, формує довіру клієнтів і створює умови для сталого розвитку у довгостроковій перспективі.

Найважливішими напрямами та індикаторами оцінювання кредитної безпеки банківських установ є такі:

1. Якість кредитного портфеля (мікрорівень):

– частка проблемної заборгованості (*NPL/NPE*), темпи її зміни; порогові орієнтири для «значного» рівня *NPL* у практиці ЄС (≈5% брутто-показника);

– покриття NPL резервами (*NPL coverage*), співвідношення застав / гарантій до ризиків;

– концентрації за позичальниками / галузями / видами продуктів; частка валютного кредитування.

Частка проблемної заборгованості (*NPL/NPE*) є одним із ключових індикаторів фінансової безпеки та стабільності банківської системи, оскільки вона демонструє співвідношення кредитів, за якими боржники не виконують свої зобов'язання, до загального кредитного портфеля. Динаміка змін цього показника дозволяє визначити тенденції у сфері кредитних ризиків і своєчасно реагувати на можливі загрози фінансовій стійкості банку. У міжнародній практиці, зокрема в Європейському Союзі, вважається, що перевищення рівня *NPL* у 5% від загального обсягу кредитів є критичним порогом, що сигналізує про значне погіршення якості кредитного портфеля та потребує негайних управлінських і регуляторних заходів. Саме тому моніторинг частки проблемної заборгованості та контроль за її зростанням є фундаментально важливими для забезпечення кредитної безпеки як окремих фінансових установ, так і банківської системи в цілому. Основні порогові орієнтири для *NPL/NPE* у різних країнах наведено в додатку Д.

2. Ризикові параметри та очікувані збитки:

– розрахунок *PD, LGD, EAD* (ймовірність дефолту, втрата в разі дефолту, експозиція на дату дефолту) у межах стандартних або внутрішніх підходів (*IRB*);

– очікуваний кредитний збиток розраховують за допомогою формули $EL = PD \times LGD \times EAD$;

– вимоги до оцінювання *PD/LGD* та до обробки дефолтних експозицій у керівництвах *EBA*.

3. Капітал проти ризику. Розрахунок *RWA* за кредитним ризиком (стандартний *vs IRB*) і вплив на нормативи достатності капіталу; відмінності між підходами за даними порівняльних досліджень.

4. Регуляторні перевірки, моделі та звітність. В Україні банки зобов'язані застосовувати встановлені НБУ методики визначення кредитного ризику (індивідуальна / групова оцінка, підходи до застав, порядок формування резервів, мінімальні процедури), а також вимоги до RWA.

5. Стрес-тестування кредитного ризику. Оцінка втрат у несприятливих сценаріях (падіння ВВП, девальвація, відсоткові шоки), їх вплив на капітал і виконання нормативів; актуальні методики НБУ і практика воєнного періоду. Стрес-тестування кредитного ризику є важливим інструментом управління, оскільки дає можливість банкам заздалегідь оцінити стійкість до макроекономічних та фінансових шоків. Воно допомагає визначити, наскільки банк здатний виконувати нормативи капіталу в умовах кризових подій, та вчасно коригувати свою політику управління ризиками.

На додаток використання сценарного аналізу в поєднанні з методами стрес-тестування сприяє формуванню резервів під можливі втрати, що підвищує рівень фінансової безпеки банківської установи. В умовах воєнного стану в Україні ці практики набули особливого значення, адже дозволяють більш реалістично прогнозувати вплив нестабільності на кредитні портфелі та здійснювати превентивні заходи.

6. Інтегральні/композитні оцінки безпеки. Академічні підходи пропонують індикативні системи та інтегральні індекси економічної/фінансової безпеки банків (зважені суми нормалізованих показників, матриці пріоритетів). Є корисні для бенчмарку між банками/часовими періодами. Інтегральні або композитні оцінки дозволяють узагальнено відобразити рівень фінансової безпеки банківської установи шляхом поєднання багатьох окремих показників в єдиний індекс. Це забезпечує можливість простежити динаміку змін безпеки у часі та швидко ідентифікувати тенденції, які не завжди очевидні з аналізу окремих коефіцієнтів.

Крім того, такі оцінки можуть бути використані регуляторами та аналітичними центрами для створення

рейтингів фінансової стійкості, що допомагає визначати слабкі місця у діяльності банків та формувати рекомендації для їх підвищення. Це робить метод ефективним інструментом стратегічного управління кредитними ризиками та порівняльного аналізу в банківському секторі.

Комплексна оцінка кредитної безпеки банку – це поєднання портфельних метрик, моделей ризику, капітальних тестів і регуляторної відповідності. Вона дає відповідь на три запитання: наскільки якісний портфель, чи достатньо резервів і капіталу і як банк переживе стрес. Саме така рамка наразі закріплена у сучасних європейських настановах та українській практиці НБУ, включно з регулярними стрес-тестами та оновленими вимогами до оцінки кредитного ризику у 2025 році.

4.4. Оцінка рівня кредитоспроможності позичальника в системі фінансово-кредитної безпеки

Оцінка кредитоспроможності позичальника – це комплексний багатоступеневий процес, спрямований на виявлення фінансових можливостей підприємства чи фізичної особи своєчасно виконувати зобов'язання за кредитними договорами. Мета цього аналізу полягає у зменшенні кредитних ризиків, формуванні об'єктивної картини фінансової стійкості позичальника та забезпеченні інтересів кредитора. Застосування різних методів і підходів дає змогу всебічно оцінити як поточний фінансовий стан, так і перспективи діяльності боржника.

Оцінка кредитоспроможності має бути проведена детально, за актуальними даними фінансової звітності та управлінського обліку, із верифікацією інформації з незалежних джерел (податкові витяги, кредитні бюро, реєстри судових рішень, дані контрагентів). Аналіз повинен охоплювати динаміку щонайменше за 8–12 останніх кварталів, щоб відстежити тренди ліквідності, платоспроможності, рентабельності та структури боргу, а також враховувати якісні чинники – якість менеджменту, концентрацію на ключових клієнтах / постачальниках, ризики судових спорів і ділової репутації.

Цілі оцінки кредитоспроможності позичальника подано на рис. 4.3.

Рис. 4.3. Цілі оцінки кредитоспроможності позичальника

Оцінка кредитоспроможності має суттєві переваги як для підприємств, так і для банківських установ. Для самих підприємств вона виступає інструментом перевірки власної фінансової стійкості та надійності, дозволяє виявити сильні та слабкі сторони фінансової діяльності. Завдяки цьому підприємство може своєчасно вживати заходів щодо підвищення ліквідності, оптимізації боргового навантаження та вдосконалення системи управління ресурсами. Крім того, позитивна оцінка кредитоспроможності підвищує репутацію організації на ринку, створює умови для залучення інвестицій та формує конкурентні переваги у відносинах із партнерами.

Для кредитних установ і банків оцінка кредитоспроможності позичальників є важливим механізмом управління ризиками. Вона дає змогу мінімізувати ймовірність виникнення проблемної заборгованості, підвищує якість кредитного портфеля та забезпечує стабільність фінансової системи

банку. Окрім цього, точна оцінка допомагає банку визначати умови кредитування, що найбільше відповідають фінансовим можливостям позичальника, знижуючи ризики неповернення коштів. У стратегічному плані це сприяє зміцненню довіри клієнтів і партнерів до банку, стабільному зростанню його прибутковості та довгостроковій фінансовій безпеці.

Оцінка кредитоспроможності позичальника відбувається за певними напрямами та методами:

1. Використання фінансового аналізу для оцінки. Фінансовий аналіз є ключовим елементом у визначенні кредитоспроможності. Він передбачає дослідження фінансової звітності з метою виявлення сильних і слабких сторін у діяльності підприємства. Основні складові цього аналізу:

– аналіз балансу – вивчається структура активів і пасивів, співвідношення власного та позикового капіталу;

– оцінка звіту про фінансові результати – визначається прибутковість, рівень витрат та ефективність господарської діяльності;

– аналіз ліквідності – розраховуються коефіцієнти, які відображають здатність підприємства погашати короткострокові борги:

$$К_{\text{поточ. лікв}} = \frac{\text{Оборотні активи}}{\text{Поточні зобов'язання}}; \quad (4.1)$$

$$К_{\text{швид. лікв}} = \frac{\text{Оборотні активи – Запаси}}{\text{Поточні зобов'язання}}; \quad (4.2)$$

– аналіз платоспроможності – досліджується спроможність підприємства виконувати довгострокові зобов'язання:

$$К_{\text{автономії}} = \frac{\text{Власний капітал}}{\text{Усього активів}}; \quad (4.3)$$

$$К_{\text{покриття відсотків}} = \frac{EBIT}{\text{Відсотки до сплати}}. \quad (4.4)$$

2. Аналіз грошових потоків (*Cash Flow Analysis*). Дає змогу оцінити, чи достатньо грошових надходжень генерує компанія для покриття своїх витрат і боргів. Аналізуються:

– операційні потоки – надходження від основної діяльності;

– інвестиційні потоки – витрати на придбання основних засобів та інвестицій;

– фінансові потоки – погашення боргів та залучення нових кредитів;

– чистий грошовий потік – це сума різниці між вхідним грошовим потоком підприємства (*In Cash Flow*) та вихідним грошовим потоком підприємства (*Out Cash Flow*):

$$Cash\ Flow = ICF - OCF. \quad (4.5)$$

Додатковий показник:

$$FCF = CFO - CapEx, \quad (4.6)$$

де *FCF* – вільний грошовий потік, *CFO* – кошти від операційної діяльності, *CapEx* – капітальні витрати.

Загальна класифікація грошових потоків підприємства подана в додатку Е.

3. Оцінка кредитної історії. Аналіз дисциплінованості позичальника у минулих розрахунках. Перевіряється: наявність прострочень, судових спорів, кількість і частота отриманих кредитів, якість їх погашення. Чиста кредитна історія підвищує рівень довіри кредитора. Оцінка кредитної історії передбачає не лише перевірку своєчасності погашення боргів, а й аналіз рівня відповідальності позичальника у фінансових відносинах. Враховується також співвідношення між обсягом отриманих кредитів та фактичними фінансовими можливостями боржника, що дозволяє оцінити його здатність управляти борговим навантаженням.

Особливу увагу банки приділяють повторюваності прострочок та наявності реструктуризованих боргів, адже вони можуть сигналізувати про низьку дисципліну або фінансову нестабільність. У свою чергу, позитивна кредитна історія формує довіру з боку фінансових установ і часто стає підґрунтям для надання більш вигідних умов кредитування. Шкала кредитної історії може мати певний вигляд (табл. 4.4).

4. Метод рейтингової оцінки. Фінансові установи створюють власні внутрішні рейтингові системи, які враховують широкий спектр фінансових і нефінансових параметрів. До основних показників, що беруться до уваги, відносять: платоспроможність компанії, її ліквідність, прибутковість діяльності, структуру капіталу, рівень диверсифікації джерел фінансування, стабільність грошових потоків, а також наявність ліквідного забезпечення чи гарантій.

Таблиця 4.4

Шкала оцінки кредитної історії

Рівень оцінки	Характеристика
Відмінна кредитна історія (рівень 5)	Позичальник не має жодних прострочених платежів, всі зобов'язання виконувалися вчасно і в повному обсязі. Відсутні судові справи чи реструктуризації боргу. Така історія дає змогу отримати найкращі умови кредитування та високий рівень довіри кредитора.
Добра кредитна історія (рівень 4)	Можуть бути поодинокі випадки несуттєвих прострочень, які були швидко врегульовані. Боргове навантаження відповідає фінансовим можливостям позичальника. Кредитор вважає такого клієнта надійним із низьким рівнем ризику.
Задовільна кредитна історія (рівень 3)	Є кілька випадків прострочених платежів середнього строку або реструктуризація одного з кредитів. Фінансовий стан стабільний, але кредитор може запропонувати менш вигідні умови або додаткові гарантії.
Слабка кредитна історія (рівень 2)	Систематичні прострочення, наявність реструктуризацій чи високого боргового навантаження. Існують ризики невиконання зобов'язань у майбутньому. Для отримання кредиту обов'язковою умовою стає застава або поручительство.
Дуже слабка кредитна історія (рівень 4)	Тривалі прострочення, значні борги, судові процеси або факти невиконання зобов'язань. Позичальник вважається високоризиковим і, як правило, отримує відмову у кредитуванні.

На основі цих характеристик підприємству присвоюється певний кредитний рейтинг, який відображає ступінь ризику та визначає умови кредитування – від відсоткової ставки до обсягу можливого фінансування.

Крім того, рейтингові моделі враховують якісні фактори: ділову репутацію компанії, ефективність системи корпоративного управління, якість менеджменту, а також перспективи розвитку галузі, в якій функціонує підприємство. Такий підхід дозволяє комплексно оцінити не лише поточний фінансовий стан позичальника, а також його потенційну здатність обслуговувати боргові зобов'язання в майбутньому. Використання рейтингових систем забезпечує більш об'єктивний розподіл клієнтів за рівнем надійності та підвищує прозорість кредитних рішень банку.

5. Метод аналізу фінансових коефіцієнтів (*Ratio Analysis*). Орієнтується на співвідношення ключових фінансових показників:

– коефіцієнт ліквідності:

$$К_{лікв} = \frac{\text{Оборотні активи}}{\text{Поточні зобов'язання}}; \quad (4.7)$$

– коефіцієнт заборгованості (Debt Ratio):

$$DR = \frac{\text{Зобов'язання}}{\text{Активи}}; \quad (4.8)$$

– коефіцієнт покриття боргу:

$$DSRR = \frac{\text{Чистий операційний прибуток}}{\text{Боргова служба}}; \quad (4.9)$$

– коефіцієнт рентабельності активів:

$$ROA = \frac{\text{Чистий прибуток}}{\text{Усього активів}}. \quad (4.10)$$

Ці показники допомагають визначити, наскільки ефективно позичальник використовує активи та чи може він обслуговувати свої борги.

6. SWOT-аналіз оцінює сильні та слабкі сторони компанії, а також можливості і загрози, що можуть вплинути на здатність погашати кредит. Це дозволяє зрозуміти ризики та можливості розвитку компанії в контексті ринкових умов (проаналізовано у темі 3).

7. Оцінка застави. Якщо кредит забезпечений заставою, необхідно оцінити ліквідність і вартість заставного майна. Застава є додатковим засобом забезпечення кредиту, і її оцінка відіграє важливу роль у прийнятті рішення про надання позики.

8. Метод скорингу (*Credit Scoring*). Цей метод базується на математичному та статистичному аналізі показників кредитоспроможності. Скорингова модель автоматично оцінює кредитний ризик, використовуючи низку показників (доходи, кредитну історію, витрати, вік та інше) і присвоює бал, що визначає можливість надання кредиту.

Також рекомендовано:

– використовувати набір коефіцієнтів (ліквідність, покриття відсотків, *leverage*, оборотність), *cash-flow* аналіз (операційний, вільний грошовий потік), *PD/LGD/EAD* для очікуваних збитків, а також скорингові й рейтингові моделі;

– виконати стрес-тести (шоки виручки, маржі, відсоткових ставок, курсу) і сценарний аналіз (базовий/несприятливий/критичний) із перевіркою ковенантів;

– підтягнути позабалансові ризики (гарантії, поручительства, факторинг без регресу, судові претензії) і податкові/регуляторні зобов'язання;

– перевірити забезпечення: ліквідність і дисконт застав, адекватність покриття LTV, юридичну чистоту активів;

– оцінити ESG/операційні ризики (перерви ланцюгів постачання, воєнні впливи, кіберризики), що можуть пришвидшити дефолт;

– зафіксувати cut-off date аналізу та вимоги до періодичності оновлення (місячно/квартально), політику тригерів для перегляду лімітів і цінових надбавок за ризик.

Питання для самоконтролю

1. У чому полягає сутність кредитної безпеки організації та як вона впливає на фінансову стійкість?
2. Які фактори внутрішнього та зовнішнього середовища формують рівень кредитних загроз підприємства?
3. У чому полягає різниця між кредитоспроможністю та кредитною безпекою підприємства?
4. Які основні принципи необхідно враховувати під час побудови системи кредитної безпеки організації?
5. Які методи оцінки кредитних ризиків застосовуються на сучасних підприємствах та у банківській практиці?
6. Якими є цілі управління кредитною безпекою організації у коротко- та довгостроковій перспективі?
7. У чому полягає роль суб'єктів управління кредитною безпекою та які завдання вони виконують?
8. Які етапи включає процес управління кредитними ризиками та як вони взаємопов'язані між собою?
9. У чому полягає значення кредитної історії позичальника для оцінки його кредитоспроможності?
10. Які сучасні міжнародні підходи (наприклад, вимоги Базельських угод, стандарти ЄС) використовуються для підвищення рівня кредитної безпеки фінансових установ?

Тестові завдання

1. Яка основна мета кредитної безпеки підприємства?

а) Забезпечення найвищого прибутку незалежно від ризиків;

б) залучення максимальної кількості кредитних ресурсів;

в) забезпечення стабільності та мінімізації ризиків у сфері кредитних відносин;

г) виключно контроль грошових потоків.

2. Що відноситься до внутрішніх чинників кредитної безпеки?

а) Політична стабільність у країні;

б) ефективність управління фінансами та рівень ліквідності підприємства;

в) рівень конкуренції на ринку банківських послуг;

г) наявність кризових явищ у світовій економіці.

3. Яке визначення найточніше характеризує поняття «кредитоспроможність»?

а) Здатність підприємства накопичувати боргові зобов'язання;

б) здатність підприємства вчасно та повністю виконувати кредитні зобов'язання;

в) наявність забезпечення у вигляді застави;

г) здатність підприємства інвестувати у нові проєкти.

4. Який із методів використовується для оцінки кредитоспроможності позичальника?

а) Економетричне прогнозування;

б) SWOT-аналіз, фінансовий аналіз та скорингові моделі;

в) лише вивчення кредитної історії;

г) оцінка міжнародного іміджу країни.

5. Яка функція системи кредитної безпеки є основною?

а) Виключно моніторинг інвестиційної діяльності;

б) забезпечення захищеності організації від кредитних ризиків та неплатоспроможності;

в) розвиток міжнародного партнерства;

г) управління матеріально-технічною базою.

6. Яке значення має кредитна історія позичальника?

а) Не відіграє суттєвої ролі для кредиторів, не впливає на розмір кредитного договору клієнта;

б) визначає рівень дисциплінованості щодо погашення боргів та впливає на умови кредитування, відсотків та способу погашення заборгованості;

в) відображає лише розмір боргових зобов'язань;

г) використовується лише для внутрішнього обліку банку.

7. Який принцип управління кредитною безпекою є найважливішим?

а) Максимізація прибутку за рахунок кредитного навантаження;

б) прозорість, системність та превентивність заходів;

в) виключно концентрація на інвестиційних ризиках;

г) повна відмова від позикового фінансування.

8. У чому полягає перевага використання скорингових моделей?

а) У ручному аналізі кредитної історії;

б) у швидкості та об'єктивності визначення рівня кредитного ризику;

в) у визначенні вартості заставного майна;

г) у виключно прогнозуванні грошових потоків.

9. Чому управління кредитною безпекою є важливим для банківських установ?

а) Дозволяє уникнути валютних ризиків;

б) забезпечує збереження ліквідності та фінансової стійкості банку;

в) сприяє виключно збільшенню статутного капіталу;

г) допомагає мінімізувати витрати на персонал.

10. Яке із тверджень відображає стратегічну ціль управління кредитною безпекою?

а) Залучення кредитів у будь-який спосіб;

б) зниження ризику неповернення боргів і створення передумов для сталого розвитку;

в) виключно формування резервних фондів;

г) виникнення інноваційних методів управління ризиками.

Практичні завдання

Завдання 1.

ТОВ «Омега» планує отримати банківський кредит у розмірі 5 млн грн на 3 роки для модернізації виробництва. Для попередньої оцінки кредитоспроможності банк аналізує фінансову звітність підприємства.

Відомі дані (тис. грн):

- Активи всього – 18 000 тис. грн
- Власний капітал – 6 000 тис. грн
- Довгострокові зобов'язання – 7 500 тис. грн
- Короткострокові зобов'язання – 4 500 тис. грн
- Чистий прибуток – 1 200 тис. грн

– Виторг від реалізації – 15 000 тис. грн
– Оборотні активи – 6 800 тис. грн
– Поточні зобов'язання – 4 500 тис. грн

1. Розрахуйте коефіцієнт автономії (Власний капітал / Активи).

2. Визначте коефіцієнт поточної ліквідності (Оборотні активи / Поточні зобов'язання).

3. Обчисліть рентабельність продажів (Чистий прибуток / Виторг × 100%).

4. Зробіть висновок, чи має підприємство достатній рівень кредитної безпеки для отримання позики.

Завдання 2.

АТ «ФінПром» має такі показники (млн грн):

– Загальна сума активів – 40 тис. грн
– Власний капітал – 10 тис. грн
– Загальна сума зобов'язань – 30 тис. грн
– Операційний прибуток (EBIT) – 6 тис. грн
– Витрати на обслуговування боргу (відсотки) – 2 тис. грн
– Чистий прибуток – 3 тис. грн

1. Розрахуйте коефіцієнт фінансового левериджу (Зобов'язання / Власний капітал).

2. Обчисліть коефіцієнт покриття відсотків (EBIT / Витрати на відсотки).

3. Оцініть, чи є рівень боргового навантаження прийнятним для забезпечення кредитної безпеки.

4. Запропонуйте два управлінські рішення, які дозволять знизити кредитні ризики підприємства.

Завдання 3.

ТОВ «ФінБуд» займається наданням логістичних і консалтингових послуг. У період економічної нестабільності компанія активно залучала кредитні кошти для фінансування оборотного капіталу, придбання техніки та розвитку нових напрямів бізнесу. У результаті за останні два роки загальний обсяг короткострокових і довгострокових зобов'язань суттєво зріс. Хоча підприємство вчасно виконує свої зобов'язання перед банками, у керівництва виникли побоювання щодо надмірного боргового навантаження та зниження фінансової стійкості.

Додатковою проблемою стало те, що частина кредитів залучена під високі відсоткові ставки, а умови договорів містять жорсткі вимоги щодо забезпечення. До того ж, війна та пов'язані з нею

обстріли негативно вплинули на діяльність партнерів компанії, що призвело до затримки виконання контрактів та ризику зростання дебіторської заборгованості. В підсумку у підприємства з'явилися нові загрози: можливі штрафні санкції від банків за несвоєчасні платежі, ризик втрати частини заставного майна, а також погіршення ділової репутації перед кредиторами та інвесторами.

Керівництво компанії поставило завдання розробити комплексну систему управління кредитною безпекою, яка має передбачати ідентифікацію кредитних ризиків, аналіз умов кредитних договорів, оптимізацію структури боргових зобов'язань, розробку механізмів моніторингу платоспроможності, а також заходи зі захисту фінансових ресурсів у кризових ситуаціях.

1. Визначте основні кредитні ризики, що виникають у діяльності ТОВ «ФінБуд».

2. Запропонуйте управлінські рішення, які можуть знизити вплив негативних факторів на кредитну безпеку.

3. Обґрунтуйте, чому важливо поєднувати фінансові, юридичні та організаційні заходи при формуванні системи управління кредитною безпекою.

ТЕМА 5
УПРАВЛІННЯ ІНВЕСТИЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

5.1. Сутність та складові інвестиційної безпеки

5.2. Емісійна та дивідендна політика в системі інвестиційної безпеки

5.3. Напрями оцінки інвестиційної безпеки організації

5.4. Роль фінансових посередників у забезпеченні інвестиційної безпеки організації

Основні поняття і терміни: організація, інвестиції, інвестиційна безпека, цінні папери, інвестиційні ризики, дивідендна політика, емісійна політика, ризик-менеджмент, акції, облігації, фінансові посередники.

5.1. Сутність та складові інвестиційної безпеки

В умовах сучасної економіки інвестиційна безпека є одним із основних елементів загальної системи економічної безпеки підприємства. Вона визначає здатність організації залучати, ефективно використовувати та захищати інвестиційні ресурси від зовнішніх і внутрішніх загроз. Інвестиційна безпека передбачає не лише наявність достатніх фінансових ресурсів для реалізації проєктів, а й створення передумов для їх раціонального розподілу, контролю ризиків та досягнення стратегічних цілей розвитку.

У нинішніх умовах діяльності організацій, що характеризуються високою турбулентністю ринків, нестабільністю законодавчого середовища та зростанням конкуренції, управління інвестиційною безпекою набуває особливої ваги. Воно надає можливості не лише уникати фінансових втрат і недоотримання прибутку, а й формує підґрунтя для довгострокового розвитку та підвищення інвестиційної привабливості підприємства. Забезпечення інвестиційної безпеки включає прогнозування можливих загроз, оцінку ризиків, оптимізацію структури інвестицій та використання сучасних методів їх захисту.

Інвестиційна безпека підприємства тісно пов'язана з інвестиційною, емісійною та дивідендною діяльністю, оскільки саме вони визначають можливість організації формувати й ефективно використовувати власний та залучений капітал. Інвестиційна діяльність створює базу для розвитку підприємства, дозволяє оновлювати основні фонди, впроваджувати інноваційні технології та підвищувати конкурентоспроможність продукції. Водночас емісійна політика впливає на здатність компанії залучати додаткові фінансові ресурси шляхом випуску цінних паперів, що напряму відображається на стабільності та захищеності підприємства від зовнішніх загроз. Дивідендна політика, своєю чергою, формує довіру інвесторів і акціонерів, а також визначає рівень їхньої зацікавленості у подальшому співробітництві з підприємством.

Взаємозв'язок цих сфер діяльності проявляється у формуванні збалансованої фінансової стратегії, яка повинна одночасно гарантувати економічну стійкість підприємства та створювати привабливі умови для інвесторів. Якщо інвестиційна політика забезпечує розвиток і модернізацію виробництва, то емісійна формує джерела фінансування, а дивідендна підтримує стабільність і довіру до компанії. Завдяки їх узгодженості можна мінімізувати ризики, зберегти фінансову незалежність і забезпечити тривалу стійкість підприємства навіть у несприятливих умовах, що робить інвестиційну безпеку головним чинником у системі загальної економічної безпеки організації.

Інвестиційну безпеку дійсно можна розглядати у двох ключових аспектах – з погляду інвестора та з боку організації-емітента, яка залучає інвестиції через випуск цінних паперів. Обидва підходи взаємопов'язані, проте мають різні акценти, завдання й механізми забезпечення. Для інвестора інвестиційна безпека означає гарантії захищеності вкладених коштів та отримання очікуваного прибутку без надмірних ризиків. Вона включає:

– фінансовий аспект – збереження вартості вкладених активів, можливість отримання дивідендів чи відсотків, мінімізація втрат від коливань ринку або банкрутства емітента;

– правовий аспект – наявність ефективного законодавчого захисту прав інвестора, прозорість корпоративного управління та механізмів контролю за діяльністю компанії;

– інформаційний аспект – своєчасний доступ до достовірної інформації про фінансовий стан компанії-емітента, її ризики та перспективи розвитку;

– стратегічний аспект – можливість реалізувати довгострокові інвестиційні цілі (наприклад, зростання капіталу чи участь у стратегічних проєктах);

– соціально-етичний аспект – дотримання принципів корпоративної соціальної відповідальності, прозорої взаємодії з працівниками, партнерами та суспільством, що підвищує довіру до компанії та робить її більш привабливою для інвесторів;

– екологічний аспект – врахування екологічних стандартів і практик у діяльності організації, що знижує ризики санкцій, штрафів та втрати репутації, а також відповідає сучасним вимогам сталого розвитку;

– міжнародний аспект – орієнтація компанії на відповідність глобальним стандартам ведення бізнесу, захист інвестицій у транскордонних угодах та інтеграція у світові фінансові ринки, що створює умови для розширення кола інвесторів і диверсифікації ризиків.

Для організації, яка випускає (здійснює емісію) цінні папери або залучає капітал, інвестиційна безпека полягає у здатності забезпечити стабільний приплив інвестиційних ресурсів, підтримати довіру інвесторів і використати отримані кошти максимально ефективно. Вона охоплює:

– фінансову стійкість – організація має демонструвати платоспроможність, прозору структуру капіталу, здатність обслуговувати боргові зобов'язання;

– репутаційний фактор – високий рівень корпоративного управління та дотримання зобов'язань формують довіру інвесторів і знижують вартість залученого капіталу;

– оптимізацію інвестиційної політики – ефективне управління інвестиційними проєктами, що гарантує досягнення очікуваного ефекту від залучених ресурсів;

– захист від загроз – мінімізація ризиків рейдерства, фінансових маніпуляцій, шахрайства чи недружніх поглинань;

– довгострокову привабливість – створення умов для стабільного розвитку, що підвищує капіталізацію компанії та робить її цінні папери конкурентоспроможними на ринку.

Сутність інвестиційної безпеки полягає у забезпеченні стійкості та захищеності інвестиційних процесів від негативних впливів зовнішнього та внутрішнього середовища. Вона є частиною загальної економічної безпеки організації і передбачає управління інвестиційними ризиками з метою збереження і примноження капіталу, забезпечення стійкого розвитку підприємства. Інвестиційна безпека забезпечує підтримку достатнього рівня інвестиційних ресурсів та їх ефективного використання в економічній діяльності.

Основна мета інвестиційної безпеки – забезпечити стабільність і ефективність інвестиційного процесу, що включає розробку стратегій управління ризиками, оцінку економічної доцільності вкладень та запобігання загрозам, які можуть негативно вплинути на інвестиційний потенціал організації.

Важливе місце у формуванні політики інвестиційної діяльності підприємства займають суб'єкти, до яких відносяться власники організації (але лише тої, що здійснює емісію цінних паперів), акціонери, інвестори, фінансові посередники (професійні учасники фондового ринку), державні органи (які є причетними до інвестиційного процесу).

Об'єктами інвестиційної безпеки є:

– інвестиційні ресурси – власний і залучений капітал, що спрямовується на реалізацію інвестиційних проєктів;

– інвестиційні проєкти – програми розвитку, модернізації, впровадження інновацій, у які вкладаються кошти;

– фінансові інструменти – цінні папери (додаток Ж), корпоративні права, кредити, які використовуються для фінансування інвестиційної діяльності;

– інформаційні ресурси – аналітичні дані, звітність, прогнози, що формують інформаційну базу для ухвалення рішень;

– інтелектуальні та технологічні активи – інновації, ноу-хау, патенти, які визначають конкурентоспроможність організації;

– кадровий потенціал – працівники, залучені до розробки та реалізації інвестиційних проєктів, їхня кваліфікація та професійні компетенції;

– майнові активи – матеріальні ресурси (будівлі, обладнання, інфраструктура), які беруть участь у реалізації інвестиційних програм;

– ділова репутація та імідж – довіра інвесторів, партнерів і контрагентів, яка визначає інвестиційну привабливість компанії;

– інтереси інвесторів і власників – очікуваний рівень дохідності та захищеність їхніх вкладень;

– правове середовище – умови функціонування, які гарантують правовий захист інвестиційної діяльності.

Управління інвестиційною безпекою – це системний процес, спрямований на формування та підтримку належного рівня захищеності інвестиційних ресурсів підприємства від можливих внутрішніх і зовнішніх загроз. Воно охоплює планування, організацію, контроль і координацію інвестиційних процесів, унаслідок чого забезпечується ефективне використання капіталу та досягнення стратегічних цілей розвитку. Особливе значення управління інвестиційною безпекою набуває в умовах економічної нестабільності, коли ризики втрат і недоотримання прибутку суттєво зростають. У цьому контексті управління включає прогнозування ризиків, оцінку інвестиційної привабливості проєктів, оптимізацію структури інвестицій та створення механізмів захисту від можливих загроз.

Водночас управління інвестиційною безпекою виступає не лише як інструмент збереження фінансової стабільності, а й як важлива передумова довгострокового розвитку організації. Завдяки ефективному менеджменту підприємство може забезпечувати стабільність грошових потоків, залучати нових інвесторів, підвищувати рівень капіталізації та конкурентоспроможності. Крім того, правильне управління сприяє зміцненню довіри партнерів і формує позитивну ділову репутацію на ринку. Таким чином, інвестиційна безпека стає інтегральною складовою економічної стратегії, яка гарантує стійкість бізнесу в динамічному та ризикованому середовищі.

Оскільки інвестиційна безпека напряму пов’язана зі системою управління ризиками, що впливають на процеси інвестування, то в загальному їх можна поділити на зовнішні та внутрішні (рис. 5.1).

Рис. 5.1. Фактори, що впливають
на інвестиційну безпеку організації

Складовими інвестиційної безпеки організації є такі:

1. Фінансова складова. Забезпечує наявність стабільних джерел фінансування та контроль за ефективністю використання інвестиційних ресурсів. Вона охоплює ліквідність, рентабельність інвестиційних проєктів, структуру капіталу та здатність компанії виконувати зобов'язання перед інвесторами.

2. Правова складова. Передбачає наявність нормативно-правової бази, що регулює відносини між інвестором та організацією, захист прав власників цінних паперів, прозорість укладених контрактів та дотримання законодавчих вимог у сфері інвестиційної діяльності.

3. Інформаційна складова. Включає своєчасне отримання повної та достовірної інформації щодо ринку, стану компанії,

інвестиційних ризиків і можливостей. Забезпечує інвесторів та керівництво аналітичними даними, необхідними для прийняття обґрунтованих рішень.

4. Організаційно-управлінська складова. Відображає якість системи менеджменту, що відповідає за планування, моніторинг і контроль інвестиційних процесів. Сюди належать механізми управління ризиками, система внутрішнього аудиту та контроль за використанням капіталу.

5. Ризикова складова. Пов'язана з ідентифікацією, оцінкою та мінімізацією можливих інвестиційних ризиків (ринкових, фінансових, валютних, політичних, репутаційних). Забезпечує формування резервів і страхових механізмів для нейтралізації негативних наслідків.

6. Технологічна складова. Стосується інноваційності й технічного рівня інвестиційних проєктів. Вона визначає здатність компанії залучати інвестиції у новітні технології та зберігати конкурентоспроможність на основі технічного прогресу.

7. Соціальна складова. Відображає рівень довіри персоналу та інвесторів до компанії, соціальну відповідальність бізнесу та його вплив на трудові ресурси. Забезпечує стабільність колективу та підтримку соціального партнерства.

8. Зовнішньоекономічна складова. Стосується здатності підприємства протистояти впливу зовнішніх факторів, зокрема коливань валютних курсів, змін умов міжнародної торгівлі, інтеграційних процесів і глобальних інвестиційних трендів.

9. Репутаційна складова. Формує довіру інвесторів і партнерів до компанії, впливає на її інвестиційну привабливість та умови залучення фінансових ресурсів. Репутація визначає здатність організації підтримувати вигідні відносини з ринком капіталу.

5.2. Емісійна та дивідендна політика в системі інвестиційної безпеки

Емісійна політика організації – це система заходів і рішень, спрямованих на регулювання процесу випуску та розміщення цінних паперів. Її головна мета полягає

у забезпеченні ефективного залучення інвестиційних ресурсів та створенні сприятливих умов для фінансування розвитку підприємства. Вона охоплює визначення обсягів і структури емісії, вибір часу виходу на фондовий ринок, встановлення оптимальних умов обігу цінних паперів, а також дотримання правових і регуляторних вимог.

З практичної точки зору емісійна політика є одним із ключових інструментів управління фінансовою безпекою та інвестиційною привабливістю організації. Вона дає змогу збалансувати інтереси власників і потенційних інвесторів, сформувати прозору інформаційну політику, підвищити рівень довіри до компанії. Крім того, ефективна емісійна політика сприяє оптимізації структури капіталу, зниженню вартості залучення коштів та зміцненню конкурентних позицій на ринку.

Організація виступає центральним суб'єктом емісійного процесу, оскільки саме вона визначає потребу в додатковому капіталі, формує параметри випуску цінних паперів і здійснює управління ними на всіх етапах їх обігу. Роль організації полягає також у створенні системи корпоративного управління, яка забезпечує прозорість, захист інтересів інвесторів і відповідність міжнародним стандартам. Успішна емісійна політика дозволяє компанії залучати додаткові фінансові ресурси для інноваційного розвитку, розширення виробництва та підвищення ринкової вартості. Етапи емісійної політики зображено в табл. 5.1.

Кожен етап формування емісійної політики має вагоме значення для розвитку організації, адже саме він визначає якість і результативність процесу залучення інвестицій. На початкових стадіях (визначення потреби та аналіз умов) підприємство формує стратегічні пріоритети фінансування та оцінює ризики, що дозволяє уникнути неефективних рішень. Вибір виду цінних паперів, умов і способу розміщення напряму впливає на вартість залученого капіталу та структуру власності, що визначає подальшу фінансову стабільність. Інформаційний супровід та прозорість формують довіру інвесторів, що підвищує репутацію компанії на ринку. Моніторинг і оцінка ефективності емісії забезпечують можливість адаптації до ринкових змін і вироблення нових стратегій,

Таблиця 5.1

Етапи формування емісійної політики організації

Етап	Характеристика етапу
Визначення потреби у фінансуванні	Організація оцінює обсяги необхідних фінансових ресурсів, цілі залучення коштів (інвестиційні проєкти, розширення виробництва, модернізація, погашення боргів тощо) та можливі джерела їх отримання.
Аналіз внутрішніх і зовнішніх умов	На цьому етапі враховуються фактори ринкової кон'юнктури, стан фондового ринку, рівень інвестиційної привабливості компанії, а також макроекономічні та правові умови емісії.
Визначення виду цінних паперів та обсягу випуску	Приймається рішення про інструмент залучення капіталу (акції, облігації, опціони тощо), його кількість і номінальну вартість, терміни обігу та умови розміщення.
Розробка умов емісії та реєстрація випуску	Формуються умови випуску та розміщення, готуються необхідні документи для регулятора, проводиться реєстрація емісії відповідно до законодавчих норм.
Вибір способу розміщення	Вирішується, чи буде це відкрита (публічна) пропозиція на фондовому ринку, чи закрите (приватне) розміщення серед обмеженого кола інвесторів.
Організація інформаційного супроводу	Підприємство формує прозору інформаційну політику для інвесторів: готує проспект емісії, публічні звіти, маркетингові матеріали, проводить комунікацію з потенційними інвесторами.
Проведення розміщення цінних паперів	Безпосередній етап продажу акцій чи облігацій інвесторам із залученням біржових майданчиків, андеррайтерів чи фінансових посередників.
Моніторинг результатів та управління обігом цінних паперів.	Після завершення емісії організація здійснює контроль за динамікою курсової вартості, підтримує репутацію та довіру інвесторів, дотримується стандартів корпоративного управління.
Оцінка ефективності емісійної політики	Здійснюється аналіз результатів розміщення: чи вдалося досягти запланованих фінансових цілей, як змінилась структура капіталу та інвестиційна привабливість організації.

сприяючи сталому розвитку організації, підвищенню її конкурентоспроможності та зміцненню інвестиційної безпеки.

Отже, емісійна політика являє собою логічно впорядковану систему стратегічних рішень і дій емітента, що забезпечують випуск, розміщення та обіг цінних паперів з урахуванням умов ринку та інтересів інвесторів. Вона передбачає встановлення цілей залучення капіталу, моделювання структури акціонерного капіталу, підтримання ліквідності цінних паперів і максимізацію доходів від їх розміщення. Завдяки цій політиці емітент спроможний збалансувати інтереси розвитку, фінансової стабільності та задоволення вимог ринку, а також адаптуватися до змін зовнішнього середовища та очікувань інвесторів.

Вплив емісійної політики на інвестиційну безпеку організації проявляється через кілька ключових механізмів:

– забезпечення доступу до фінансових ресурсів – грамотно сформована емісійна політика дає змогу організації залучати додатковий капітал за рахунок випуску цінних паперів (акцій, облігацій), що підвищує інвестиційні можливості та зменшує залежність від кредитних ресурсів;

– формування оптимальної структури капіталу – політика емісії допомагає збалансувати співвідношення власних і позикових коштів, що безпосередньо впливає на фінансову стійкість і знижує ризик втрати інвестиційної привабливості;

– підвищення довіри інвесторів – прозорість умов емісії, належне розкриття інформації та контроль за обігом цінних паперів формують у інвесторів впевненість у надійності підприємства, знижуючи ризики відтоку капіталу;

– підтримка ліквідності та вартості цінних паперів – чітко спланована емісійна політика дозволяє підтримувати стабільний попит на цінні папери, що забезпечує їхню ліквідність і захищає від знецінення, а також стимулює вторинний ринок;

– захист від зовнішніх загроз – використання різних інструментів емісійної політики (застосування привілейованих акцій, облігацій з фіксованим доходом тощо) надає можливості підприємству адаптуватися до змін кон'юнктури ринку та економічної нестабільності.

Дивідендна політика – це частина загальної фінансової стратегії акціонерного товариства, що визначає рівень і механізми розподілу чистого прибутку між виплатами дивідендів акціонерам та реінвестуванням у розвиток компанії. Вона встановлює співвідношення між сумами, які направляються на виплати, і тими, що залишаються для подальшого зростання організації.

Дивідендна політика – це стратегія компанії щодо того, як і коли вона розподілятиме прибутки серед своїх акціонерів. Вона охоплює рішення про частоту виплат, розмір дивідендів і умови їх виплати, враховуючи фінансові можливості компанії та очікування інвесторів.

Роль дивідендної політики у забезпеченні інвестиційної безпеки виявляється через такі аспекти:

1. Баланс між виплатами та реінвестуванням. Дивідендна політика виступає інструментом, який визначає, яка частина прибутку буде спрямована акціонерам у вигляді дивідендів, а яка залишиться для розвитку компанії. Від того, наскільки збалансовано підприємство поєднує ці два напрями, залежить його здатність підтримувати фінансову стійкість та інвестиційну привабливість.

2. Формування довіри інвесторів. Стабільна та прозора дивідендна політика підвищує рівень довіри з боку існуючих і потенційних інвесторів. Передбачуваність виплат сприяє зниженню ризиків для власників капіталу та мотивує їх до довгострокового співробітництва з організацією. Це прямо впливає на рівень інвестиційної безпеки, адже компанія отримує надійні джерела фінансування.

3. Захист від фінансових ризиків. Продумана дивідендна політика дозволяє підприємству уникнути надмірного боргового навантаження, створювати резерви для кризових періодів і забезпечувати достатній рівень ліквідності. Це знижує ймовірність виникнення інвестиційних загроз та підвищує стійкість компанії в умовах економічної нестабільності.

4. Інструмент стратегічного управління. Окрім фінансових аспектів, дивідендна політика виконує роль сигналу для ринку: стабільні або зростаючі дивідендні виплати є ознакою здорового фінансового стану підприємства.

Це позитивно впливає на ринкову капіталізацію компанії, зменшує ризики відтоку капіталу та підсилює інвестиційну безпеку на довгостроковій основі.

5.3. Напрями оцінки інвестиційної безпеки організації

Оцінка інвестиційної безпеки є одним із основних напрямів управління фінансово-економічною стійкістю сучасних організацій. Вона дає можливість визначити здатність підприємства залучати та ефективно використовувати інвестиційні ресурси, забезпечувати захист від внутрішніх і зовнішніх загроз, а також створювати передумови для стабільного розвитку. Своєчасна та комплексна оцінка інвестиційної безпеки надає змогу виявити ризики, які можуть вплинути на дохідність та окупність проєктів, визначити оптимальні напрями інвестиційної політики, а також підвищити рівень довіри інвесторів і партнерів. У сучасних умовах динамічних ринкових змін така оцінка стає невід'ємним елементом стратегічного управління та забезпечення довгострокової конкурентоспроможності організації (рис. 5.2).

Рис. 5.2. Напрями оцінки інвестиційної безпеки організації в сучасних умовах

1. Фінансово-аналітичний напрям. Вказаний напрям передбачає аналіз динаміки основних фінансових показників, зокрема ліквідності, платоспроможності та рентабельності, які відображають поточний рівень фінансової стійкості компанії. Окрім цього, у межах цього напряму проводиться оцінка ефективності використання інвестиційних ресурсів, їх окупності та впливу на загальний фінансово-економічний результат діяльності підприємства. Важливою складовою є прогнозування інвестиційних можливостей на основі аналізу тенденцій розвитку ринку та внутрішніх резервів організації, що дозволяє формувати обґрунтовані управлінські рішення. Його основна мета – оцінка внутрішнього стану компанії, її здатності залучати, використовувати й обслуговувати інвестиційні ресурси:

– коефіцієнт рентабельності інвестицій (*ROI*):

$$ROI = \frac{\text{Чистий прибуток}}{\text{Інвестиції}} \times 100\%; \quad (5.1)$$

– чистий приведений дохід (*NPV*):

$$NPV = \sum_{t=1}^{n} \frac{1\ CF_t}{(1+r)^t} - IC, \quad (5.2)$$

де CF_t – грошовий потік у період t, r – ставка дисконту, IC – початкові інвестиційні витрати. Внутрішня норма дохідності (*IRR*): значення ставки дисконту, при якій $NPV = 0$;

– індекс рентабельності інвестицій (*PI*):

$$PI = \frac{\sum \frac{CF_t}{(1+r)^t}}{IC}, \quad (5.3)$$

– період окупності (PP):

$$PP = \frac{\text{IC}}{\text{Середній щорічний грошовий потік}}. \quad (5.4)$$

2. Ризик-орієнтований напрям. Вказаний напрям оцінки інвестиційної безпеки зосереджується на виявленні, аналізі та кількісній оцінці ризиків, які можуть супроводжувати інвестиційну діяльність організації. У межах цього підходу розглядаються як внутрішні, так і зовнішні ризики – фінансові, ринкові, політичні, правові, технологічні – для визначення їх імовірності та потенційного впливу на стабільність і прибутковість інвестицій. Особлива увага приділяється розробці сценаріїв розвитку подій і побудові механізмів

мінімізації можливих негативних наслідків для збереження стійкості організації в умовах невизначеності. Основна мета – оцінка інвестиційних ризиків та ймовірності їх реалізації. Для оцінювання використовується:

– дисперсія та стандартне відхилення доходності проєкту – характеризує волатильність результатів;

– коефіцієнт варіації (CV):

$$CV = \frac{\sigma}{\mu}, \tag{5.5}$$

де σ – стандартне відхилення, μ – середня дохідність;

– метод сценаріїв – розрахунок результатів за базовим, оптимістичним і песимістичним сценаріями;

– *value at Risk* (*VaR*): оцінка максимально можливих втрат за певний період з визначеною ймовірністю.

3. Ринково-конкурентний напрям. Цей напрям оцінки інвестиційної безпеки зосереджується на дослідженні позицій організації на ринку, рівня її конкурентоспроможності та здатності протидіяти впливу конкурентів. Він передбачає аналіз ринкової частки, привабливості інвестиційного середовища, динаміки попиту й пропозиції, а також ефективності стратегії розвитку в умовах конкурентного тиску. Мета – оцінка зовнішніх умов для безпечного інвестування. Основними методами та показниками є:

– аналіз ринкової кон'юнктури (динаміка попиту та пропозиції);

– оцінка рівня галузевих ризиків та бар'єрів входу;

– порівняльний аналіз (*Benchmarking*) з іншими компаніями;

– коефіцієнт ринкової капіталізації до прибутку (*P/E*):

$$\frac{P}{S} = \frac{\text{Ринкова ціна акції}}{\text{Прибуток на акцію}}; \tag{5.6}$$

– коефіцієнт ринкової капіталізації до виручки (*P/S*):

$$\frac{P}{S} = \frac{\text{Ринкова капіталізація}}{\text{Чистий дохід}}. \tag{5.7}$$

Окремим важливим показником є ринкова капіталізація підприємства, яка визначає позиціювання на фондовому ринку, вартість та рівень довіри з боку інвесторів. Ринкова капіталізація – це показник, що відображає загальну ринкову вартість компанії, яка визначається на основі ціни її акцій

на фондовому ринку. Вона є важливим орієнтиром для інвесторів, адже демонструє рівень довіри ринку до підприємства, його інвестиційну привабливість і масштаби діяльності. Розраховується ринкова капіталізація за формулою:

$$MC = P \times N, \quad (5.8)$$

де MC – ринкова капіталізація, P – поточна ринкова ціна однієї акції, N – загальна кількість випущених в обіг акцій.

Що вищою є ринкова капіталізація, то більш стабільною і фінансово сильною вважається компанія на ринку, а її акції сприймаються інвесторами як менш ризикові для вкладень.

4. Інституційно-правовий напрям. Вказаний напрям оцінки інвестиційної безпеки зосереджується на аналізі того, наскільки стабільною та ефективною є законодавча й регуляторна база, в межах якої функціонує організація. Цей підхід передбачає дослідження державної політики у сфері інвестицій, податкового та митного законодавства, а також рівня захисту прав інвесторів. Важливим аспектом є оцінка незалежності судової системи та ефективності регуляторних органів, оскільки саме від цього залежить довіра до інвестиційного середовища. Крім того, враховуються міжнародні стандарти і вимоги, зокрема імплементація норм ЄС чи рекомендацій міжнародних фінансових організацій, що безпосередньо впливають на інвестиційну привабливість і безпеку організації. Його мета – оцінка захищеності інвестора та підприємства в правовому полі, зокрема з використанням таких методів, як:

– аналіз нормативно-правового середовища, що регулює інвестиційну діяльність;

– моніторинг змін у податковому, корпоративному, антимонопольному законодавстві;

– оцінка рівня захисту прав власників цінних паперів, прозорості корпоративного управління.

5. Соціально-репутаційний напрям. Такий напрям оцінки інвестиційної безпеки спрямований на аналіз рівня довіри суспільства, інвесторів і ділових партнерів до організації, що формується на основі її репутації, прозорості діяльності та корпоративної соціальної відповідальності. Високий рівень соціально-репутаційної безпеки підвищує

привабливість компанії для інвесторів, зменшує ризики втрати клієнтів і сприяє зміцненню її довгострокової конкурентоспроможності. Основна мета – виявлення нематеріальних факторів, що впливають на інвестиційну безпеку, а методами оцінювання є:

– аналіз корпоративної репутації та прозорості діяльності;

– оцінка ESG-факторів (екологічні, соціальні, управлінські стандарти);

– індикатори довіри інвесторів (наприклад, кількість партнерських угод, обсяг іноземних інвестицій).

6. Комплексні інтегральні методи. Вказані методи оцінки інвестиційної безпеки ґрунтуються на поєднанні багатьох показників, які нормалізуються та зважуються, що дозволяє сформувати єдиний інтегральний індекс рівня безпеки. Такі підходи забезпечують всебічну оцінку стану організації, враховуючи фінансові, ринкові, ризикові та інституційно-правові фактори, і дають можливість порівнювати різні підприємства або відстежувати динаміку в часі. Метою цього методу є узагальнення результатів оцінки за різними напрямами:

– інтегральний показник інвестиційної безпеки:

$$I_{\text{інв.без.}} = \sum_{t=1}^{n} w_i \times x_i , \qquad (5.9)$$

де x_i – нормалізовані значення показників, w_i – їх вагові коефіцієнти;

– SWOT-аналіз інвестиційної безпеки – виявлення сильних і слабких сторін, можливостей та загроз;

– індикативні системи – порівняння фактичних значень показників із пороговими орієнтирами.

5.4. Роль фінансових посередників у забезпеченні інвестиційної безпеки організації

Сучасний етап розвитку фондового ринку вирізняється істотними зрушеннями у сфері фінансового посередництва, де з’являються нові інструменти та сервіси, спрямовані на впровадження стратегічно важливих, інноваційних та прибуткових рішень. Професійні учасники ринку вже не обмежуються лише класичними операціями з інвестиційними

ресурсами, а активно формують нові можливості для інтеграції національного ринку в міжнародний фінансовий простір, відкриваючи шляхи для залучення як вітчизняних, так і іноземних інвесторів та емітентів.

В Україні класифікація професійних учасників фондового ринку здійснюється Національною комісією з цінних паперів та фондового ринку відповідно до чинних нормативно-правових актів. Вона базується на розмежуванні видів діяльності у сфері цінних паперів та визначає перелік суб'єктів, які мають право на здійснення посередницьких, організаційних і розрахунково-клірингових функцій (рис. 5.3).

Додатково варто зазначити, що ефективність функціонування професійних учасників фондового ринку безпосередньо впливає на рівень інвестиційної безпеки країни. Саме вони забезпечують прозорість операцій, формують конкурентне середовище, підвищують довіру до фінансової системи та сприяють стабілізації ринку капіталу, що особливо важливо для розвитку національної економіки в умовах глобалізації.

Фінансові посередники відіграють ключову роль у діяльності організацій, оскільки саме вони створюють умови для ефективного функціонування інвестиційних та емісійних процесів:

– в інвестиційній сфері: забезпечують організаціям доступ до фінансових ресурсів, сприяють диверсифікації інвестиційних ризиків та пропонують інструменти для залучення капіталу, аналізують ринок, формують портфелі цінних паперів, здійснюють управління активами та консультують щодо вибору найефективніших варіантів вкладень;

– у сфері емісійної діяльності: виконують роль організаторів і координаторів процесу емісії; здійснюють підготовку проспекту емісії, маркетинг серед потенційних інвесторів, проводять розміщення цінних паперів та гарантують дотримання нормативних вимог. Такі посередники, як фондові біржі, депозитарні та клірингові установи, забезпечують прозорість операцій, захищають права інвесторів та сприяють підвищенню довіри до емітента;

– у фінансово-господарській діяльності: виступають містком між підприємствами та фінансовим ринком;

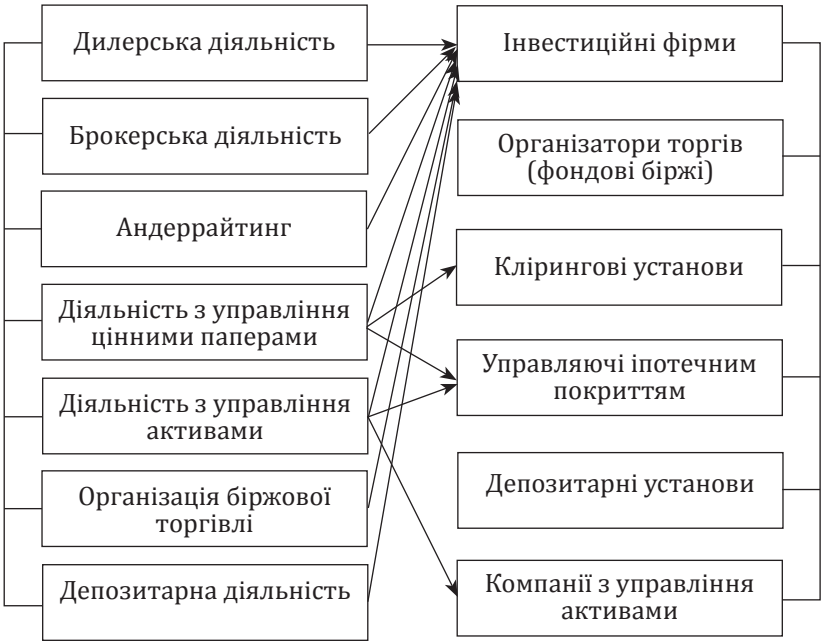


Рис. 5.3. Професійні учасники фондового ринку
та їхня діяльність на фондовому ринку відповідно до регулятора

сприяють залученню довгострокових інвестицій, підтримують ліквідність цінних паперів, а також створюють механізми захисту від фінансових ризиків; у процесі співпраці організації отримують не лише фінансові ресурси, а й комплекс професійних послуг, які забезпечують стабільність, розвиток та конкурентоспроможність у динамічних ринкових умовах.

Роль фінансових посередників у площині їх впливу на інвестиційну безпеку організацій у розрізі кожного суб'єкта охарактеризована в табл. 5.2.

Фінансові посередники відіграють ключову роль у забезпеченні інвестиційної безпеки організації, оскільки виступають ефективною ланкою між інвесторами та емітентами, сприяючи мобілізації фінансових ресурсів і їх раціональному розподілу. Вони допомагають підприємствам залучати капітал, одночасно знижуючи інвестиційні ризики шляхом

Таблиця 5.2

Роль професійних учасників фондового ринку

Професійні учасники ринку	Характеристика щодо інвестиційної безпеки
Інвестиційні фірми	Вони виступають посередниками між інвесторами та емітентами, забезпечуючи доступ підприємств до фінансових ресурсів і сприяючи формуванню оптимальної структури інвестицій. Завдяки аналітиці, консалтингу та організації операцій із цінними паперами інвестиційні фірми знижують ризики для обох сторін і підвищують прозорість інвестиційного процесу.
Організатори торгівлі (фондові біржі)	Створюють регульоване середовище для купівлі-продажу цінних паперів, забезпечуючи їхню ліквідність і справедливе ціноутворення. Вони впливають на інвестиційну безпеку через гарантію прозорості операцій, дотримання стандартів корпоративного управління та мінімізацію маніпуляцій із ринковими цінами.
Клірингові установи	Основна їхня функція – забезпечення розрахунків між учасниками ринку цінних паперів. Вони гарантують завершення угод, що зменшує ризик невиконання зобов'язань, а також сприяють довірі до фінансової системи та стабільності інвестиційного середовища.
Управляючі іпотечним покриттям	Такі суб'єкти забезпечують належне управління іпотечними активами, які виступають забезпеченням для іпотечних цінних паперів. Їхня роль полягає в підтриманні надійності інвестицій у сфері іпотеки та зниженні ризиків, пов'язаних із невиконанням боргових зобов'язань.
Депозитарні установи	Вони відповідають за зберігання та облік прав власності на цінні папери. Депозитарії гарантують юридичну захищеність власників активів і прозорість операцій, що істотно підвищує рівень довіри інвесторів і зміцнює інвестиційну безпеку.
Компанії з управління активами	Ці компанії спеціалізуються на формуванні та управлінні інвестиційними портфелями, застосовуючи сучасні методи аналізу й диверсифікації. Їхня діяльність дозволяє організаціям мінімізувати ризики, підвищити дохідність і забезпечити стале зростання вартості капіталу в довгостроковій перспективі.

контролю, аналізу та диверсифікації. Завдяки посередникам підвищується прозорість інвестиційних процесів, формується довіра до фінансового ринку і забезпечується стабільність інвестиційного середовища. В підсумку їхня діяльність створює передумови для довгострокового розвитку компаній та підвищення інвестиційної привабливості економіки загалом.

Фінансові посередники активно застосовують смарт-технології для управління інвестиційними ризиками. По-перше, системи *Big Data* і штучного інтелекту аналізують величезні масиви ринкової та клієнтської інформації, виявляючи приховані ризикові тенденції й формуючи прогнози щодо можливих змін у вартості активів. По-друге, блокчейн і цифрові платформи забезпечують прозорість та захищеність інвестиційних операцій, мінімізуючи ризики шахрайства і підвищуючи довіру між учасниками ринку.

Питання для самоконтролю

1. У чому полягає сутність поняття інвестиційної безпеки організації та як вона співвідноситься з фінансовою безпекою?
2. Які основні загрози інвестиційній безпеці можуть виникати на рівні підприємства, галузі та держави?
3. Які показники використовуються для оцінювання рівня інвестиційної безпеки підприємства?
4. Яку роль відіграє державна політика та нормативно-правова база у формуванні інвестиційної безпеки бізнесу?
5. Які методи оцінки інвестиційних ризиків застосовуються в управлінні безпекою інвестиційної діяльності (експертні, статистичні, моделювання, сценарні)?
6. Як структура капіталу та джерела фінансування впливають на рівень інвестиційної безпеки організації?
7. У чому полягає значення диверсифікації інвестиційного портфеля для забезпечення стійкості підприємства?
8. Які інструменти смарт-технологій можуть бути використані для моніторингу та прогнозування інвестиційних ризиків?
9. Як результати оцінки інвестиційної безпеки впливають на стратегічні управлінські рішення організації?
10. Якими є основні напрями підвищення інвестиційної безпеки підприємства у післявоєнних умовах розвитку економіки України?

Тестові завдання

1. Що є основною метою управління інвестиційною безпекою організації?

а) Максимізація поточного прибутку за будь-яку ціну;

б) забезпечення стійкості інвестиційної діяльності, мінімізація ризиків і збереження інвестиційного потенціалу підприємства;

в) підвищення рівня оподаткування;

г) формування позитивного іміджу без урахування фінансових результатів.

2. Який з наведених факторів найбільше впливає на рівень інвестиційної безпеки підприємства?

а) Тільки внутрішня структура персоналу;

б) рівень диверсифікації інвестицій, якість управління ризиками та стабільність фінансового середовища;

в) географічне розташування офісу;

г) наявність короткострокових кредитів.

3. Які основні показники використовуються для оцінки інвестиційної безпеки?

а) Лише коефіцієнт ліквідності;

б) рентабельність інвестицій, коефіцієнт покриття, індекс ризику, співвідношення власного і залученого капіталу;

в) рівень заробітної плати працівників;

г) баланс товарних запасів.

4. Який метод найчастіше використовується для оцінювання інвестиційних ризиків?

а) Метод середнього арифметичного;

б) експертні оцінки, сценарний аналіз, метод коефіцієнтів варіації та аналіз чутливості інвестиційних проєктів;

в) лише SWOT-аналіз;

г) порівняння зі середньогалузевими показниками без урахування ризиків.

5. Яке місце посідає державне регулювання в системі інвестиційної безпеки?

а) Має лише консультативний характер;

б) забезпечує формування законодавчих, податкових і фінансових механізмів для захисту інвесторів та стимулювання інвестицій;

в) повністю контролює всі інвестиційні процеси в приватному секторі;

г) не має впливу на інвестиційну безпеку.

6. Яка стратегія є найбільш ефективною для мінімізації інвестиційних ризиків?

а) Ігнорування змін зовнішнього середовища;

б) диверсифікація портфеля інвестицій і використання страхових механізмів для зниження втрат;

в) зосередження інвестицій в одному напрямі;

г) відмова від інноваційних проєктів.

7. Яке значення мають смарт-технології в управлінні інвестиційною безпекою?

а) Вони застосовуються лише у сфері виробництва;

б) надають можливість проводити моніторинг інвестиційних ризиків у реальному часі, прогнозувати зміни ринку та автоматизувати аналітику рішень;

в) використовуються лише для рекламних кампаній;

г) не мають практичного значення у сфері безпеки.

8. Які основні внутрішні загрози можуть знизити рівень інвестиційної безпеки підприємства?

а) Висока кваліфікація персоналу та прозорість управління;

б) корупційні дії, зловживання службовим становищем, неефективне управління інвестиційними проєктами, кадрова нестабільність;

в) зростання обсягів інвестицій;

г) високий рівень корпоративної культури.

9. Як результати оцінки інвестиційної безпеки впливають на управлінські рішення?

а) Не мають практичного значення;

б) використовуються для розроблення антикризових стратегій, оптимізації структури капіталу та підвищення ефективності інвестиційних програм;

в) лише для статистичної звітності;

г) слугують виключно підставою для скорочення персоналу.

10. Які напрями є найважливішими для підвищення інвестиційної безпеки організацій у післявоєнний період?

а) Зменшення державного контролю та скорочення резервів, щоб підвищити рівень безпеки;

б) розвиток державно-приватного партнерства, створення гарантій для інвесторів, цифровізація аналітики й посилення міжнародної співпраці;

в) ізоляція від зовнішніх ринків;

г) зниження рівня прозорості фінансових операцій.

Практичні завдання

Завдання 1.

Підприємство ТОВ «Інвест-Тех» у 2027 році реалізує проєкт модернізації виробничих потужностей. Загальний обсяг інвестицій становить 12 млн грн, з яких 8 млн – власні кошти, 4 млн – залучений банківський кредит під 14% річних. Очікуваний чистий прибуток від проєкту після оподаткування – 2,7 млн грн на рік протягом трьох років. Коефіцієнт дисконтування прийнято на рівні 10%. Підприємство планує реалізувати проєкт у три етапи: модернізацію обладнання, автоматизацію виробничих процесів та впровадження системи енергозбереження. Очікується, що після завершення інвестиційного циклу рівень операційних витрат знизиться на 15%, а продуктивність праці зросте на 20%. Для оцінки ефективності проєкту керівництво підприємства розглядає декілька варіантів фінансування, включаючи можливість реінвестування отриманого прибутку у другий рік реалізації програми.

1. *Розрахуйте чисту теперішню вартість (NPV) проєкту.*
2. *Визначте, чи забезпечує проєкт належний рівень інвестиційної безпеки.*
3. *Поясніть, як зміна вартості позикового капіталу вплине на інвестиційну стійкість підприємства.*

Завдання 2.

Підприємство ПАТ «Альфа Агро», яке займається переробкою сільськогосподарської продукції, розглядає можливість залучення іноземних інвестицій. Під час аналізу виявлено низку проблем:

– значна частка короткострокових позик у структурі капіталу (65%);
– відсутність резервного фонду для покриття ризиків;
– низький рівень прозорості фінансової звітності;
– слабка цифрова система контролю за витратами.

1. *Визначте основні загрози інвестиційній безпеці підприємства.*
2. *Запропонуйте заходи для стабілізації структури капіталу та підвищення довіри інвесторів.*
3. *Обґрунтуйте роль впровадження смарт-аналітичних технологій у зменшенні ризиків для компанії.*

Завдання 3.

Компанія «Гамма Інвест» планує вийти на новий міжнародний ринок у складних економічних умовах. Серед ризиків виділяють: коливання валютних курсів, можливі зміни у податковому

законодавстві, зростання конкуренції та нестачу залучених інвестиційних ресурсів. Для оцінки фінансово-економічного стану компанії було зібрано такі дані:

– Кількість випущених акцій – 5 000 000 шт.
– Поточна біржова ціна однієї акції – 48 грн.
– Чистий прибуток за рік – 96 млн грн.
– Власний капітал – 300 млн грн.
– Залучений капітал (довгострокові кредити та зобов'язання) – 180 млн грн.
– Дивідендні виплати за рік – 24 млн грн.

1. Допоможіть керівництву компанії оцінити ринкову капіталізацію компанії.

2. Визначте інвестиційну привабливість і ризики перед виходом на новий ринок.

ТЕМА 6
СИСТЕМА КОРПОРАТИВНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

6.1. Сутність, функції та принципи корпоративної безпеки
6.2. Рівні корпоративної безпеки організації
6.3. Фактори впливу на корпоративну безпеку організації
6.4. Структура системи корпоративної безпеки організації

Основні поняття і терміни: організація, безпека, фактори впливу, корпоративна безпека, корпоративна стратегія, культура безпеки, персонал, керівники організації, менеджери, кадрова безпека, ділова репутація, рівень корпоративної безпеки, контроль доступу.

6.1. Сутність, функції та принципи корпоративної безпеки

Корпоративна безпека організації є однією з важливих умов стабільного функціонування та стратегічного розвитку підприємства в сучасному конкурентному середовищі. Вона охоплює комплекс заходів, спрямованих на захист матеріальних, фінансових, інформаційних і кадрових ресурсів, а також забезпечення правової та репутаційної захищеності компанії. Система корпоративної безпеки розглядається як інтегрований механізм, що об'єднує організаційні, правові, економічні та технічні інструменти з метою попередження загроз і ризиків внутрішнього й зовнішнього характеру. Її належна побудова та ефективне управління дозволяють підприємству підтримувати конкурентоспроможність, формувати довіру з боку партнерів та інвесторів, а також забезпечувати умови для довготривалої діяльності та розвитку.

Корпоративна безпека розглядається як інтегрована система заходів і механізмів, спрямованих на збереження інтересів підприємства, його матеріальних і нематеріальних активів, ділової репутації та стабільного функціонування в умовах зростаючої кількості ризиків. Це поняття

багатовимірне, оскільки включає захист не лише від фізичних і технічних загроз, але й від інформаційних витоків, економічних коливань, правових спорів та внутрішніх організаційних проблем.

Корпоративна безпека організації – це цілісна система управлінських, правових, інформаційних, економічних і технічних заходів, спрямованих на збереження життєво важливих інтересів підприємства, його активів, персоналу та репутації в умовах динамічного внутрішнього і зовнішнього середовища. Вона передбачає прогнозування й виявлення потенційних загроз, їх попередження та мінімізацію негативних наслідків, що забезпечує стійкість бізнесу, конкурентоспроможність і можливість довгострокового розвитку.

На відміну від класичного підходу до безпеки, корпоративна безпека охоплює ширший спектр сфер: фінансову, інформаційну, кадрову, правову, екологічну, технічну та фізичну, інтегруючи їх у єдину систему. Її головне завдання полягає не лише у відверненні кризових ситуацій, а й у створенні стабільного середовища для досягнення стратегічних цілей компанії та формуванні довіри серед інвесторів, клієнтів і партнерів.

Сутність корпоративної безпеки можна визначити через кілька базових характеристик:

– інтегрований підхід – корпоративна безпека охоплює різноманітні напрями захисту, зокрема фізичний, інформаційний, економічний, правовий та кадровий, створюючи єдину узгоджену систему;

– попереджувальний характер – основний акцент робиться не лише на ліквідації наслідків загроз, а передусім на їх завчасному виявленні та запобіганні виникненню;

– динамічність і безперервність – система корпоративної безпеки повинна постійно вдосконалюватися, оновлюватися та адаптуватися до трансформацій внутрішнього середовища організації та умов зовнішнього ринку.

Корпоративна безпека являє собою попереджувальну систему, яка формує набір заходів і стратегій для організації у разі виникнення ризиків та кризових ситуацій. Вона не обмежується лише реагуванням на проблеми, а створює основу для передбачення загроз та своєчасного формування механізмів їхнього усунення.

Цей інструмент включає безпеку у широкому розумінні, зокрема інтеграцію з бізнес-процесами, забезпечення фізичного захисту, підтримання безперервності бізнесу, відповідність законодавчим і нормативним вимогам. Отож корпоративна безпека є комплексним підходом, що поєднує правові, організаційні, технічні та фінансові аспекти.

Її основна роль полягає у збереженні матеріальних і нематеріальних активів, захисті персоналу, підтриманні стабільності фінансових результатів і запобіганні втратам. Вона також допомагає зміцнити ділову репутацію, підвищити інвестиційну привабливість та створити довіру серед партнерів і клієнтів. У сучасних умовах глобалізації та зростання кіберзагроз корпоративна безпека стає невід'ємною складовою стратегічного управління, оскільки визначає здатність організації не лише виживати, а й успішно розвиватися в конкурентному середовищі.

Основні функції корпоративної безпеки організації наведено на рис. 6.1.

Головне призначення корпоративної безпеки полягає в тому, щоб завчасно ідентифікувати можливі ризики, здійснювати їх глибокий аналіз та впроваджувати заходи для запобігання негативним наслідкам. Це не лише реакція на вже існуючі загрози, а насамперед проактивна система управління, яка дозволяє компанії діяти на випередження. Сфера корпоративної безпеки є багатогранною та охоплює ключові напрями, серед яких:

– ризик-менеджмент та антикризове управління;

– контроль нефінансових ризиків (правових, екологічних, соціальних);

– захист інформації та кадрова безпека;

– система комплаєнсу та дотримання законодавчих вимог;

– виявлення шахрайських дій та заходи щодо їх запобігання;

– фізична і технічна безпека підприємства;

– управління діловою репутацією та захист іміджу компанії.

Відсутність належної системи корпоративної безпеки робить організацію вразливою до широкого спектра загроз –

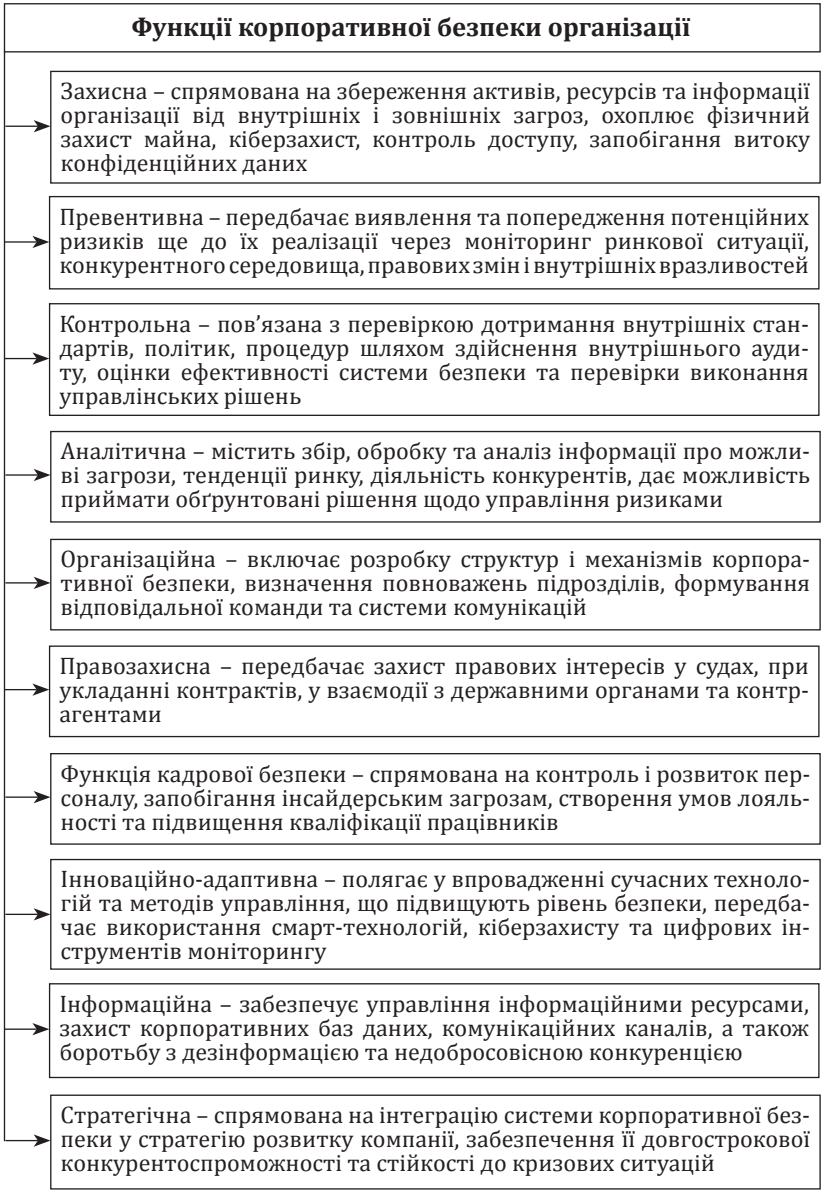


Рис. 6.1. Перелік основних функцій
корпоративної безпеки організації

від фінансових збитків до втрати партнерів і довіри з боку клієнтів. Тому незалежно від галузі чи масштабу бізнесу кожна компанія має формувати власний план безпеки, який відповідає її стратегічним цілям та особливостям діяльності. Це не лише дозволяє знизити ризики, а й створює стійкі передумови для довгострокового розвитку та конкурентоспроможності на ринку.

Принципи забезпечення корпоративної безпеки організації формують основу для побудови ефективної системи захисту та управління ризиками. Вони відображають ключові вимоги до діяльності, що забезпечує стабільність, стійкість і конкурентоспроможність компанії.

По-перше, важливим є принцип комплексності, який передбачає одночасне врахування усіх аспектів безпеки – економічної, інформаційної, кадрової, правової, технічної та фізичної. Такий підхід дає змогу формувати цілісну систему, здатну реагувати на різні види загроз.

Другим виступає принцип проактивності: організація повинна передбачати можливі ризики та розробляти механізми їх запобігання до моменту виникнення проблем. Це дозволяє знизити втрати та уникнути кризових ситуацій. Третім є принцип адаптивності – система корпоративної безпеки повинна постійно оновлюватися відповідно до змін зовнішнього середовища, умов ринку та внутрішніх трансформацій компанії.

Четвертим можна визначити принцип безперервності, адже забезпечення безпеки є процесом, що не має завершеного етапу і потребує постійного моніторингу та контролю. П'ятий – принцип законності та дотримання норм. Усі заходи безпеки мають базуватися на чинному законодавстві, міжнародних стандартах та внутрішніх регламентах організації. Шостим є принцип конфіденційності та захисту інформації, який забезпечує недопущення витоку стратегічних чи персональних даних. Сьомий принцип – економічна доцільність, що означає оптимальне співвідношення витрат на заходи безпеки та потенційних ризиків. Важливим також є принцип відповідальності й персоналізації – кожен рівень управління та кожний працівник повинні мати чітко визначені обов'язки у сфері корпоративної безпеки.

Таким чином, дотримання перелічених принципів дає можливість сформувати стійку систему корпоративної безпеки, яка здатна не лише протидіяти загрозам, а й створювати передумови для довгострокового розвитку компанії.

6.2. Рівні корпоративної безпеки організації

Корпоративна безпека – це багатогранне поняття, яке охоплює різні аспекти діяльності підприємства. Організації визначають рівні корпоративної безпеки для того, щоб об'єктивно оцінити ступінь захищеності своїх ресурсів, активів і бізнес-процесів від потенційних загроз. Це дозволяє не лише виявити слабкі місця та ризикові зони, але й сформувати пріоритети у сфері безпекових заходів, забезпечити ефективний розподіл фінансових та управлінських ресурсів. Чітке визначення рівня безпеки допомагає підприємству своєчасно реагувати на зміни у зовнішньому та внутрішньому середовищі, підвищувати довіру інвесторів і партнерів, а також створює основу для довгострокового розвитку та збереження конкурентоспроможності.

Рівні корпоративної безпеки:

1. Фізичний рівень:

– захист території: охорона периметра, контроль доступу, відеоспостереження;

– захист будівель: пожежна безпека, сигналізація, броньовані двері, сейфи;

– захист обладнання: маркування, інвентаризація, фізичні бар'єри;

– транспортування цінностей: охорона вантажів, броньовані автомобілі.

2. Інформаційний рівень:

– захист інформації: шифрування, обмеження доступу, резервне копіювання;

– захист комп'ютерних систем: антивіруси, фаєрволи, системи виявлення вторгнень;

– захист мереж: шифрування трафіку, VPN, IDS/IPS.

3. Соціальний рівень:

– захист персоналу: перевірка співробітників, навчання безпечних практик, психологічна підтримка;

– захист від промислового шпигунства: контракти про нерозголошення, поліграф;

– захист від соціальної інженерії: навчання співробітників розпізнавати шахрайські схеми.

4. Організаційний рівень:

– політика безпеки: розробка та впровадження чітких правил і процедур;

– управління інцидентами: розробка планів реагування на надзвичайні ситуації;

– аудит безпеки: регулярна перевірка ефективності системи безпеки;

– співпраця з правоохоронними органами: взаємодія з поліцією, СБУ та іншими структурами.

5. Стратегічний рівень:

– стратегічне планування: розробка довгострокових планів забезпечення корпоративної безпеки з урахуванням зовнішніх і внутрішніх ризиків;

– інтеграція безпеки в бізнес-стратегію: поєднання заходів безпеки з ключовими цілями розвитку організації;

– управління репутаційними ризиками: формування позитивного іміджу компанії та попередження кризових ситуацій у медіапросторі;

– інноваційний розвиток: використання сучасних технологій, цифрових інструментів і смарт-систем для підвищення рівня корпоративної безпеки;

– міжнародна співпраця: дотримання глобальних стандартів безпеки та взаємодія з міжнародними партнерами для зміцнення позицій компанії.

6. Інноваційно-технологічний рівень:

– цифрова трансформація: інтеграція сучасних інформаційних систем і смарт-технологій у процеси управління безпекою;

– кіберзахист: захист корпоративних даних і цифрових ресурсів від кібератак, шкідливого програмного забезпечення та несанкціонованого доступу;

– автоматизація моніторингу: застосування систем штучного інтелекту та Big Data для прогнозування загроз і оперативного реагування;

– використання блокчейн-технологій: забезпечення прозорості та захищеності фінансових і контрактних операцій;

– безперервні інновації: постійне оновлення технологічних інструментів у відповідь на динамічні зміни у сфері загроз.

Корпоративна безпека є невід'ємною частиною успішного функціонування будь-якого підприємства. Вона охоплює широкий спектр заходів, спрямованих на захист активів компанії, її репутації та забезпечення безперебійної діяльності. Ефективна система безпеки дозволяє мінімізувати ризики, пов'язані з крадіжками, шахрайством, кібератаками, промисловим шпигунством та іншими загрозами. Завдяки цьому підприємство може зосередитися на своїх основних завданнях і досягати кращих результатів.

Інвестори та партнери щораз більше звертають увагу на рівень безпеки компанії. Наявність надійної системи безпеки свідчить про відповідальне ставлення керівництва до свого бізнесу та підвищує довіру до компанії. Крім того, корпоративна безпека є важливим елементом соціальної відповідальності бізнесу. Забезпечуючи безпечні умови праці для своїх співробітників, компанія демонструє свою турботу про людей і зміцнює корпоративний дух.

Попри те що технології постійно вдосконалюються та змінюються, фундаментальні принципи безпеки залишаються незмінними протягом багатьох століть. Безпека була і залишається одним із головних чинників стабільності не лише у сфері бізнесу, а й у суспільному житті. У сучасному корпоративному середовищі вона розглядається через сім базових складників: фізичний, технічний, людський, інформаційний, комунікаційний, процедурний та управлінський.

Також організації формують типи корпоративної безпеки для більш ефективної їх оцінки крізь призму впливу факторів (рис. 6.2).

Найбільш визначальною серед усіх типів корпоративної безпеки вважається управлінська безпека, оскільки саме вона виконує функцію координатора та інтегратора для інших складових. Саме управлінський рівень формує політику безпеки, розподіляє ресурси, визначає пріоритети та відповідає за організацію взаємодії між усіма підсистемами – від фізичної охорони до інформаційної та кадрової безпеки.

Рис. 6.2. Особливості типів корпоративної безпеки

Її ключова роль полягає в тому, щоб забезпечити цілісність і узгодженість усіх заходів безпеки, перетворити окремі дії та інструменти на єдину систему. Без належної управлінської координації навіть найсучасніші технічні засоби чи ефективні процедури можуть діяти фрагментарно та втрачати результативність. Отже, управлінська безпека

є стратегічним ядром, яке визначає розвиток усієї корпоративної системи безпеки, гарантує її стабільність, безперервність та здатність адаптуватися до змін середовища.

Класифікація корпоративної безпеки за типами дозволяє комплексно оцінити рівень захищеності організації, виявити сильні та слабкі сторони системи безпеки й уникнути «білих плям» у захисті. Поділ на типи створює можливість для розподілу ресурсів та відповідальності між підрозділами, що підвищує ефективність управління ризиками. Крім того, структурованість дає змогу адаптувати систему корпоративної безпеки до змін зовнішнього середовища, швидше реагувати на загрози й формувати превентивні механізми. Зрештою такий підхід не лише підвищує захист активів і репутації організації, а й сприяє її стабільному розвитку та конкурентоспроможності.

6.3. Фактори впливу на корпоративну безпеку організації

Фактори, що впливають на корпоративну безпеку, формують основу для оцінки стійкості організації в умовах постійних змін зовнішнього та внутрішнього середовища. Вони охоплюють широкий спектр елементів – від економічних і правових до технологічних і соціальних, які безпосередньо чи опосередковано визначають рівень захищеності компанії. Розуміння цих факторів дає змогу керівництву не лише вчасно виявляти можливі ризики, але й прогнозувати їхній вплив, розробляючи ефективні превентивні заходи. Тож аналіз факторів є ключовим етапом у побудові системи корпоративної безпеки, що забезпечує стабільність функціонування та довгострокову конкурентоспроможність підприємства.

Зовнішні фактори корпоративної безпеки охоплюють усі ті впливи, які походять з-поза меж організації, але безпосередньо визначають її стабільність, фінансову стійкість і можливість довгострокового розвитку. У сучасних умовах, особливо в Україні, ці фактори посилені воєнними діями та регулярними обстрілами, що створюють додаткові виклики для збереження безпеки підприємств. Нижче подано основні фактори зовнішнього середовища з розгорнутим поясненням їх сутності (рис. 6.3).

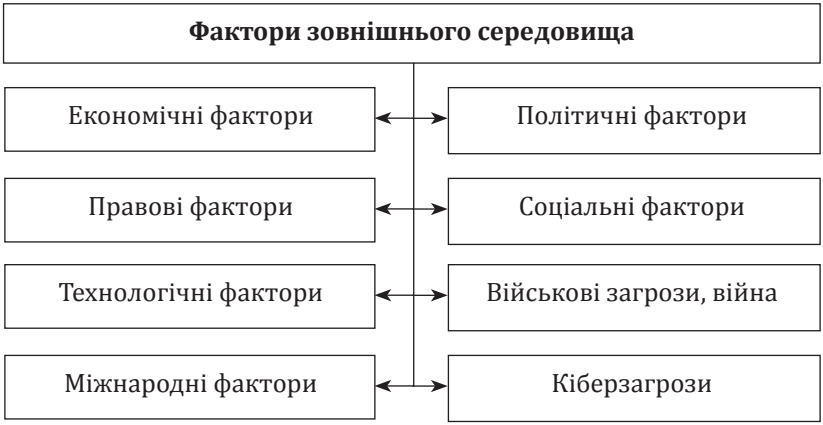


Рис. 6.3. Фактори зовнішнього середовища,
що впливають на корпоративну безпеку організації

Економічні фактори є базовими у формуванні корпоративної безпеки, оскільки вони визначають можливості підприємства щодо залучення інвестицій, формування доходів, доступу до кредитних ресурсів та здатності підтримувати платоспроможність. Інфляційні процеси, девальвація національної валюти, нестабільність банківської системи та зростання вартості енергоресурсів суттєво впливають на функціонування бізнесу. Погіршення макроекономічних показників призводить до зростання ризиків банкрутства, скорочення виробничих програм і втрати конкурентних позицій.

Політичні фактори мають визначальний характер, оскільки саме вони формують рамки регуляторного середовища та правила функціонування підприємств. В Україні сьогодні політичний контекст безпосередньо пов'язаний із війною, міжнародними санкціями, потребою у військових витратах і дипломатичною підтримкою з боку партнерів. Зміни політичного курсу чи дестабілізація влади можуть призвести до посилення невизначеності, додаткових регуляторних бар'єрів або зменшення довіри з боку інвесторів.

Правові фактори визначають ступінь захищеності бізнесу в межах чинного законодавства та регуляторної системи.

Чіткість та ефективність судової системи, прозорість регуляторних процедур, якість захисту прав власності та інтелектуальної власності безпосередньо впливають на корпоративну безпеку. В умовах воєнного стану деякі норми адаптовані чи спрощені, однак водночас існує ризик правової невизначеності, зростання кількості спорів і складності у виконанні контрактів.

Соціальні фактори включають стан суспільства, рівень життя населення, міграційні процеси та демографічні зміни, які впливають на формування трудових ресурсів і поведінку споживачів. Війна спричинила масштабні переміщення населення, зростання безробіття у певних секторах, а також психологічне напруження серед працівників. Усе це безпосередньо позначається на здатності організацій зберігати стабільний кадровий потенціал і підтримувати ефективну корпоративну культуру.

Технологічні фактори відіграють важливу роль у розвитку бізнесу, але водночас формують нові ризики. Використання цифрових технологій, автоматизації та інноваційних рішень дозволяє підвищити ефективність діяльності, проте збільшує залежність від ІТ-інфраструктури. В умовах воєнних загроз, особливо кібератак і спроб зламу інформаційних систем, технологічний чинник стає критичним для збереження безпеки й конкурентоспроможності.

Військові загрози та бойові дії є специфічним, але надзвичайно значущим фактором зовнішнього середовища в Україні. Обстріли енергетичної інфраструктури, руйнування виробничих потужностей, блокування логістичних шляхів і ризики фізичної безпеки працівників істотно впливають на діяльність організацій. Війна підвищує витрати на охорону, страхування, евакуаційні заходи та резервні системи енергозабезпечення. Крім того, саме воєнний фактор визначає масштаби інвестиційної активності та рівень міжнародної підтримки економіки.

Міжнародні фактори також формують середовище корпоративної безпеки, оскільки глобалізація економіки означає залежність від зовнішніх ринків, іноземних партнерів і міжнародних стандартів. Санкції, зміни у зовнішньоекономічних відносинах, дії міжнародних фінансових інституцій

і зміни на світових ринках (енергоносіїв, продовольства, фінансових ресурсів) безпосередньо впливають на стабільність підприємств. Для українських компаній міжнародна співпраця водночас є джерелом підтримки і ризиком залежності від зовнішньої кон'юнктури.

До речі, сучасні науковці виділяють певні види зовнішніх загроз, які значною мірою впливають на корпоративну безпеку:

– кібератаки – це навмисні дії, спрямовані на несанкціоноване втручання у функціонування комп'ютерних систем, мереж або баз даних з метою викрадення інформації, її пошкодження, модифікації чи блокування. Зловмисники можуть застосовувати різні інструменти та методи, серед яких фішинг, вірусні програми, атаки типу «відмова в обслуговуванні» чи злам захисних протоколів (рис. 6.4);

– шпигунство у сфері інтелектуальної власності проявляється у спробах сторонніх осіб або організацій заволодіти конфіденційними розробками, технологіями чи ноу-хау компанії. Витік таких даних може завдати серйозних збитків конкурентоспроможності підприємства та поставити під загрозу його інноваційний потенціал;

– торгівля людьми у сучасному світі також може мати непрямий зв'язок із корпоративною безпекою. Використання примусової праці чи експлуатація вразливих категорій населення може стати інструментом не лише порушення прав людини, але й способом здобуття конфіденційних відомостей чи ресурсів;

– тероризм становить особливу загрозу, оскільки може призвести не лише до фізичних руйнувань інфраструктури, а й до значних психологічних наслідків для персоналу та втрати довіри клієнтів чи партнерів;

– порушення міжнародних торговельних зв'язків може зумовити обмеження доступу до ринків, проблеми з експортом чи імпортом, зростання логістичних витрат, що безпосередньо впливає на економічну стійкість компанії;

– енергетична залежність від імпортованих енергоресурсів створює вразливість у випадку геополітичних криз чи перебоїв із постачанням. Це особливо актуально у період військових дій та обстрілів енергетичної інфраструктури,

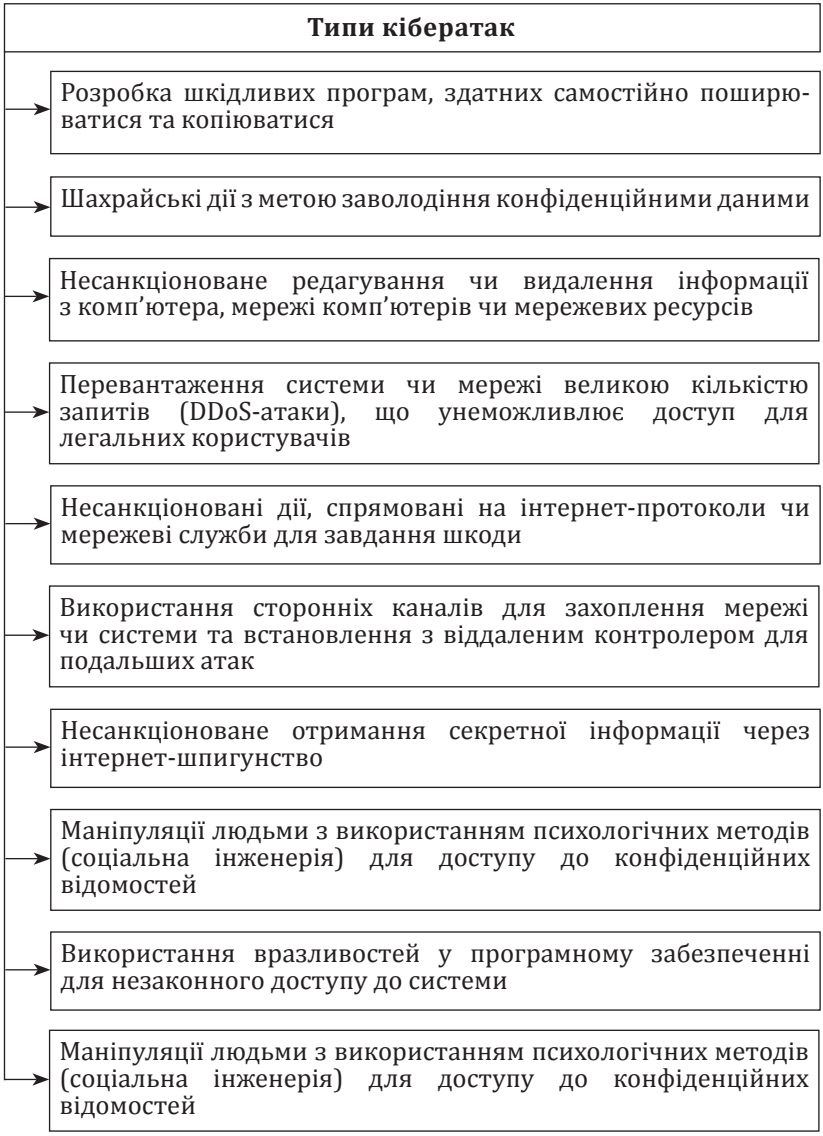


Рис. 6.4. Типи кібератак
у структурі факторів зовнішнього середовища

коли стабільність функціонування підприємств опиняється під реальною загрозою.

Внутрішні чинники корпоративної безпеки визначаються особливостями самої організації, її структури, культури, управління та ресурсного потенціалу. Вони формують основу стійкості компанії до різного роду загроз і визначають, наскільки ефективно вона здатна реагувати на ризики. Зокрема, в умовах війни та регулярних обстрілів саме внутрішні фактори відіграють вирішальну роль у підтримці функціонування підприємства та захисті його працівників. Перелік факторів внутрішнього середовища подано на рис. 6.5.

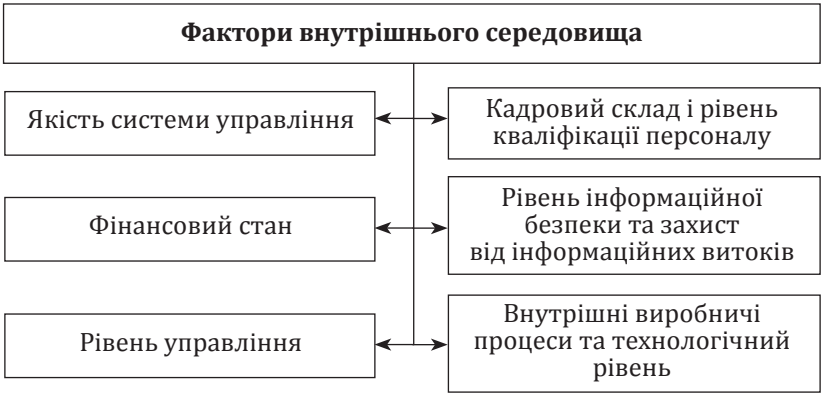


Рис. 6.5. Фактори внутрішнього середовища,
що впливають на корпоративну безпеку організації

Внутрішні фактори корпоративної безпеки формуються всередині самої організації та напряму пов'язані з ефективністю управління її ресурсами, персоналом, системами контролю та корпоративною культурою. Одним із визначальних елементів є якість менеджменту: нераціональні рішення, неузгодженість дій керівництва або відсутність чіткої стратегії можуть посилювати ризики та знижувати здатність компанії протистояти загрозам. В умовах воєнних дій та ракетних обстрілів особливо важливим стає управління кризовими ситуаціями, що включає створення планів безперервності бізнесу, забезпечення резервних каналів комунікації й альтернативних джерел енергії.

Другим ключовим фактором є кадровий склад і рівень кваліфікації персоналу. Недостатня підготовка працівників або їх низька мотивація створюють умови для зловживань, несанкціонованого доступу до інформації чи зниження продуктивності. Під час війни додатковими викликами стають ризики мобілізації працівників, вимушеної міграції або психологічне виснаження через постійні загрози, що прямо впливають на кадрову безпеку. Тому організаціям важливо інвестувати в навчання, психологічну підтримку та формування корпоративної культури, орієнтованої на збереження безпеки.

Фінансовий стан компанії також є критичним фактором. Нестача оборотних коштів, високе боргове навантаження чи відсутність резервів знижують здатність підприємства адаптуватися до непередбачуваних умов. У воєнний час, коли зростають ризики втрати клієнтів, руйнування активів або затримки в розрахунках, фінансова безпека стає головним захисним механізмом. Розвиток систем внутрішнього аудиту, ефективне управління витратами та диверсифікація джерел доходів дають змогу знизити ризики.

Не менш важливим є рівень інформаційної безпеки. Витік конфіденційних даних, злом корпоративних систем чи відсутність належного контролю за доступом до інформаційних ресурсів можуть паралізувати роботу компанії. Під час війни значно зростає кількість кібератак, спрямованих як на інфраструктуру, так і на окремі підприємства, що робить цей фактор ще більш загрозливим. Організації змушені впроваджувати сучасні засоби кіберзахисту, системи резервного копіювання та навчати персонал базових правил кібергігієни.

Внутрішні виробничі процеси і технологічний рівень також впливають на корпоративну безпеку. Низька якість обладнання, відсутність технічного обслуговування або надмірна залежність від застарілих технологій можуть призвести до збоїв у виробництві чи навіть аварій. В умовах обстрілів або перебоїв з електропостачанням підприємства повинні мати альтернативні варіанти забезпечення роботи, включаючи генератори, автономні системи енергозабезпечення та цифрові рішення для дистанційного контролю виробництва.

Ще одним внутрішнім чинником, що визначає рівень корпоративної безпеки, є якість управління організацією. Від професійності та компетентності керівників залежить здатність компанії вчасно реагувати на кризові ситуації, формувати стратегії безпеки та координувати дії різних підрозділів. Неефективне управління може призвести до хаотичних рішень, відсутності контролю за ресурсами, слабкої комунікації між підрозділами та зниження загальної стійкості підприємства. Натомість високий рівень управлінських практик дозволяє створити систему, де ризики прогнозуються заздалегідь, загрози контролюються, а персонал діє узгоджено навіть в умовах війни чи обстрілів. Тобто саме управлінський рівень є інтегруючим фактором, що поєднує фінансові, кадрові, інформаційні та виробничі складові корпоративної безпеки в єдину ефективну систему.

Таким чином, внутрішні фактори корпоративної безпеки відображають ступінь організованості та підготовленості самої компанії до зовнішніх викликів. Ефективне управління персоналом, фінансами, інформаційними ресурсами та технологічними процесами дає можливість не лише знизити рівень загроз, а й забезпечити стійкий розвиток організації навіть у кризових умовах, пов'язаних із війною та постійними обстрілами.

6.4. Структура системи корпоративної безпеки організації

Система корпоративної безпеки організації – це комплекс взаємопов'язаних структур, процесів і механізмів, спрямованих на забезпечення стабільності, безперервності та захищеності діяльності підприємства від внутрішніх і зовнішніх загроз. Вона охоплює як організаційні, так і технічні, правові, кадрові та інформаційні інструменти, які дозволяють формувати надійну модель функціонування компанії, мінімізувати ризики та забезпечувати збереження активів, ресурсів і репутації.

Сутність цієї системи полягає в інтеграції безпекових заходів у загальну стратегію управління організацією, завдяки чому можна не лише реагувати на вже наявні загрози,

але й здійснювати превентивні дії, спрямовані на їх уникнення. Система корпоративної безпеки є динамічною, адже вона повинна адаптуватися до умов економічних, соціальних і політичних змін, а також враховувати специфіку діяльності кожної окремої компанії.

У широкому розумінні система корпоративної безпеки виконує роль «щитка» організації, забезпечуючи узгодженість усіх функціональних підсистем: від фінансів і інвестицій до інформаційних технологій і кадрового менеджменту. Вона створює основу для формування конкурентних переваг, підтримки довгострокової стабільності та збереження позицій компанії в умовах невизначеності й ризиків.

Структура системи корпоративної безпеки організації є багаторівневою і охоплює комплекс взаємопов'язаних елементів, які спільно формують ефективний механізм протидії ризикам і загрозам. У її основі лежать стратегічні, організаційні та операційні компоненти, що поєднують ресурси, суб'єкти управління, принципи й інструменти. Важливим є те, що система не функціонує ізольовано – вона є складовою загальної системи менеджменту підприємства і має тісні зв'язки з усіма бізнес-процесами.

У структурі корпоративної безпеки виділяють кілька ключових елементів. Це насамперед цілі та завдання безпеки, які визначають пріоритетні напрями захисту; суб'єкти управління (керівництво, служба безпеки, окремі структурні підрозділи), що організовують і координують заходи; об'єкти безпеки, до яких відносяться ресурси, активи, інформація, репутація та персонал. До складу системи входять також принципи корпоративної безпеки, що формують базові правила управління; методи та інструменти – аудит, моніторинг, ризик-аналіз, моделювання сценаріїв; ресурсне забезпечення, яке включає фінансові, кадрові, матеріально-технічні та технологічні ресурси. Важливим є й потенціал безпеки, що вміщує накопичений досвід, технології, знання й культуру захисту (рис. 6.6).

Зв'язки між елементами системи корпоративної безпеки будуються за ієрархічним та функціональним принципом. На стратегічному рівні формується політика безпеки, визначаються напрями та довгострокові завдання. На організацій-

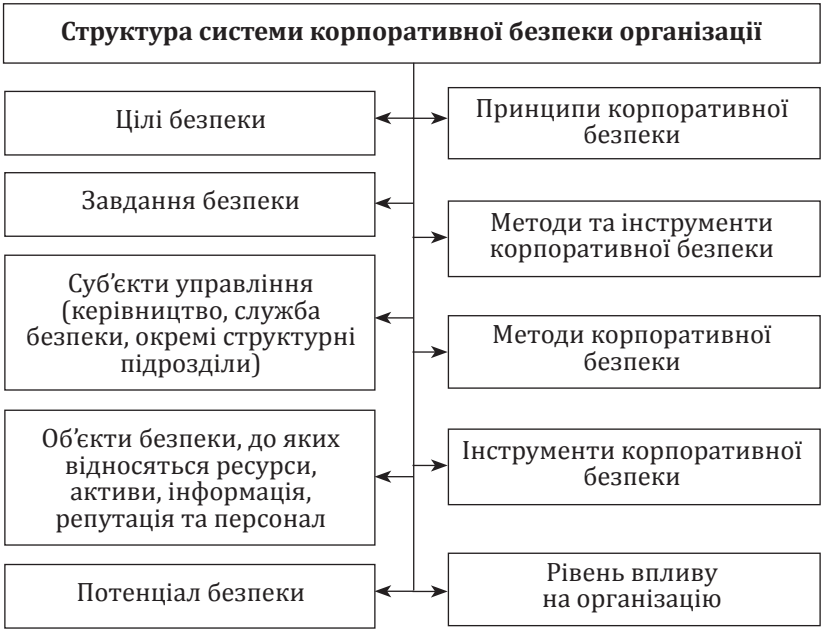


Рис. 6.6. Структурні компоненти системи корпоративної безпеки

ному – розробляється структура системи, розподіляються функції між підрозділами, налагоджуються комунікаційні канали. На операційному рівні здійснюється безпосереднє виконання заходів: контроль доступу, захист інформації, моніторинг ризиків, реагування на інциденти. Взаємодія цих компонентів створює комплексну, інтегровану систему, яка дає змогу організації забезпечувати свою стійкість, адаптивність і конкурентоспроможність у динамічному середовищі.

У структурі корпоративної безпеки одними з найважливіших елементів виступають цілі безпеки, оскільки саме вони визначають напрями і масштаби діяльності у сфері захисту організації. Цілі корпоративної безпеки формуються на основі стратегічних завдань компанії, враховують особливості внутрішнього середовища, характер загроз і рівень ризиків, а також зовнішні фактори, зокрема політичну,

економічну та соціальну ситуацію. Вони мають відображати прагнення організації забезпечити стабільність функціонування, захистити ресурси, зберегти репутацію та підвищити конкурентоспроможність.

Сутність цілей корпоративної безпеки полягає в їх багаторівневості та комплексності:

– на стратегічному рівні вони зосереджені на гарантуванні стійкості і довгострокового розвитку бізнесу;

– на тактичному рівні – на організації процесів управління ризиками;

– на операційному рівні – на впровадженні конкретних заходів і процедур захисту.

Кожна мета у сфері корпоративної безпеки повинна бути конкретною, вимірюваною та орієнтованою на досягнення практичних результатів. Таким чином, цілі безпеки не лише задають напрям діяльності всієї системи, а й допомагають координувати роботу її окремих елементів, забезпечуючи узгодженість дій і досягнення загального результату – стабільного та безпечного функціонування організації.

Завдання системи корпоративної безпеки є практичним інструментом для досягнення стратегічних і тактичних цілей організації у сфері захисту її інтересів, активів і персоналу. Вони спрямовані на створення стійкої системи протидії внутрішнім та зовнішнім загрозам, підтримання стабільності бізнес-процесів та забезпечення довгострокового розвитку компанії. Правильно сформовані завдання дозволяють організації не лише знижувати ризики, а й підвищувати конкурентоспроможність, зміцнювати репутацію та створювати умови для сталого функціонування в умовах зростаючої невизначеності середовища.

Основні завдання системи корпоративної безпеки для ефективного управління включають певні складові (табл. 6.1).

Принципи корпоративної безпеки задають «правила гри» для всієї системи: вони визначають, як планувати захист, на що спрямовувати ресурси, як координувати підрозділи та оцінювати результат. Кожен принцип має відображатися у внутрішніх політиках, процедурах і стандартах, бути зрозумілим персоналу й вимірюваним у практиці.

Таблиця 6.1

Завдання корпоративної безпеки та їхня роль

Завдання	Основна роль
Організація комплексного захисту інформаційних, фінансових, матеріальних і кадрових ресурсів	Дозволяє забезпечити надійне функціонування усіх бізнес-процесів і знизити ймовірність виникнення критичних інцидентів, що загрожують життєдіяльності компанії.
Виявлення, оцінка та прогнозування можливих загроз і ризиків	Дає змогу заздалегідь виявляти слабкі місця в системі управління та формувати превентивні заходи, спрямовані на збереження стабільності підприємства.
Розробка та впровадження заходів щодо запобігання кризовим ситуаціям і мінімізації їх наслідків	Допомагає компанії бути готовою до непередбачуваних подій, скорочуючи час на реагування та зменшуючи збитки.
Формування корпоративної політики безпеки, що інтегрується у загальну стратегію розвитку організації	Сприяє створенню єдиної концепції безпеки, яка враховує як стратегічні цілі бізнесу, так і практичні аспекти їх реалізації.
Створення механізмів моніторингу та контролю для оцінки ефективності прийнятих рішень	Забезпечує регулярну перевірку результативності системи безпеки та своєчасне коригування її елементів.
Підтримка правової захищеності діяльності компанії та забезпечення дотримання вимог законодавства	Гарантує уникнення штрафів, юридичних претензій та захист від недобросовісних дій контрагентів.
Розвиток культури безпеки серед персоналу, яка сприяє підвищенню відповідальності та обізнаності співробітників	Формує усвідомлене ставлення працівників до питань безпеки, знижує ризики людського фактору та порушень дисципліни.
Організація взаємодії з державними структурами, партнерами та громадськістю з метою зміцнення системи захисту	Підвищує довіру до компанії та забезпечує зовнішню підтримку у разі кризових подій.
Забезпечення швидкого відновлення діяльності після надзвичайних подій чи атак	Мінімізує наслідки кризових ситуацій та дає змогу компанії зберегти свою ринкову позицію, конкурентоспроможність і стабільність у довгостроковій перспективі.

Сукупно вони забезпечують цілісність і узгодженість дій на стратегічному, тактичному й операційному рівнях, дозволяють збалансувати вартість заходів і очікуваний ефект, підтримують відповідність законодавству та вимогам партнерів, а також формують культуру безпеки в організації.

Основні принципи корпоративної безпеки:

– комплексність (охоплення всіх напрямів – інформаційного, фінансового, кадрового, правового, фізичного, технічного);

– системність і інтегрованість зі загальним менеджментом (вбудування безпеки в бізнес-процеси та стратегію);

– проактивність і превентивність (орієнтація на попередження загроз, а не лише реагування);

– ризик-орієнтований підхід (пріоритизація заходів за рівнем ризику та впливу);

– безперервність і циклічність (постійний моніторинг, аудит, поліпшення);

– адаптивність (швидке оновлення політик і засобів з урахуванням змін середовища);

– законність і комплаєнс (дотримання законів, стандартів, договорів і етичних норм);

– конфіденційність, цілісність і доступність інформації (CIA-тріада як ядро захисту даних);

– персональна відповідальність і розподіл повноважень (чіткі ролі, запобігання конфлікту інтересів);

– економічна доцільність і пропорційність (оптимальне співвідношення витрат і вигод; відсутність надмірних бар'єрів);

– єдиний центр координації (керованість і узгодження дій усіх підсистем);

– сумісність і стандартизація (єдині вимоги до процесів, техніки та документів);

– прозорість і трасованість (фіксація подій, можливість розслідувань і навчання на інцидентах);

– людяність та етичність (повага до прав працівників і партнерів, недопущення дискримінації);

– безпека-*by-design* і *privacy-by-design* (вбудовування вимог безпеки та приватності на етапі розробки продуктів і процесів);

– стійкість і відновлюваність (планування безперервності бізнесу, резервування, готовність до криз).

Методи – це загальні способи організації та реалізації заходів захисту, які визначають підхід до управління ризиками та формування безпекового середовища. До них належать:

– організаційно-управлінські методи – розробка політик безпеки, створення спеціальних підрозділів, розподіл відповідальності, впровадження стандартів та внутрішніх регламентів;

– правові методи – використання норм національного та міжнародного законодавства, укладання контрактів, договорів конфіденційності, угод із партнерами та постачальниками;

– економічні методи – планування бюджетів на безпекові заходи, використання фінансових стимулів та санкцій, економічна мотивація персоналу до дотримання правил;

– технічні методи – застосування сучасних технологій моніторингу, контролю доступу, інформаційних систем захисту та кібербезпеки;

– психологічні та кадрові методи – формування культури безпеки, підвищення обізнаності персоналу, спеціальні тренінги та інструктажі, управління людським фактором.

– аналітичні методи – оцінка ризиків, проведення аудитів, SWOT- та PEST-аналіз, прогнозування потенційних загроз.

Інструменти – це конкретні засоби, програми та практики, що використовуються для реалізації методів на практиці. Серед них можна виділити:

– системи відеоспостереження та контролю доступу (електронні перепустки, біометричні сканери);

– програмне забезпечення з кіберзахисту (антивірусні системи, міжмережеві екрани, системи виявлення вторгнень);

– системи інформаційного моніторингу (аналіз корпоративних даних, виявлення аномальної активності, системи прогнозування загроз);

– юридичні інструменти (договори про конфіденційність, антикорупційні політики, положення про комерційну таємницю);

– фінансові механізми (страхування ризиків, резервні фонди, механізми компенсації);

– кадрові інструменти (перевірка персоналу при прийомі на роботу, поліграф-тестування, створення служб корпоративної етики);

– аудиторські та контрольні інструменти (внутрішні та зовнішні аудити, стрес-тестування систем, перевірка партнерів);

– комунікаційні інструменти (канали інформування персоналу, кризові комунікації, PR-стратегії захисту репутації).

Питання для самоконтролю

1. У чому полягає сутність корпоративної безпеки організації та які її ключові функції?
2. Які внутрішні та зовнішні фактори найбільше впливають на рівень корпоративної безпеки сучасних підприємств?
3. Яку роль відіграє управлінський компонент у формуванні та підтриманні системи корпоративної безпеки?
4. Як війна, геополітичні конфлікти та терористичні загрози змінюють підхід до корпоративної безпеки?
5. У чому полягає відмінність між принципами корпоративної безпеки та її методами?
6. Які завдання системи корпоративної безпеки вважаються стратегічними, а які – тактичними?
7. Як забезпечується взаємозв'язок корпоративної безпеки з інформаційною та кадровою безпекою?
8. Які рівні корпоративної безпеки можна виділити і чим вони відрізняються один від одного?
9. Чому важливо формувати корпоративну культуру безпеки серед персоналу і які інструменти для цього застосовуються?
10. Як зовнішня взаємодія з державними структурами, партнерами та громадськістю впливає на стійкість системи корпоративної безпеки?

Тестові завдання

1. Що є основною метою системи корпоративної безпеки?

а) Максимізація прибутку компанії;

б) захист інтересів, активів і репутації організації від загроз;

в) провадження новітніх технологій у виробництво та систему реалізації товарів на ринку;

г) розширення присутності на міжнародних ринках.

2. Який з наведених факторів належить до зовнішніх загроз корпоративній безпеці?

а) Низький рівень корпоративної культури;

б) недостатній контроль за фінансами;

в) геополітичні конфлікти та воєнні дії;

г) недосконала організаційна структура.

3. До внутрішніх чинників, що впливають на корпоративну безпеку, належать:

а) рівень управління та організаційна структура;

б) тероризм і кібератаки, які впливають на рівень рентабельності підприємства;

в) політична нестабільність;

г) валютні коливання та знецінення національної валюти.

4. Яку роль відіграє управлінський рівень корпоративної безпеки?

а) Забезпечує тільки фізичний захист приміщень;

б) координує всі інші напрями безпеки та інтегрує їх у єдину систему захисту підприємства;

в) відповідає лише за фінансовий моніторинг;

г) він зосереджується виключно на взаємодії з партнерами.

5. Який із принципів корпоративної безпеки означає постійне вдосконалення та адаптацію системи до нових умов?

а) Комплексність;

б) безперервність;

в) проективність;

г) ієрархічність.

6. Що входить до складу завдань системи корпоративної безпеки?

а) Лише захист інформації від несанкціонованого доступу зі зовнішніх джерел;

б) тільки запобігання фізичним загрозам;

в) організація комплексного захисту ресурсів, моніторинг загроз, формування політики безпеки;

г) виключно контроль фінансових потоків.

7. Чим відрізняються методи корпоративної безпеки від інструментів?

а) Методи – це конкретні засоби, а інструменти – загальні підходи;

б) методи – це підходи та способи дій, а інструменти – конкретні технічні й організаційні засоби їх реалізації;

в) методи та інструменти є тотожними поняттями;

г) методи застосовуються лише у фінансовій безпеці, а інструменти – в інформаційній.

8. Що є прикладом інструменту корпоративної безпеки?

а) SWOT-аналіз ризиків;

б) система відеоспостереження;

в) розробка корпоративної стратегії;

г) формування культури безпеки.

9. Важливо визначати рівні корпоративної безпеки в організації:

а) для оптимізації оподаткування;

б) щоб краще розподіляти ресурси, оцінювати загрози та ефективність заходів захисту;

в) щоб уникнути зовнішніх перевірок;

г) для підвищення інвестиційної привабливості лише на фінансовому рівні.

10. Що станеться з організацією в разі відсутності належної системи корпоративної безпеки?

а) Вона зможе швидше розвиватися завдяки економії ресурсів;

б) вона залишиться стабільною, але вразливою до ринкових змін;

в) вона буде схильною до ризиків, може зазнати фінансових і репутаційних втрат;

г) вона автоматично отримає підтримку від держави.

Практичні завдання

Завдання 1.

Підприємство «Альфа» займається виробництвом і експортом електронного обладнання. Впродовж останніх років воно активно інвестувало в цифровізацію бізнес-процесів та перевело більшість операцій в онлайн-режим. У 2024 році компанія зіткнулася зі серйозною кіберзагрозою: хакери отримали доступ до фінансової бази, викрали частину комерційної інформації та спробували заблокувати платіжні операції. В результаті діяльність підприємства була зупинена на 5 днів, що призвело до прямих збитків у розмірі 2,5 млн грн та репутаційних втрат.

1. Визначте, які елементи системи корпоративної безпеки виявилися найбільш уразливими.

2. Розробіть пропозиції щодо посилення інформаційної та технічної безпеки компанії.

3. Оцініть потенційні фінансові наслідки для підприємства, якщо подібні атаки повторюватимуться щороку.

Завдання 2.

Компанія «Бета-Логістик» спеціалізується на перевезеннях у східних областях України. У зв'язку з воєнними діями та постійними обстрілами регіонів підприємство несе значні ризики пошкодження транспорту, складів і товарних запасів. Лише за останні пів року було втрачено майна на суму понад 15 млн грн, а страхові компанії відмовляються компенсувати збитки через підвищений рівень ризику. Персонал компанії працює у постійній психологічній напрузі, що призводить до зниження продуктивності.

1. Визначте основні внутрішні та зовнішні фактори, що впливають на корпоративну безпеку компанії.

2. Запропонуйте комплекс заходів з організації фізичної та кадрової безпеки.

3. Складіть приблизний розрахунок резервного фонду, який компанія повинна формувати для покриття збитків (виходячи зі середньорічних втрат).

Завдання 3.

Організація «Гамма-Інвест» є одним із найбільших учасників фондового ринку України. Після публікації в медіа компрометуючої інформації про можливі фінансові махінації з боку топменеджменту ринкова капіталізація компанії впала на 18% протягом тижня. Незважаючи на те, що факти не підтвердилися, компанія втратила довіру інвесторів і зіткнулася з відтоком клієнтів. Рівень акцій, які ще місяць тому оцінювалися у 120 грн за штуку, знизився до 98 грн.

1. Визначте, які напрями корпоративної безпеки були проігноровані або недостатньо ефективні.

2. Розробіть план антикризових заходів, спрямованих на відновлення довіри інвесторів.

3. Оцініть нову ринкову капіталізацію компанії, якщо до кризи вона становила 2,4 млрд грн.

ТЕМА 7
МЕНЕДЖМЕНТ КАДРОВОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

7.1. Сутність кадрової безпеки організації та її аспекти
7.2. Складові управління кадровою безпекою організації
7.3. Напрями збереження кадрової безпеки: вітчизняний та світовий досвід

Основні поняття і терміни: безпека, організація, кадрова безпека, працівники, кадрові ризики, персонал, трудовий потенціал, трудовий колектив, персональні ризики, корпоративна культура, співробітники, індивідуальні ризики, людські ресурси організації.

7.1. Сутність кадрової безпеки організації та її аспекти

Кадрова безпека організації – це складова загальної системи корпоративної безпеки, яка включає захист персоналу, кадрового потенціалу та процесів управління людськими ресурсами від внутрішніх і зовнішніх загроз. У сучасних умовах кадрова безпека набуває особливого значення, адже саме люди формують основу успіху будь-якої компанії. Вона включає не лише відбір і контроль персоналу, а й запобігання витоку конфіденційної інформації, зниження ризиків недобросовісної поведінки працівників, забезпечення стабільності трудового колективу та збереження інтелектуального капіталу.

Важливість кадрової безпеки полягає в тому, що вона безпосередньо впливає на ефективність роботи підприємства, його конкурентоспроможність та інвестиційну привабливість. В умовах воєнних загроз, економічної нестабільності та високої мобільності робочої сили, захист трудового потенціалу стає одним із ключових завдань менеджменту. Системний підхід до кадрової безпеки дозволяє організації не лише мінімізувати ризики, пов’язані з персоналом, але й створити

сприятливі умови для розвитку команди, формування корпоративної культури довіри та забезпечення стабільного розвитку у довгостроковій перспективі.

Кадрова безпека – це систематичний процес, спрямований на зменшення або нейтралізацію впливу персональних ризиків та загроз на економічний стан організації через управління людськими ресурсами.

Кадрова безпека включає набір заходів і процедур, які організація застосовує для оцінки доброчесності, надійності та професійності співробітників, підрядників та інших осіб. Вона передбачає відбір, перевірки та моніторинг персоналу з метою мінімізації внутрішніх загроз, шахрайства чи несанкціонованого доступу до конфіденційної інформації.

Управлінський підхід, представлений у наукових дослідженнях, розглядає кадрову безпеку як систему організаційно-управлінських заходів, спрямованих на ефективне формування, розвиток та використання кадрового потенціалу підприємства з метою збереження його економічної стійкості, конкурентоспроможності та результативності господарської діяльності. Така інтерпретація акцентує увагу на ролі управління персоналом у забезпеченні захищеності організації від загроз, що виникають як зісередини, так і під впливом зовнішнього середовища.

Кадрова безпека організації розглядається як комплекс взаємопов'язаних складових, кожна з яких формує цілісну систему захисту працівників і забезпечує стабільність функціонування підприємства. По-перше, це безпека здоров'я, яка пов'язана з формуванням безпечних умов праці, мінімізацією виробничого травматизму та профілактикою професійних захворювань. Вона охоплює всі заходи, спрямовані на охорону життя та здоров'я співробітників під час виконання ними службових обов'язків. Другою складовою виступає фізична безпека, що передбачає захист персоналу від можливих зовнішніх небезпек, пов'язаних із трудовою діяльністю, а також забезпечення безпеки членів їхніх родин у разі загрозливих ситуацій.

Важливим компонентом є фінансова безпека працівників, яка гарантує належний рівень матеріального забезпечення відповідно до кваліфікації та результатів праці.

Вона формує впевненість у стабільності робочого місця та регулярності оплати праці. Інтелектуальна безпека пов'язана із забезпеченням доступу до сучасних знань, професійного розвитку, впровадженням інновацій та створенням умов для прояву ініціативи. Кар'єрна безпека передбачає можливість для співробітників розвиватися у професійному та посадовому вимірі, просуватися по службі відповідно до своїх компетенцій та отримувати можливості для самореалізації.

До адміністративно незалежної безпеки належать заходи, що забезпечують об'єктивне оцінювання працівників і виключають ризик призначення на керівні посади некомпетентних осіб через родинні чи інші суб'єктивні зв'язки. Технологічна безпека охоплює впровадження сучасного обладнання та новітніх технологій, що створюють комфортні та продуктивні умови праці. Пенсійно-страхова безпека включає соціальний захист працівників, страхування та гарантії якісного медичного обслуговування.

Окремо слід виділити патріотичну безпеку, яка виявляється у формуванні позитивного психологічного клімату та відданості співробітників цілям компанії. Антиконфліктна безпека зосереджується на створенні атмосфери співпраці та злагоди в колективі. Психолого-комунікаційна безпека сприяє гармонійному спілкуванню між керівництвом і підлеглими, формує довіру та взаємну повагу. Нарешті, естетична безпека пов'язана із розвитком особистісного іміджу працівників, організацією освітніх та культурних заходів, які мотивують персонал та підвищують задоволеність роботою.

Цей підхід позиціонує кадрову безпеку не лише як захисний механізм, а й як важливу основу розвитку персоналу, що безпосередньо впливає на стійкість і конкурентоспроможність організації.

Основними цілями кадрової безпеки виступають:

– забезпечення стабільності функціонування організації та своєчасне реагування на ризики;

– захист законних прав та інтересів підприємства від протиправних дій працівників або третіх осіб;

– попередження шахрайства, розкрадань фінансових і матеріально-технічних ресурсів, збереження майна, а також захист від витоку чи спотворення службової інформації;

– підтримка безперебійності виробничих процесів і належної роботи засобів інформатизації;

– підвищення рівня лояльності персоналу та створення сприятливого психологічного клімату;

– забезпечення професійного зростання та розвитку компетенцій співробітників;

– формування механізмів профілактики та вирішення трудових конфліктів;

– запровадження системи оцінки й моніторингу кадрових ризиків;

– створення умов для ефективної взаємодії персоналу з керівництвом і партнерами.

Таким чином, кадрова безпека розглядається не лише як захисний механізм, а й як важливий елемент управління розвитком підприємства. У науковій літературі виділяють різні підходи до її трактування – цільовий, процесний, функціональний, структурний, ресурсний та інші (табл. 7.1). Це свідчить про багатогранність поняття і необхідність його комплексного вивчення в контексті загальної системи корпоративної безпеки.

Таблиця 7.1

Підходи до трактування кадрової безпеки організації

Підхід	Характеристика
1	*2*
Цільовий підхід	Розглядає кадрову безпеку як стан захищеності підприємства від потенційних і реальних небезпек, що виникають у процесі його діяльності. Основна увага приділяється тому, що саме безпека персоналу та кадрового потенціалу є ключовою умовою досягнення стратегічних цілей організації. У цьому випадку кадрова безпека постає як результат і як бажаний стан, до якого прагне компанія, формуючи свої механізми управління та політику розвитку.
Процесний підхід	Акцентує на тому, що кадрова безпека – це динамічний процес, який охоплює безперервну роботу із запобігання негативним впливам і загрозам, що можуть порушити функціонування організації. Такий підхід розглядає кадрову безпеку не лише як статичний стан, а як сукупність дій і управлінських процедур, спрямованих на збереження стабільності колективу, підвищення його ефективності та захист від деструктивних чинників.

Завершення табл. 7.1

1	*2*
Системний підхід	Трактує кадрову безпеку як невід'ємну частину загальної системи економічної безпеки підприємства. Тут вона виступає структурним елементом, який пов'язаний із іншими видами безпеки – фінансовою, інформаційною, правовою, організаційною. Такий підхід підкреслює взаємозалежність усіх складових безпеки та важливість інтегрованого механізму, що забезпечує захист організації від внутрішніх і зовнішніх загроз.
Функціональний підхід	Визначає кадрову безпеку як специфічний вид діяльності, який охоплює реалізацію конкретних заходів і програм із протидії загрозам. У цьому випадку кадрова безпека розглядається крізь призму виконання практичних функцій – від виявлення та моніторингу ризиків до створення системи кадрового контролю та підвищення рівня корпоративної культури. Такий підхід орієнтує на результативність і реальні дії, які мають забезпечити стабільність персоналу.
Компаративний підхід	Спрямований на дослідження значення кадрової безпеки в різних умовах економічної трансформації. Він дозволяє порівнювати стан кадрової захищеності підприємства в різні історичні періоди або в умовах різних соціально-економічних систем, роблячи акцент на тому, що вимоги до кадрової безпеки постійно змінюються відповідно до викликів часу. Такий підхід підкреслює еволюційний характер поняття та необхідність адаптації до глобальних і національних змін.
Управлінський підхід	Розглядає кадрову безпеку як сукупність цілеспрямованих управлінських заходів, що стосуються ефективного формування, розвитку й використання кадрового потенціалу. Він робить акцент на управлінських технологіях, інструментах і процедурах, які забезпечують стійкість персоналу та мінімізують ризики, пов'язані з людським фактором. Цей підхід тісно пов'язаний із розвитком HR-менеджменту та стратегічного управління персоналом.
Ресурсний підхід	Інтерпретує кадрову безпеку через призму забезпечення підприємства управлінськими та виробничими кадрами, акцентуючи увагу на їх кількісних та якісних характеристиках. Тут ключовим стає питання, наскільки персонал відповідає вимогам організації, чи достатньо він компетентний і мотивований, щоб гарантувати захист інтересів компанії. Такий підхід дозволяє оцінити кадрову безпеку як важливий ресурс, без якого неможливе стале функціонування організації.

Основна роль у забезпеченні кадрової безпеки організації належить саме її суб'єктам, оскільки вони безпосередньо визначають якість реалізації кадрової політики та здатність компанії протидіяти загрозам, пов'язаним із людським фактором. Керівництво підприємства формує стратегічні пріоритети у сфері управління персоналом, встановлює правила та стандарти кадрової роботи, а також приймає ключові рішення щодо відбору, розвитку й утримання працівників. Від злагодженої роботи управлінських структур залежить рівень професійної підготовки колективу, його мотивація та ефективність діяльності.

Служби безпеки, кадрові підрозділи та юридичні відділи реалізують управлінські рішення на практиці, здійснюючи моніторинг ризиків, пов'язаних із персоналом. Вони виявляють і запобігають загрозам, таким як шахрайство, витік інформації, нелояльність чи недобросовісність співробітників. Саме ці суб'єкти створюють систему контролю й превентивних заходів, завдяки яким організація може функціонувати стабільно навіть в умовах зовнішніх і внутрішніх викликів.

Важливу роль відіграють і самі працівники, адже їхня дисципліна, лояльність та відповідальність формують основу кадрової стабільності. Співробітники виступають не лише об'єктами, а й активними учасниками системи безпеки, оскільки від їхніх дій залежить рівень захищеності компанії від внутрішніх загроз (рис. 7.1). Отже, суб'єкти кадрової безпеки створюють комплексний механізм, що поєднує управління, контроль, правовий захист і розвиток персоналу, роблячи їх ключовим елементом у системі забезпечення безпеки підприємства.

Об'єкти кадрової безпеки – це ті елементи людського та пов'язаного з ним ресурсного простору організації, на які спрямовані заходи зі захисту, превенції та управління ризиками, що пов'язані з персоналом. По суті об'єкти – це все те, що може бути уразливим через людський фактор або в чому проявляються наслідки порушень кадрової дисципліни: люди, їхні знання та компетенції, інформація про них, процеси управління, матеріальні та технічні засоби, а також зовнішні інституційні зв'язки. Ідентифікація і класифікація таких об'єктів дає змогу цілеспрямовано будувати політику

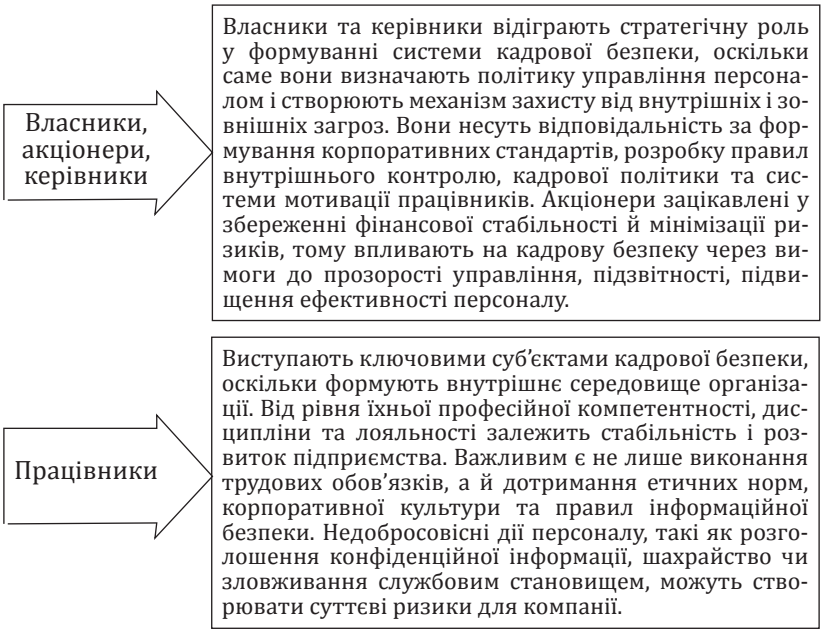


Рис. 7.1. Роль суб'єктів у забезпеченні кадрової безпеки організації

підбору, контролю, навчання, мотивації та правового захисту персоналу, а також мінімізувати ризики витоку інформації, шахрайства, внутрішньої недисциплінованості чи інших загроз.

До переліку **об'єктів кадрової безпеки** організації відносять:

1. Людські ресурси:

– загальний штат працівників – всі співробітники організації як сукупність економічного ресурсу;

– ключовий персонал (топменеджери, фахівці з критичними компетенціями) – особлива зона захисту через вплив на стратегічні рішення;

– контрагенти і підрядники, що працюють на території або з даними компанії, – джерело додаткового ризику;

– соціально незахищені чи вразливі категорії працівників (тимчасові, сезонні, дистанційні) – потребують окремих заходів захисту і мотивації.

2. Кадрові процеси та практики:

– підбір і найм (рекрутинг, попередні перевірки) – об'єкт через ризики помилкового найму або інфільтрації;

– адаптація і навчання – процеси, що впливають на компетентність і безпеку поведінки;

– оцінка та атестація персоналу – визначення відповідності вимогам безпеки;

– мотивація і винагорода (політика винагород) – інструмент попередження корупції та демотивації;

– управління кар'єрою і планування наступництва – об'єкт, що забезпечує безперервність діяльності;

– внутрішні переміщення та доступи (передавання прав, делегування).

3. Інформаційні об'єкти, пов'язані з персоналом:

– особисті дані співробітників (паспортні дані, ІПН, контакти) – потребують захисту від витоку;

– рекрутингові й кадрові записи (інтерв'ю, мотиваційні листи, поліграф/перевірки) – чутливі документи;

– результати оцінювання та атестації, файли з показниками ефективності;

– доступи та облікові записи (логіни, паролі, токени, біометрія) – технічний об'єкт безпеки;

– корпоративна електронна пошта, внутрішні чати й документи – джерела конфіденційної інформації.

4. Інтелектуальний капітал і знання:

– ноу-хау та професійні знання співробітників;

– бази даних, клієнтські списки, комерційна таємниця;

– документація про технологічні процеси і секретні алгоритми.

5. Матеріально-технічні об'єкти, пов'язані з персоналом:

– офіси, виробничі приміщення і складські площі;

– технічні засоби доступу (турнікети, контролери), робочі місця;

– обладнання, носії інформації, мобільні пристрої співробітників;

– сервіси та інфраструктура для віддаленої роботи (*VPN*, корпоративні хмари).

6. Процедурні та нормативні об'єкти:

– внутрішні політики, інструкції, положення про конфіденційність;

– трудові договори, угоди про нерозголошення (*NDA*), дисциплінарні правила;

– стандарти комплаєнсу та етичні кодекси.

7. Організаційні зв'язки і зовнішні відносини:

– взаємини з постачальниками, партнерами і клієнтами, що пов'язані через персонал;

– зовнішні служби (аудитори, консультаційні фірми), які мають доступ до даних;

– публічний імідж та репутація компанії як об'єкт, уразливий через дії персоналу.

8. Охорона здоров'я та безпека праці:

– фізичний і психологічний стан працівників;

– програми підтримки, евакуації, медичні ресурси – важливі для збереження працездатності в кризах.

9. Соціальні та культурні об'єкти:

– корпоративна культура, цінності й корпоративні ритуали;

– взаємини в колективі, рівень довіри і моральний клімат.

10. Системи контролю і моніторингу персоналу:

– системи внутрішнього аудиту, моніторингу доступу і логів;

– аналітичні платформи для оцінки ризиків, системи інцидент-менеджменту.

Кадрова безпека є критично важливою складовою загальної системи безпеки організації, оскільки людський ресурс є як найбільшою цінністю, так і головним джерелом внутрішніх ризиків. Її першочергове завдання полягає у запобіганні загрозам, пов'язаним із персоналом, включаючи шахрайство, промислове шпигунство, корупцію та несанкціоноване розголошення конфіденційної інформації. Ефективний менеджмент кадрової безпеки забезпечує ретельний відбір, перевірку та моніторинг співробітників, гарантуючи, що до критично важливих процесів і даних допущені лише надійні та лояльні особи. Це безпосередньо впливає на операційну безперервність та економічну стійкість, мінімізуючи втрати, спричинені суб'єктивним фактором.

Крім захисної функції, кадрова безпека відіграє вирішальну роль у підвищенні загальної ефективності

та конкурентоспроможності підприємства. Створення середовища, де панує висока корпоративна культура, довіра та чітке дотримання внутрішніх правил, сприяє зниженню плинності кадрів і підвищенню рівня мотивації. Регулярне навчання персоналу правил безпеки перетворює співробітників з потенційних джерел ризику на активних елементів захисту компанії. Таким чином, інвестиції в кадрову безпеку трансформуються в стратегічну перевагу, підтверджуючи, що надійність організації нерозривно пов'язана з надійністю її людського капіталу.

Функції кадрової безпеки організації охоплюють широкий спектр заходів, спрямованих на захист підприємства від загроз, що походять від людського фактору, а також на підтримку його стабільності та ефективності:

1. Захисна функція є першочерговою і полягає у створенні багаторівневого захисного механізму від протиправних або несанкціонованих дій співробітників, а також зовнішніх агентів, які можуть вплинути на персонал. Це включає запобігання крадіжкам, саботажу, промисловому шпигунству та неправомірному використанню службової інформації.

2. Превентивна функція фокусується на запобіганні ризиковим ситуаціям ще до їхнього настання. Вона реалізується через ретельну перевірку кандидатів на роботу (*due diligence*), психологічне тестування, профілактичні бесіди та формування внутрішніх стандартів поведінки, що мінімізують імовірність учинення неправомірних дій.

3. Аналітична функція передбачає систематичний збір, обробку та оцінку інформації, пов'язаної з персоналом, для виявлення потенційних загроз та вразливостей. Це включає аналіз плинності кадрів, вивчення причин незадоволеності співробітників, моніторинг дотримання внутрішніх політик та прогнозування можливих кадрових криз.

4. Регулятивна функція забезпечує розробку та впровадження внутрішніх нормативних документів, політик, інструкцій та процедур, які чітко регламентують права, обов'язки та відповідальність працівників у сфері безпеки. Вона також встановлює порядок доступу до конфіденційної інформації та відповідальність за його порушення.

5. Розвивальна (мотиваційна) функція сприяє підвищенню лояльності та компетентності персоналу у питаннях безпеки.

Це досягається через регулярне навчання, тренінги, формування високої корпоративної культури, що базується на довірі та взаємній відповідальності, а також створення прозорої системи винагород за дотримання стандартів безпеки.

6. Функція контролю та моніторингу забезпечує постійний нагляд за дотриманням встановлених правил безпеки, використанням інформаційних ресурсів та фізичних активів. Вона включає проведення внутрішніх розслідувань у разі виявлення порушень та використання технічних засобів контролю для оперативного виявлення та реагування на інциденти.

7.2. Складові управління кадровою безпекою організації

Управління кадровою безпекою є досить складним процесом, оскільки воно включає не лише організаційні та правові аспекти, а й психологічні, соціальні та навіть культурні фактори, які безпосередньо впливають на якість роботи персоналу та його лояльність до організації. Забезпечення високого рівня кадрової безпеки вимагає комплексного підходу, що поєднує системну оцінку ризиків, контроль за кадровими процесами, а також створення ефективної системи мотивації, яка мінімізує можливості виникнення внутрішніх загроз.

Основна складність полягає в тому, що людський фактор є найбільш непередбачуваним у системі безпеки, і будь-які помилки в доборі, навчанні чи мотивації персоналу можуть перерости у серйозні ризики для діяльності організації. Тому управління кадровою безпекою передбачає постійний моніторинг поведінкових і професійних характеристик співробітників, перевірку їх надійності та доброчесності, а також створення умов, за яких працівники зацікавлені у стабільній і чесній співпраці з роботодавцем.

Крім того, важливою складовою є захист конфіденційної інформації, до якої мають доступ працівники, адже витік даних через людський фактор може завдати найбільшої шкоди. Саме тому кадрова безпека виступає не лише елементом загальної безпекової системи, а й стратегічним інструментом збереження конкурентоспроможності організації та гарантією її сталого розвитку.

У сучасній економічні літературі визначення сутності управління кадровою безпекою організації можна розглядати за допомогою управлінського, ризик-орієнтованого та інтегрованого підходів.

Управління кадровою безпекою – це системна діяльність керівництва та спеціалізованих підрозділів організації, спрямована на формування, розвиток та ефективне використання трудового потенціалу з урахуванням ризиків, пов'язаних із людським фактором. Такий підхід передбачає впровадження організаційних, правових і соціально-психологічних заходів, які дозволяють знизити рівень загроз від персоналу та забезпечити стабільність роботи підприємства.

Під управлінням кадровою безпекою можна розуміти комплекс управлінських процедур, спрямованих на виявлення, оцінку та мінімізацію ризиків, пов'язаних із діяльністю працівників та кадровою політикою підприємства. Воно включає контроль за доброчесністю персоналу, запобігання плинності кадрів, протидію внутрішнім загрозам (шахрайство, зловживання, витік інформації) та створення умов, що мотивують співробітників до відповідальної роботи.

Управління кадровою безпекою – це інтегрована складова загальної системи корпоративної безпеки, що охоплює планування потреб у персоналі, забезпечення його професійної підготовки, створення системи контролю та моніторингу поведінки працівників, а також формування корпоративної культури довіри і відповідальності. Такий підхід поєднує правові, економічні, організаційні та психологічні інструменти з метою збереження кадрового потенціалу як головного ресурсу для розвитку організації.

До структури управління відносяться суб'єкти і об'єкти (розглянуто вище), а також основні методи та інструменти, які використовують організації для розробки стратегій, напрямів управління та зменшення впливу ризиків на економічну діяльність та кадрову політику зокрема. **Методами управління** кадровою безпекою є:

1. Адміністративно-правові методи. Цей підхід базується на розробці внутрішніх нормативних документів, регламентів і положень, які визначають правила поведінки персоналу, порядок доступу до інформації та матеріальних

цінностей. Його суть полягає в тому, що чітко встановлені норми і правила зменшують імовірність порушень та зловживань. До того ж завдяки адміністративним методам можна швидко реагувати на інциденти та притягати винних до відповідальності.

2. Економічні методи. Економічні інструменти стимулюють працівників дотримуватися корпоративних стандартів безпеки через систему матеріального заохочення чи штрафних санкцій. Сюди належать премії за сумлінну роботу, підвищення заробітної плати, соціальні пакети, а також фінансові втрати у разі порушень дисципліни. Такий підхід формує у персоналу економічну зацікавленість у збереженні стабільності та безпеки організації.

3. Організаційні методи. Організаційний підхід полягає у створенні відповідних структурних підрозділів, які контролюють кадрову безпеку, а також у впровадженні процедур відбору, адаптації, ротації та звільнення персоналу. Такі заходи дають змогу підвищити якість кадрового складу та знизити ризик потрапляння на робочі місця ненадійних осіб. Важливим інструментом є також регулярні внутрішні перевірки та контроль дотримання правил.

4. Соціально-психологічні методи. Вони спрямовані на формування здорового морально-психологічного клімату в колективі, розвиток корпоративної культури та створення умов, які знижують імовірність конфліктів чи зрадницьких дій з боку співробітників. Практичні заходи включають психологічне тестування, проведення тренінгів, коучингу та побудову ефективної системи комунікацій. Цей підхід дозволяє зміцнити довіру між керівництвом та працівниками і підвищити їхню лояльність до організації.

5. Інформаційно-аналітичні методи. Цей напрям передбачає моніторинг і аналіз кадрової інформації, перевірку біографічних даних працівників, їхнього професійного досвіду, кредитної та судової історії. Такі методи допомагають заздалегідь виявляти потенційні ризики, пов'язані з наймом або діяльністю співробітників. Своєчасний аналіз забезпечує можливість швидкого реагування на потенційні загрози та їх усунення.

6. Технічні методи. Вони включають використання сучасних технологій і програмних засобів для контролю

доступу, моніторингу інформаційних потоків і запобігання витоку даних. Наприклад, встановлення відеоспостереження, використання електронних систем контролю відвідуваності чи програмних засобів кіберзахисту. Ці методи відіграють допоміжну роль, підвищуючи ефективність адміністративних та організаційних заходів.

Інструменти кадрової безпеки – це практичні засоби й рішення, які дозволяють організації мінімізувати ризики, пов'язані з персоналом, і забезпечити стабільність діяльності. Вони охоплюють як технічні, так і організаційні заходи, що спрямовані на захист від зловживань, недобросовісності чи неефективності співробітників. Використання таких інструментів допомагає своєчасно виявляти потенційні загрози, попереджати кадрові кризи та підтримувати високий рівень довіри й дисципліни в колективі (табл. 7.2).

Інструменти кадрової безпеки безпосередньо впливають на рівень захищеності організації, оскільки вони надають можливості попереджати ризики, виявляти слабкі місця та підтримувати стабільність кадрового потенціалу. Скажімо, система перевірки персоналу при прийомі на роботу дає змогу знизити ймовірність потрапляння до колективу недобросовісних чи нелояльних співробітників. Інструменти контролю доступу до інформації мінімізують загрози витоку даних і забезпечують збереження комерційної таємниці.

Регулярне навчання й підвищення кваліфікації працівників допомагає формувати високий рівень компетентності та професійної культури, що зменшує ризики неякісного виконання обов'язків і сприяє розвитку лояльності. Використання інструментів моніторингу та внутрішніх аудитів дозволяє вчасно виявляти порушення чи недоліки у роботі, а також оперативно коригувати кадрову політику. Важливим також є застосування програм соціального захисту та мотиваційних систем, адже вони знижують плинність кадрів і підвищують відповідальність персоналу. Таким чином, інструменти кадрової безпеки формують цілісну систему превентивних та коригувальних заходів, яка прямо визначає рівень стійкості організації в умовах зовнішніх і внутрішніх викликів.

Наступною складовою є ризики, які утруднюють управління кадровою безпекою організації. Вони пов'язані

Таблиця 7.2

Інструменти кадрової безпеки організації

Інструмент	Характеристика
Службові контракти та посадові інструкції	Визначають права, обов'язки та відповідальність працівника, запобігаючи зловживанням і конфліктам.
Системи перевірки персоналу (background check)	Дають змогу оцінити доброчесність кандидата чи співробітника, перевіряючи його трудову історію, освіту, фінансовий стан чи можливі судимості.
HRM-системи (Human Resource Management Systems)	Автоматизують управління кадрами, забезпечують контроль за кадровими процесами та формують бази даних співробітників.
Системи контролю доступу	Обмежують фізичний і віртуальний доступ працівників до ресурсів організації відповідно до їхніх посадових обов'язків.
Оцінка компетенцій та атестація персоналу	Дозволяє визначати рівень знань, професійних навичок і придатність до виконання певних завдань.
Мотиваційні програми	Включають премії, бонуси, страхування, можливості кар'єрного розвитку для підвищення лояльності персоналу.
Соціологічні опитування та психологічне тестування	Виявляють рівень задоволеності роботою, лояльність та потенційні проблеми в колективі.
Внутрішній аудит кадрової політики	Перевірка відповідності процесів управління персоналом внутрішнім регламентам та законодавству.
Системи корпоративної культури	Формування цінностей, норм і правил поведінки, які сприяють зниженню ризиків недобросовісних дій з боку персоналу.

як із поведінкою персоналу, так і з внутрішніми та зовнішніми умовами діяльності. Найпоширеніші кадрові ризики включають плинність кадрів, що спричиняє втрату досвіду, зниження продуктивності та збільшення витрат на підбір і навчання нових працівників. Значною загрозою є недобросовісність співробітників, яка проявляється у шахрайстві, розкраданні ресурсів, навмисному порушенні трудової дисципліни або співпраці з конкурентами. Також важливо

враховувати демотивацію персоналу, що може призвести до зниження якості роботи, втрати ініціативності та посилення внутрішніх конфліктів.

До суттєвих ризиків відносять зловживання доступом до службової інформації, витік конфіденційних даних чи використання їх у власних інтересах. Окремої уваги потребують ризики, пов'язані з низькою кваліфікацією або відсутністю необхідних компетенцій у персоналу, адже це прямо впливає на ефективність виробничих процесів. Не менш небезпечними є ризики саботажу чи свідомого пошкодження майна, а також зростання рівня стресу та психологічного виснаження працівників у кризових умовах (наприклад, під час війни та обстрілів).

До перелічених ризиків варто також віднести проблеми з нелояльністю окремих співробітників, які можуть свідомо передавати конкурентам внутрішню інформацію чи шкодити інтересам організації. Серед небезпечних чинників називається саме плинність кадрів, адже постійна зміна персоналу призводить до втрати досвіду, збільшення витрат на адаптацію та зниження стабільності бізнес-процесів. Додаткову загрозу становлять недосконаліть внутрішніх процедур контролю та відсутність сучасних технологій моніторингу, що робить організацію більш уразливою до внутрішніх і зовнішніх атак на кадрову безпеку.

За напрямом впливу фактори можна розподілити на внутрішні та зовнішні (рис. 7.2).

Також основні ризики та результати дослідження ризиків у воєнний період представлені у додатку 3, демонструючи найбільші перешкоди та ризики сьогодення вітчизняних організацій. Враховуючи вплив війни на економічну складову держави і діяльність наших організацій у складних умовах, важливо визначати не лише поточний рівень їхньої стійкості, а й здатність адаптуватися до нових викликів. У сучасних реаліях підприємства змушені працювати в умовах постійних ризиків, пов'язаних із руйнуванням інфраструктури, логістичними обмеженнями, зростанням витрат на енергоресурси та загрозами для персоналу. Тому акцент робиться на формуванні системи управління безпекою, яка здатна

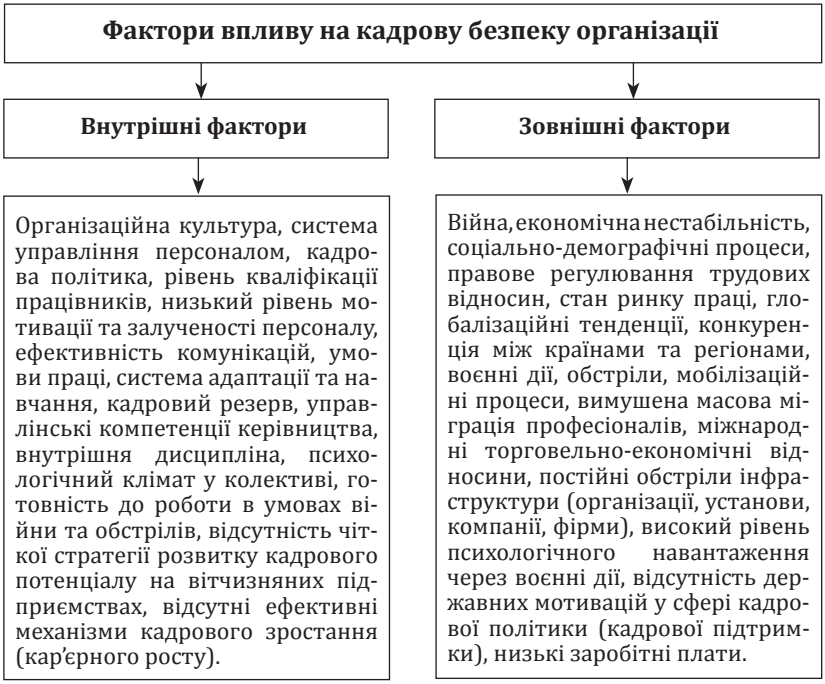


Рис. 7.2. Фактори,
що здійснюють вплив на кадрову безпеку організації

інтегрувати фінансові, кадрові та інвестиційні механізми для забезпечення безперервності діяльності.

Окрім цього, визначення стратегічних пріоритетів у сфері корпоративної та кадрової безпеки стає ключовим завданням для збереження конкурентоспроможності організацій на внутрішньому та зовнішньому ринках. Важливим є і проактивний підхід, що дозволяє завчасно передбачати можливі загрози, готувати плани антикризових дій та зміцнювати довіру інвесторів, партнерів і суспільства до підприємств, які функціонують у воєнний час.

7.3. Напрями збереження кадрової безпеки: вітчизняний та світовий досвід

Кадрова безпека організації – це цілісна система заходів і механізмів, спрямованих на захист інтересів підприємства у сфері роботи з персоналом. Вона охоплює не лише класичні аспекти добору й адаптації співробітників, а й питання збереження конфіденційної інформації, недопущення внутрішніх загроз і забезпечення стабільного кадрового потенціалу. У сучасних умовах кадрова безпека набуває особливої ваги, оскільки конкуренція на ринку праці зростає, війна та економічна нестабільність посилюють ризики, а цифровізація створює нові виклики, пов'язані з кіберзагрозами.

До ключових традиційних напрямів кадрової безпеки можна віднести: перевірку кандидатів під час працевлаштування, яка дозволяє виявити можливі ризики, пов'язані з ненадійністю чи низькою кваліфікацією; управління доступом до матеріальних і нематеріальних активів організації для запобігання витоку інформації чи зловживання службовим становищем; організацію системи захисту інформації, що включає як технічні, так і організаційні засоби; антикорупційні заходи, спрямовані на прозорість управлінських рішень; недопущення конфлікту інтересів шляхом впровадження корпоративних кодексів поведінки. Важливу роль відіграє й соціальний захист працівників, який підвищує їхню лояльність та знижує ризик зловживань, а також управління кадровими ризиками через систему моніторингу, аудиту та внутрішніх розслідувань (табл. 7.3).

Додатково до цих традиційних напрямів сучасна кадрова безпека включає ще кілька нових – це розвиток корпоративної культури та формування ціннісно орієнтованої поведінки персоналу, що зменшує схильність до порушень; психологічна та емоційна підтримка працівників в умовах високого рівня стресу, особливо під час воєнних дій; впровадження смарт-технологій і аналітичних систем для прогнозування поведінки персоналу й раннього виявлення потенційних загроз; співпраця з правоохоронними органами й державними структурами для посилення захисту у випадках критичних інцидентів (табл. 7.4).

Таблиця 7.3

Традиційні напрями збереження кадрової безпеки організації

Напрями кадрової безпеки	Характеристика та роль
Перевірка кандидатів при працевлаштуванні	Включає аналіз резюме, збір рекомендацій, перевірку біографічних даних і судимостей, психологічне тестування, що дозволяє знизити ризики працевлаштування ненадійних співробітників.
Управління доступом	Система заходів щодо обмеження та контролю доступу до матеріальних цінностей та конфіденційної інформації. Використовуються перепустки, паролі, контрольні журнали, розподіл обов'язків.
Захист інформації	Політики та технології, спрямовані на запобігання витоку службових відомостей: антивірусні програми, файрволи, корпоративні стандарти інформаційної гігієни.
Антикорупційні заходи	Кодекси етики, прозорі механізми прийняття рішень, внутрішні розслідування для запобігання хабарництву та зловживанням владою.
Запобігання конфлікту інтересів	Врегулювання ситуацій, коли працівники можуть використовувати службове становище у власних цілях; розробка корпоративних політик і кодексів поведінки.
Соціальний захист персоналу	Надання працівникам соціальних гарантій, пільг, страхування, створення сприятливого мікроклімату в колективі для підвищення лояльності.
Внутрішні розслідування	Виявлення порушень внутрішніх правил та запобігання повторним випадкам через контроль і аудит діяльності співробітників.

Тема війни та обстрілів є надзвичайно актуальною для кадрової безпеки, оскільки вона напряму впливає на психічний стан працівників, їхню працездатність і готовність залишатися частиною організації. Військові дії, ракетні обстріли та постійна загроза для життя створюють надмірний рівень стресу, що негативно відбивається на персоналі. Працівники можуть переживати посттравматичні розлади, відчуття тривожності, страху та нестабільності, що призводить до зниження продуктивності, підвищення плинності кадрів і зростання ризику неконтрольованих конфліктів. Окрім цього, в умовах війни часто порушується фізична безпека співробітників, що стає одним із ключових викликів кадрової політики.

Таблиця 7.4

Новітні (сучасні) напрями збереження кадрової безпеки організації

Напрями кадрової безпеки	Характеристика та роль
Розвиток корпоративної культури	Формування єдиної системи цінностей і норм поведінки, що знижує ймовірність виникнення внутрішніх конфліктів і недобросовісних дій персоналу.
Психологічна підтримка	Забезпечення програм адаптації, коучингу, зниження стресу, особливо в умовах воєнних дій чи економічної нестабільності.
Використання смарт-технологій	Аналітичні системи прогнозування ризиків, автоматизовані HR-платформи, системи відеоспостереження та аналізу поведінки персоналу.
Співпраця з державними органами	Налагодження комунікації з правоохоронними структурами та органами влади для захисту від зовнішніх і внутрішніх загроз.
Навчання персоналу	Постійне підвищення кваліфікації, тренінги з інформаційної безпеки, семінари щодо запобігання шахрайству та зловживанням.
Цифрова гігієна	Створення правил поводження з інформаційними ресурсами, навчання користувачів базових цифрових навичок безпеки.

Організації, які прагнуть забезпечити кадрову безпеку, повинні приділяти велику увагу збереженню психічного здоров'я персоналу. Це включає створення програм психологічної підтримки, організацію консультацій з фахівцями, проведення тренінгів із подолання стресу та розвитку стресостійкості. Важливо впроваджувати заходи для зниження напруженості: гнучкі графіки роботи, віддалений формат роботи, надання додаткових відпусток у випадку психологічного вигорання.

Для кадрової безпеки у воєнний час важливим є забезпечення фізичного захисту працівників – облаштування укриттів, розробка планів евакуації, створення каналів термінового оповіщення. Паралельно необхідно зміцнювати довіру та корпоративну культуру, аби люди відчували підтримку організації і не залишалися сам на сам зі своїми проблемами.

Окремим напрямом є інформаційна безпека: керівництво має запобігати панічним настроям, поширенню дезінформації та забезпечувати прозору комунікацію з персоналом.

Розглянемо характеристику зарубіжних моделей кадрової безпеки як таких, котрі можна брати за основу при розробці сучасних вітчизняних підходів до реалізації кадрової безпеки.

Японська модель кадрової безпеки традиційно орієнтована на колективізм та довготривалі відносини між компанією і працівником. Компанії в Японії часто використовують такі методи, як:

– жорсткий відбір персоналу – до компанії потрапляють ті, хто не тільки володіє необхідними професійними навичками, але й відповідає корпоративній культурі;

– пожиттєве наймання – це створює відчуття стабільності та лояльності у працівників, знижуючи ризики витоку інформації;

– система менторства – досвідчені співробітники передають знання та корпоративні цінності молодим фахівцям, сприяючи формуванню єдиної корпоративної культури;

– сильна корпоративна культура – об'єднує працівників і створює відчуття спільності, що знижує ризик внутрішніх конфліктів та зрадництва.

Американська модель кадрової безпеки більше орієнтована на індивідуалізм та конкуренцію. Основні методи захисту кадрової безпеки в США включають:

– строгі договори про нерозголошення комерційної таємниці – практично всі співробітники підписують такі договори, що чітко визначають їхні обов'язки щодо захисту інформації компанії;

– регулярні перевірки на поліграфі – особливо це стосується працівників, які мають доступ до конфіденційної інформації;

– системи контролю доступу – складні системи дозволів обмежують доступ співробітників до інформаційних систем і фізичних об'єктів;

– постійне навчання співробітників – працівники регулярно проходять навчання щодо інформаційної безпеки, щоби бути в курсі нових загроз та способів захисту від них.

Німецька модель кадрової безпеки базується на високій дисципліні, законодавчому регулюванні та співпраці між роботодавцями і працівниками. Основними інструментами кадрової безпеки тут є такі:

– колективні договори та сильні профспілки – вони виконують важливу роль у захисті прав працівників і регулюванні трудових відносин;

– дуальна система освіти – поєднання теоретичного навчання і практичної підготовки дозволяє формувати кваліфікованих працівників, знижуючи ризики некомпетентності персоналу;

– соціальне страхування – кожен працівник має гарантії захисту у випадку хвороби, втрати роботи чи нещасних випадків;

– культура дисципліни і точності – чітке дотримання правил і процедур знижує ризики внутрішніх порушень і помилок.

Швейцарська модель кадрової безпеки. Швейцарія традиційно робить акцент на гнучкості, високому рівні довіри та поєднанні державного і приватного регулювання. Основні характеристики моделі:

– персоналізація трудових відносин – кожен працівник має індивідуальний контракт, що дає можливість враховувати особливості його діяльності;

– багатомовність і мультикультуральність – управління персоналом враховує різноманіття культур і мов, що знижує ризики конфліктів і сприяє комунікації;

– потужна система страхування – включає медичне, пенсійне та безробітне страхування, що гарантує соціальну стабільність;

– акцент на інноваціях – компанії інвестують у підвищення кваліфікації та розвиток працівників, щоб уникати відтоку кадрів.

Британська модель кадрової безпеки орієнтована на дотримання стандартів і гнучке управління трудовими ресурсами в умовах глобального ринку. Характерні риси:

– сильна роль держави у встановленні стандартів праці та антикорупційних норм – це створює прозорі умови для діяльності підприємств;

– жорстка політика щодо захисту даних (GDPR) – компанії змушені впроваджувати сучасні інструменти захисту інформації від витоку через працівників;

– розвиток системи корпоративної соціальної відповідальності – увага приділяється не лише фінансовим результатам, а й добробуту персоналу;

– широке використання аутсорсингу і тимчасової зайнятості – це дозволяє знизити ризики надмірних витрат, але водночас потребує суворих процедур контролю кадрів.

Для забезпечення ефективного відновлення кадрової безпеки в Україні у постворенний період доцільно запозичити такі практики зі зарубіжних моделей:

1. Із японської моделі: акцент на довготривалій зайнятості та корпоративній лояльності – створення програм утримання персоналу, інвестування в навчання і розвиток навичок працівників, формування сильної корпоративної культури, яка підвищує стабільність кадрів.

2. Із американської моделі: застосування контрактних підходів та сучасних систем контролю доступу й безпеки інформації – введення обов'язкових угод про нерозголошення, регулярних перевірок і навчання з кібербезпеки для персоналу, що має доступ до критичних ресурсів.

3. Із німецької моделі: впровадження дуальної системи освіти та тісна взаємодія бізнесу з навчальними закладами – розвиток систем, які готують кадри зі специфічними компетенціями, потрібними для реконструкції та модернізації підприємств.

4. Зі швейцарської моделі: гнучкі трудові відносини, високий рівень соціального захисту і страхування, адаптивність до змін – введення механізмів соціальної підтримки працівників, які пережили воєнні події, а також можливостей перекваліфікації та тимчасової зайнятості.

5. Із британської моделі: сильне правове регулювання трудових відносин, прозорість і корпоративна соціальна відповідальність – удосконалення трудового законодавства, встановлення чітких стандартів поведінки працівників, розвиток програм корпоративної відповідальності, які включають підтримку психологічного стану та благополуччя співробітників.

Питання для самоконтролю

1. У чому полягає сутність кадрової безпеки організації та чому вона є базовою складовою економічної безпеки?
2. Які внутрішні й зовнішні фактори найбільше впливають на стан кадрової безпеки сучасного підприємства?
3. Назвіть основні підходи до визначення сутності кадрової безпеки та охарактеризуйте їх зміст.
4. Які суб'єкти кадрової безпеки відіграють основну роль у її забезпеченні?
5. Охарактеризуйте об'єкти кадрової безпеки та поясніть, чому вони є вразливими до ризиків.
6. Які методи та інструменти найчастіше використовують в управлінні кадровою безпекою?
7. Які типові кадрові ризики найбільш небезпечні для організації у воєнний і післявоєнний період?
8. Як впливають соціально-психологічні фактори (мотивація, корпоративна культура, конфлікти) на кадрову безпеку?
9. Які моделі кадрової безпеки застосовуються у зарубіжних країнах і що з їхнього досвіду доцільно впровадити в Україні?
10. У чому полягає важливість управління кадровими ризиками та які наслідки може спричинити його відсутність?

Тестові завдання

1. Під кадровою безпекою підприємства розуміють:

а) систему заходів, спрямованих на захист фінансових ресурсів та прибутків компанії у короткостроковій перспективі;

б) сукупність дій і механізмів, що забезпечують захищеність персоналу та мінімізацію кадрових ризиків;

в) лише перевірку персоналу перед прийомом на роботу;

г) встановлення системи відеоспостереження в офісі.

2. Яка основна мета кадрової безпеки?

а) Підвищення конкурентоспроможності продукції;

б) захист законних інтересів організації від внутрішніх і зовнішніх загроз, пов'язаних із персоналом;

в) скорочення податкового навантаження на підприємство;

г) підвищення рівня автоматизації бізнес-процесів.

3. Ключовими суб'єктами кадрової безпеки є:

а) державні органи;

б) власники, менеджери, служби безпеки, кадрові служби, самі працівники;

в) постачальники та підрядники;

г) лише охоронні компанії.

4. До яких об'єктів відноситься кадрова безпека?

а) Виключно технічне обладнання;

б) персонал, кадрові процеси, корпоративна культура, інформаційні ресурси;

в) тільки фінансові ресурси організації;

г) тільки трудові договори.

5. Які з наведених ризиків можна віднести до кадрових?

а) Плинність кадрів, витік конфіденційної інформації, недобросовісність працівників;

б) коливання валютних курсів та інфляція;

в) зміни в податковому законодавстві;

г) політична нестабільність.

6. Які інструменти найчастіше застосовують у кадровій безпеці?

а) Перевірка персоналу, контроль доступу, внутрішні регламенти, система мотивації;

б) виключно маркетингові дослідження;

в) аналіз макроекономічних тенденцій;

г) ведення бухгалтерського обліку.

7. Який метод передбачає оцінку співробітників через співбесіди, анкетування та тестування?

а) Аналітичний метод;

б) соціально-психологічний метод;

в) метод внутрішнього аудиту;

г) технічний метод.

8. Що є перевагою впровадження кадрової безпеки для підприємства?

а) Зменшення витрат на сировину;

б) стабільність роботи колективу, зниження рівня ризиків і конфліктів, зростання довіри між працівниками та керівництвом;

в) збільшення кількості зовнішніх партнерів;

г) прискорення обороту капіталу.

9. Якою особливістю вирізняється японська модель кадрової безпеки?

а) Пожиттєве наймання, система наставництва, сильна корпоративна культура, відповідальність за всіх працівників;

б) використання поліграфа та договорів про нерозголошення;

в) абсолютна гнучкість трудових відносин;

г) переважання віддаленої роботи.

10. В умовах війни кадрова безпека набуває особливого значення:

а) тому що зростає потреба у швидкому освоєнні нових ринків;

б) через загрози фізичній безпеці працівників, психологічному стану персоналу, а також через ризики масових міграцій і втрати кваліфікованих кадрів;

в) лише через зміну системи оподаткування;

г) через зростання конкуренції серед підприємств.

Практичні завдання

Завдання 1.

Компанія «Альфа» планує розширити свій штат для забезпечення нових контрактів із закордонними партнерами. У зв'язку з воєнними діями в країні зросли ризики проникнення до організації осіб із підробленими документами, а також можливість шпигунської діяльності. На співбесіду прийшли 15 кандидатів, серед яких у 4 відсутні повні пакети документів, а в 2 виявлено розбіжності в трудових книжках. Крім цього, керівництво виявило підвищену напругу в колективі через невпевненість у майбутньому та поширення чуток, що негативно вплинули на психологічний стан.

1. Визначте, які інструменти кадрової безпеки слід застосувати для перевірки кандидатів.

2. Запропонуйте систему заходів для зниження внутрішніх ризиків і відновлення довіри в колективі.

3. Оцініть фінансові та репутаційні втрати компанії у випадку, якщо кадрові ризики будуть проігноровані.

Завдання 2.

У великій торговельній мережі «Вектор» було виявлено, що начальник відділу постачання укладав угоди з компаніями, які належать його близьким родичам. Унаслідок цього підприємство переплачувало за продукцію на 15% від ринкової вартості. Паралельно з цим у колективі зросла плинність кадрів, оскільки співробітники вважали кадрову політику несправедливою. Служба безпеки підприємства підозрює наявність змови та вимагає впровадження нових процедур контролю.

1. Сформулюйте, які саме кадрові ризики виявилися в цій ситуації.

2. Розробіть пропозиції щодо запобігання конфлікту інтересів у майбутньому.

3. Обґрунтуйте, як це вплине на корпоративну культуру та довгострокову кадрову безпеку.

Завдання 3.

Промислове підприємство «Оріон», яке продовжує роботу в зоні підвищеної небезпеки, зіткнулося з проблемами демотивації та психологічного вигорання працівників. Під час останніх обстрілів було пошкоджено частину виробничих приміщень, а кілька співробітників отримали поранення. У колективі поширюється страх, знижується продуктивність праці, а відділ кадрів фіксує збільшення заяв на звільнення. Власники підприємства розглядають можливість впровадження програм підтримки персоналу, але не знають, які саме заходи будуть найбільш ефективними.

1. Запропонуйте комплекс заходів кадрової безпеки для підтримки психічного здоров'я працівників.

2. Визначте, які методи управління ризиками можна застосувати в цій ситуації.

3. Обґрунтуйте роль кадрової безпеки у збереженні кадрового потенціалу підприємства в умовах війни.

ТЕМА 8

ІНФОРМАЦІЙНА БЕЗПЕКА В СТРУКТУРІ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ

8.1. Сутність інформаційної безпеки організації
8.2. Види і принципи інформаційної безпеки
8.3. Джерела загроз інформаційній безпеці організації
8.4. Напрями запобігання інформаційним ризикам в організації та управління ними

Основні поняття і терміни: інформація, інформаційна безпека, організація, програмні засоби, менеджмент інформаційної безпеки, інформаційні загрози, кібератаки, захист інформації, технічні загрози, інформаційні системи, інформація в доступі, обмежена інформація.

8.1. Сутність інформаційної безпеки організації

Інформаційна безпека в сучасних умовах є однією з найважливіших складових діяльності організації, адже саме інформація сьогодні виступає стратегічним ресурсом, який визначає конкурентоспроможність і стабільність бізнесу. Вона передбачає комплекс заходів і технологій, спрямованих на захист даних, інформаційних систем і комунікаційних каналів від несанкціонованого доступу, втрати, викривлення чи знищення. Забезпечення інформаційної безпеки має ключове значення не лише для захисту комерційної таємниці та конфіденційних відомостей, а й для підтримання довіри клієнтів, партнерів та інвесторів. З огляду на це побудова надійної системи інформаційної безпеки стає невід'ємною частиною загальної корпоративної стратегії будь-якої організації.

Інформаційна безпека – це галузь знань та практичних заходів, що спрямовані на забезпечення захисту інформаційних ресурсів фізичних і юридичних осіб, а також державних структур від будь-яких загроз, які можуть призвести до втрати даних, порушення їх цілісності, спотворення, несанкціонованого використання чи копіювання. Вона охоплює

організаційні, технічні та правові механізми, які дозволяють зберігати стабільність функціонування інформаційних систем і мінімізувати ризики несанкціонованого втручання.

У сучасних умовах інформаційна безпека стає критично важливою складовою діяльності будь-якої організації, оскільки від рівня захищеності інформаційних потоків залежить конкурентоспроможність, фінансова стійкість та ділова репутація компанії. Тому інформаційну безпеку слід розглядати не лише як технічну сферу, а й як стратегічний елемент управління ризиками, що потребує інтеграції в загальну систему корпоративної безпеки.

Інформаційна безпека організації – це сукупність організаційних, технічних та правових заходів, спрямованих на захист інформаційних активів підприємства, включно з даними, системами та комунікаціями, від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності інформації.

Інформаційна безпека в межах організації – це система управління ризиками, яка передбачає створення та підтримання умов, за яких інформаційні ресурси (у будь-якій формі) зберігаються, обробляються та передаються захищено, із мінімальними вразливостями та ризиками громадсько-управлінського, фінансового чи технічного характеру.

Також інформаційну безпеку організації можна розглядати з декількох ракурсів:

– технічний – передбачає використання технічних засобів захисту даних, таких як системи контролю доступу, шифрування, міжмережеві екрани, антивірусні програми та системи виявлення вторгнень. Це дозволяє запобігати несанкціонованому доступу, пошкодженню або знищенню інформації;

– організаційний – включає розробку внутрішніх політик, регламентів і процедур, які регулюють порядок роботи з інформаційними ресурсами. Йдеться про розподіл прав доступу, відповідальність співробітників, процедури реагування на інциденти та контроль дотримання правил безпеки;

– правовий – передбачає дотримання чинного законодавства та нормативних актів у сфері захисту інформації, захисту персональних даних і комерційної таємниці.

Також важливим є застосування договорів про нерозголошення та відповідальність за їх порушення;

– людський – одним із ключових елементів вважається персонал організації, адже навіть найкращі технічні засоби не забезпечать безпеки без належної поведінки співробітників. Тому важливим є навчання кадрів, формування культури інформаційної безпеки, а також психологічна готовність до дотримання правил;

– стратегічний – розглядається як складова загальної стратегії розвитку організації. Вона включає довгострокове планування захисту даних, врахування нових технологічних викликів, інвестиції у модернізацію систем і побудову конкурентоспроможності на основі безпеки даних.

Засоби та методи забезпечення інформаційної безпеки мають різне функціональне призначення та спрямовані на захист даних від зовнішніх і внутрішніх загроз. Програмні засоби охоплюють антивірусний захист, системи автентифікації та інші рішення для ідентифікації користувачів. Технічні інструменти включають механізми фізичного та електронного захисту інформаційних систем від несанкціонованого доступу чи пошкодження. Адміністративні методи полягають у створенні внутрішніх регламентів і правил взаємодії працівників з інформаційними ресурсами. Важливим елементом є й морально-етичні принципи, що формують культуру відповідального користування інформацією. Правові підходи встановлюють правила використання даних, а також визначають юридичну відповідальність за їх порушення.

Етичні стандарти передбачають недопущення використання комп'ютерної техніки або програмного забезпечення для заподіяння шкоди іншим людям, а також зобов'язують поважати авторські права. Правові основи інформаційної безпеки формуються на базі спеціальних законодавчих актів, які гарантують права людини у сфері захисту даних та передбачають відповідальність за правопорушення. В Україні до таких нормативних документів належать закони України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних», «Про авторське право та суміжні права» та низка постанов, які формують цілісну правову базу для підтримання високого рівня інформаційної безпеки.

Роль інформаційної безпеки у діяльності організації є однією з головних, адже вона безпосередньо впливає на стабільність бізнес-процесів, конкурентоспроможність і довіру до компанії. Забезпечення захисту даних дозволяє організації уникати фінансових втрат, що можуть виникнути через витік конфіденційної інформації, шахрайство або кібератаки. Крім того, інформаційна безпека є основою для збереження ділової репутації, адже порушення в цій сфері часто призводять до втрати партнерів, клієнтів і інвесторів.

У стратегічному вимірі інформаційна безпека створює умови для довгострокового розвитку організації. Вона гарантує надійність бізнес-процесів, забезпечує захист інтелектуальної власності, інновацій та технологій. Важливо й те, що завдяки ефективній системі інформаційної безпеки компанія спроможна дотримуватися вимог законодавства та міжнародних стандартів, що є запорукою її легітимності на ринку. Таким чином, інформаційна безпека виконує функцію не лише захисту від загроз, а й інструмента підвищення стійкості й конкурентних переваг організації.

Отже, **інформаційна безпека організації** – це система заходів, що забезпечує захист інформаційних ресурсів і даних від несанкціонованого доступу, витоку, модифікації або знищення. Вона охоплює технологічні, адміністративні та фізичні аспекти, що гарантують конфіденційність, цілісність та доступність інформації, необхідної для ефективного функціонування організації. Основною метою інформаційної безпеки є мінімізація ризиків, пов'язаних з інформаційними загрозами, та забезпечення безперервності бізнес-процесів.

Менеджмент інформаційної безпеки організації – це комплекс управлінських процесів, що забезпечують систематичний підхід до захисту інформаційних активів від загроз. Він включає в себе розробку політик, процедур і стратегій, оцінку ризиків, управління інцидентами, навчання персоналу, а також моніторинг і аудит заходів безпеки. Основною метою менеджменту інформаційної безпеки є створення ефективної системи захисту інформації, яка забезпечує її конфіденційність, цілісність і доступність, а також відповідає вимогам законодавства та стандартів у цій сфері.

Безпосереднє забезпечення інформаційної безпеки організації пов'язане з діяльністю різних суб'єктів, які виконують

спеціалізовані функції та відповідають за конкретні аспекти захисту інформаційних ресурсів. Передусім до них належать керівники та власники компанії, адже саме вони формують політику безпеки, визначають пріоритети та виділяють ресурси на створення комплексної системи захисту. Важливу роль відіграють ІТ-підрозділи та служби інформаційної безпеки, що безпосередньо займаються технічними аспектами: впровадженням програмних і апаратних засобів захисту, моніторингом інформаційних потоків, виявленням загроз та реагуванням на інциденти організації (додаток К).

Не менш значущими суб'єктами є працівники всіх рівнів, оскільки від їхньої обізнаності, дисципліни та дотримання правил залежить ефективність інформаційної безпеки. Навчання персоналу правил роботи з конфіденційною інформацією, правильне використання паролів та засобів автентифікації знижує ризики випадкового чи навмисного витоку даних:

1. Керівництво організації – визначає політику інформаційної безпеки, забезпечує ресурсами і підтримує ініціативи в цій сфері.

2. Відділ інформаційної безпеки – відповідає за реалізацію політики безпеки, розробку процедур, оцінку ризиків і реагування на інциденти.

3. Співробітники – усі працівники організації, які мають доступ до інформаційних ресурсів, повинні дотримуватися встановлених норм і процедур.

4. ІТ-відділ – забезпечує технологічні рішення для захисту інформації, включаючи апаратні та програмні засоби безпеки.

5. Аудитори та зовнішні консультанти – оцінюють рівень інформаційної безпеки, проводять зовнішні перевірки та пропонують рекомендації.

6. Правові органи та регулятори – забезпечують відповідність організації законодавству і стандартам у сфері інформаційної безпеки.

Додатковими суб'єктами виступають державні органи та регулятори, що встановлюють нормативно-правову базу й контролюють дотримання законодавчих вимог у сфері кібербезпеки. В окремих випадках до процесу забезпечення

Таблиця 8.1

Види і характеристика об'єктів інформаційної безпеки організації

Об'єкти інформаційної безпеки	Характеристика
Інформаційні ресурси	Сукупність даних і знань, що створюються, обробляються і зберігаються в організації, включаючи бази даних, документи, програмне забезпечення, результати досліджень.
Технічні системи та інфраструктура	Сервери, комп'ютери, мережеве обладнання, засоби телекомунікації та інформаційні системи, які забезпечують зберігання та передачу даних.
Кадровий потенціал	Співробітники, які мають доступ до інформації, їхня компетентність, рівень обізнаності та відповідальність у сфері інформаційної безпеки.
Фінансова інформація	Дані про фінансовий стан компанії, звітність, інвестиції, операції з активами та зобов'язаннями, комерційні та банківські таємниці.
Комерційна таємниця	Відомості про технології, ноу-хау, бізнес-плани, контракти, стратегії, які мають конкурентну цінність і підлягають захисту від витоку.
Персональні дані	Інформація про співробітників, клієнтів чи партнерів, що регламентується законодавством і вимагає спеціального захисту.
Канали комунікації	Внутрішні та зовнішні засоби обміну інформацією (електронна пошта, месенджери, телефонні лінії, відеоконференції), які можуть бути об'єктом несанкціонованого доступу.
Інтелектуальна власність	Результати інноваційної діяльності: патенти, авторські права, програмні продукти, торгові марки, які формують додану вартість організації.
Репутаційна інформація	Дані, що формують імідж і довіру до компанії в очах клієнтів, інвесторів та партнерів, включаючи публічні заяви, відгуки та медіаматеріали.
Інформаційне середовище	Зовнішні джерела інформації, що впливають на діяльність організації: ринок, нормативно-правова база, діяльність конкурентів та регуляторів.

інформаційної безпеки залучаються зовнішні підрядники, консалтингові компанії та служби аудиту, які здійснюють незалежну оцінку захищеності систем та розробляють рекомендації щодо її підвищення. Таким чином, інформаційна безпека є результатом спільної діяльності внутрішніх і зовнішніх суб'єктів, чия взаємодія створює цілісну систему захисту.

Об'єкти інформаційної безпеки організації та їх характеристика подані в табл. 8.1.

8.2. Види і принципи інформаційної безпеки

Сьогодні інформаційна безпека виконує надважливу роль у функціонуванні сучасних підприємств, установ та організацій, адже від рівня захищеності даних напряму залежить ефективність їхньої діяльності та конкурентоспроможність. З огляду на те, що більшість бізнес-процесів інтегровані в цифрове середовище, саме інформаційні ресурси стають найбільш цінним активом і водночас найбільш уразливим об'єктом. Загрози можуть надходити як зі зовнішнього середовища (кібератаки, промислове шпигунство, війна та пов'язані з нею обстріли інфраструктури), так і з внутрішніх джерел (недобросовісність персоналу, технічні помилки, порушення правил доступу). Внаслідок порушення інформаційної безпеки організація ризикує зазнати фінансових збитків, втратити партнерів, клієнтів та репутацію.

Водночас варто зазначити, що кількість загроз інформаційній безпеці з кожним роком лише зростає, і це обумовлює потребу у впровадженні комплексних систем захисту. Вони мають враховувати як технологічні інструменти (системи шифрування, контроль доступу, моніторинг мереж), так і організаційні підходи (навчання персоналу, аудит інформаційних процесів, формування політики безпеки). У сучасних умовах інформаційна безпека вже не розглядається лише як технічне питання, а є невід'ємною складовою загальної стратегії управління підприємством. Саме тому ефективне управління інформаційною безпекою стає передумовою стійкого розвитку та підвищення довіри з боку інвесторів, партнерів і клієнтів та вимагає визначення різних видів

з метою більш чіткої оцінки та управління. Інформаційну безпеку організації можна класифікувати за такими ознаками:

1. За рівнем захисту інформаційних ресурсів:

– публічна інформація – дані, призначені для відкритого доступу і не потребують жорстких заходів захисту;

– внутрішня інформація – матеріали, що використовуються в рамках організації і не призначені для поширення за її межами;

– конфіденційна інформація – відомості, доступ до яких обмежений і які потребують захищеного зберігання та передачі;

– секретна (або строго секретна) інформація – дані найвищої чутливості, розголошення яких може завдати серйозної шкоди організації, а також доступ суворо регламентований.

2. За складовими (аспектами) інформаційної безпеки:

– технічна безпека – захист апаратної та програмної інфраструктури (мережі, сервери, пристрої) від несанкціонованого доступу, ушкодження чи втрати;

– організаційна безпека – створення політик, процедур і структур, які регламентують роботу з інформаційними ресурсами, ролі та відповідальність працівників;

– правова безпека – застосування нормативно-правових актів, стандартів і договорів, які регулюють захист даних, відповідальність за їх розголошення або втрату;

– людський (соціальний) аспект – пов'язаний з підготовкою персоналу, культурою безпеки, етичними нормами, усвідомленням загроз і дисциплінованою поведінкою працівників у сфері інформації.

3. За технологічними доменами:

– мережева безпека – охоплює захист інфраструктури передачі необхідних даних (LAN, WAN, VPN) від атак і несанкціонованого проникнення;

– безпека кінцевих пристроїв (Endpoint Security) – захист окремих пристроїв (ноутбуків, смартфонів, планшетів) через антивірус, контроль доступу, шифрування;

– безпека застосунків (Application Security) – забезпечення безпеки програмного забезпечення в процесі розробки, тестування, впровадження та експлуатації;

– хмарна безпека (Cloud Security) – заходи захисту ресурсів, що розміщені в хмарному середовищі, в умовах зміни кордонів і контролю над даними.

4. За функціональним призначенням заходів:

– профілактика (preventive) – заходи, спрямовані на недопущення інцидентів (наприклад, політики безпеки, шифрування, навчання персоналу);

– виявлення (detective) – системи і процедури, що дають можливість діагностувати порушення безпеки чи аномалії у роботі систем (IDS, моніторинг, логування);

– коригування (corrective/response) – дії, спрямовані на мінімізацію наслідків інцидентів, відновлення функціональності та підвищення стійкості систем.

5. За доменом застосування:

– фізична інформаційна безпека – захист фізичних носіїв, обладнання, приміщень, переміщень інформаційних ресурсів;

– операційна інформаційна безпека – заходи, пов'язані зі щоденною діяльністю: резервне копіювання, контроль змін, управління доступом;

– аналітична (інтелектуальна) безпека – пов'язана з аналізом загроз, прогнозуванням сценаріїв, управлінням ризиками, виявленням витоків і непрямих загроз;

– стратегічна інформаційна безпека – інтегрування інформаційної безпеки в загальну стратегію організації, врахування цифрових трансформацій, взаємодія з зовнішнім середовищем, конкурентними і технологічними змінами.

6. За часовим горизонтом:

– оперативна безпека – заходи, що забезпечують негайний захист інформації в режимі реального часу (системи моніторингу, антивіруси, IDS/IPS);

– тактична безпека – планування та реалізація середньострокових рішень, які відповідають на актуальні виклики (оновлення політик, модернізація техніки, підготовка персоналу);

– стратегічна безпека – довгострокове бачення та інтеграція інформаційної безпеки у стратегію розвитку організації, включно з прогнозуванням нових ризиків та сценаріїв.

7. За рівнем організації (системності):

– локальна інформаційна безпека – охоплює окремі підрозділи чи відділи організації, конкретні інформаційні системи;

– корпоративна інформаційна безпека – стосується всієї компанії в цілому, інтегрується з іншими видами корпоративної безпеки (кадровою, фінансовою, технічною);

– галузева і державна – стосується підприємств на рівні галузей чи секторів економіки, а також загальнонаціональних інформаційних систем (банківських, енергетичних, оборонних).

8. За природою загроз:

– природні загрози – стихійні лиха, пожежі, відключення електроенергії, які можуть пошкодити інформаційні ресурси;

– техногенні загрози – аварії обладнання, помилки програмного забезпечення, збої систем;

– людський фактор – помилки користувачів, недобросовісні дії співробітників, соціальна інженерія;

– кіберзагрози – хакерські атаки, шкідливе ПЗ, фішинг, DDoS.

9. За рівнем критичності даних (Data sensitivity):

– несуттєва інформація – її розголошення не завдасть шкоди організації;

– обмежено важлива – потребує базових заходів захисту, оскільки має значення для бізнес-процесів;

– критична інформація – дані, розкриття чи втрата яких може призвести до серйозних фінансових або репутаційних збитків;

– життєво важлива – дані, що є основою діяльності підприємства; їх втрата може призвести до зупинки бізнесу чи катастрофічних наслідків.

Інформаційна безпека на будь-якому рівні управління ґрунтується на дотриманні базових принципів (рис. 8.1), що виступають вихідними орієнтирами, встановленими нормами та правилами поведінки для всіх суб'єктів господарської діяльності. Саме ці засади формують основу політики захисту інформації та визначають стандарти взаємодії між учасниками організаційних процесів.

Рис. 8.1. Принципи забезпечення інформаційної безпеки

Якщо розглядати наведені принципи детальніше, то:

– принцип цілісності означає захист інформації від спотворення, пошкодження чи несанкціонованих змін, оскільки забезпечення цілісності гарантує, що дані залишаються достовірними й коректними на всіх етапах їх обробки та передачі;

– принцип конфіденційності полягає в обмеженні доступу до інформації лише для тих осіб, які мають відповідні повноваження. Конфіденційність захищає дані від витоку чи неправомірного розкриття;

– принцип доступності полягає в забезпеченні безперервного та своєчасного доступу до інформації для уповноважених користувачів. Недоступність даних у потрібний момент може стати серйозною загрозою для функціонування організації;

– принцип автентичності гарантує, що інформація отримана саме від того джерела, від якого очікувалось, і що вона не була змінена сторонніми під час передавання та забезпечує довіру до комунікацій і транзакцій;

– принцип надійності передбачає стабільність функціонування систем захисту та відсутність збоїв у роботі, при цьому системи повинні витримувати навантаження і протидіяти загрозам навіть у кризових ситуаціях;

– принцип контрольованості означає можливість відстеження дій користувачів і систем, ведення журналів подій та проведення аудиту. Контрольованість допомагає виявляти інциденти й запобігати повторним порушенням;

– принцип правомірності має забезпечуватися відповідно до чинних законів і нормативних актів та означає дотримання прав людини, авторських прав, а також законів про захист даних;

– принцип законності в системі інформаційної безпеки означає, що всі дії підприємства у сфері захисту даних мають ґрунтуватися на чинному законодавстві України та відповідати міжнародним угодам і стандартам;

– принцип права власності вимагає гарантування прав суб'єктів на інформацію, що створена ними чи належить на законних підставах, при цьому обмеження доступу до таких даних допускається лише в межах, передбачених законом, і лише з метою захисту безпеки;

– принцип економічної доцільності акцентує увагу на тому, що вартість інформації та її захист повинні бути враховані у загальній структурі витрат підприємства. Порушення безпеки може спричинити значні фінансові збитки, тому керівництво має завчасно оцінювати потенційні ризики та мінімізувати їхні економічні наслідки;

– принцип комплексності передбачає створення єдиної системи, де заходи фізичної, технічної, організаційної та кадрової безпеки взаємопов'язані та узгоджені між собою. Це дозволяє не лише локалізувати окремі загрози, але й забезпечувати багаторівневий захист усього інформаційного середовища організації. Системність такого підходу сприяє зменшенню помилок та забезпечує узгодженість дій усіх підрозділів.

– принцип безперервності означає, що захист інформації має здійснюватися постійно, на всіх етапах життєвого циклу даних і йдеться не тільки про оперативні заходи, а й про регулярні аудити, тестування захисних систем та превентивні дії, які допомагають адаптуватися до нових загроз.

8.3. Джерела загроз інформаційній безпеці організації

Питання джерел загроз інформаційній безпеці є відправною точкою для формування будь-якої ефективної системи захисту організації. Сутність проблеми полягає в тому, що кіберзагрози не є статичними, а являють собою динамічний і багатовекторний ландшафт, який постійно еволюціонує, вимагаючи від менеджменту безперервної адаптації. У науковому розумінні джерела загроз поділяють на внутрішні (ендогенні) та зовнішні (екзогенні), причому їхня взаємодія часто призводить до найбільш руйнівних наслідків. Недостатньо зосереджувати увагу лише на зовнішніх атаках, оскільки, за статистикою, людський фактор (ненавмисні помилки або умисні дії інсайдерів) залишається одним із найкритичніших і найскладніших для контролю векторів проникнення.

Дослідження джерел загроз є необхідним для превентивного управління ризиками, оскільки дозволяє коректно розподілити ресурси захисту. Зовнішні джерела, такі як кіберзлочинні угруповання, державні суб'єкти чи конкуренти, застосовують складні технічні методи (наприклад, складні стійкі загрози, або APT-атаки) та соціальну інженерію. Водночас внутрішніми джерелами є недосконалість бізнес-процесів, слабкі політики безпеки та технічні вразливості (помилки конфігурації чи застаріле обладнання). Успішне управління інформаційною безпекою вимагає чіткого розуміння цих джерел, їхньої мотивації та потенційних цілей, що дозволяє організації перейти від реагування до стратегічного прогнозування та запобігання інцидентам.

Основні джерела, що впливають на інформаційну безпеку сучасних підприємств, можна класифікувати за такими ознаками:

1. Технічні та мережеві загрози:

– шкідливе програмне забезпечення (malware) – віруси, трояни, руткіти та інші програми, що руйнують або викрадають дані;

– програми-вимагачі (ransomware) – шифрування корпоративних файлів із вимогою викупу за розблокування;

– розподілені атаки відмови в обслуговуванні (DDoS) – перевантаження мережевих ресурсів для паралічу сервісів;

– ботнети і мережі зламаних пристроїв – масове використання компрометованих кінцевих точок для атак;

– атаки «людина-посередині» (MitM) – перехоплення і підміна комунікацій між системами;

– експлуатація вразливостей програм і «нульовий день» (zero-day) – використання невиправлених багів для проникнення;

– SQL-ін'єкції, XSS та інші вебвразливості – атаки на прикладний рівень для викрадення даних або виконання команд;

– крадіжка облікових даних і перехоплення сесій (credential theft, session hijacking);

– неправильні конфігурації хмарних сервісів (misconfiguration) – відкриті бакети / бази, слабкі політики доступу;

– API-зловживання – використання вразливих або відкритих інтерфейсів для несанкціонованого доступу.

2. Людський фактор та соціальна інженерія:

– фішинг і Spear-phishing – обманні листи / повідомлення для викачування паролів або виконання шкідливих дій;

– соціальна інженерія офлайн (телефонні шахрайства, pretexting) – маніпулювання працівниками для отримання доступу;

– помилки персоналу і ненавмисні витоки – випадкове відправлення конфіденційних файлів, неправильна публікація;

– зловмисні інсайдери – співробітники, які навмисно шкодять організації (крадіжка даних, саботаж);

– колаборація інсайдера зі зовнішніми акторами – організована внутрішньо-зовнішня змова.

3. Загрози, пов'язані з доступом і управлінням привілеями:

– неправильне надання або відсутність контролю над правами доступу (excessive privileges);

– викрадення привілейованих облікових записів (privileged account compromise);

– відсутність або порушення політик управління паролями та MFA-політик.

4. Зовнішні й організаційні ризики:

– корпоративне шпигунство і промислова розвідка – цілеспрямований збір конфіденційної інформації конкурентами або державними акторами;

– репутаційні кампанії і дезінформація – штучне поширення компрометуючої інформації з метою нашкодити іміджу;

– юридичні та нормативні ризики (non-compliance) – штрафи і санкції через невідповідність законам про захист даних;

– контракти з ненадійними постачальниками (third-party / vendor risk) – ризики через треті сторони та аутсорсинг.

5. Фізичні та інфраструктурні загрози:

– крадіжка або загублення пристроїв (ноутбуки, накопичувачі) – фізична втрата носія з чутливою інформацією;

– саботаж та фізичні атаки на дата-центри або офіси (включно з підірваними чи знищеними сервісами);

– відключення електроенергії, пожежа, повені – природні чи техногенні інциденти, що впливають на доступність;

– воєнні дії і обстріли – руйнування інфраструктури, перебої в роботі, підвищені ризики безпеки персоналу.

6. Загрози ланцюга постачання (supply-chain):

– вбудовані в поставлене ПЗ/обладнання бекдори та шкідливий код;

– компрометація постачальників, що має «ефект доміно» для клієнтів;

– неперевірені або піратські компоненти й бібліотеки (OSS supply risks).

7. Загрози для приватності та персональних даних:

– витоки персональних даних клієнтів і працівників – порушення *GDPR*/локальних законів, заподіяння шкоди репутації;

– неналежне зберігання/знищення даних, відсутність політик архівації та видалення.

8. Загрози, пов'язані з новими технологіями:

– уразливості IoT-пристроїв та ботнет-інфекції IoT;

– ризики хмарних платформ: недостатня сегментація, неправильні IAM-налаштування;

– атаки на промислові системи (ICS/SCADA) – загроза для виробництва і критичної інфраструктури;

– атаки на моделі машинного навчання: отруєння даних (data poisoning), adversarial attacks, викрадення моделей;

– загроза квантових обчислень у майбутньому – криптографічні ризики для наявних шифрів.

9. Фінансові та економічні загрози:

– шахрайство з фінансовими транзакціями, фальсифікація платіжних документів;

– крадіжка платіжних реквізитів, компрометація платіжних шлюзів;

– курсова та макроекономічна нестабільність, що впливає на безпеку постачань та інвестицій.

10. Операційні та процедурні загрози:

– недостатній або відсутній контроль змін (change management failures);

– неефективні резервні копії або їх відсутність (backup/restore failures);

– відсутність планів безперервності бізнесу і реакції на інциденти (BCP/DRP).

11. Соціально-політичні та геополітичні загрози:

– кібероперації та кібервійни, здійснювані державами або організованими групами;

– санкції, торгові обмеження, політичні рішення, що блокують доступ до сервісів чи ресурсів;

– протести, масові заворушення і соціальна нестабільність, що шкодять роботі й безпеці персоналу.

12. Репутаційні та інформаційні загрози:

– небезпечний витік внутрішньої інформації в ЗМІ чи соцмережах;

– цілеспрямовані кампанії компрометації – «smear campaigns», фальшиві новини.

13. Інші технічні та спеціалізовані загрози:

– побічні (side-channel) атаки, електромагнітне просочування даних;

– маніпуляція часовими мітками чи логами для приховування слідів;

– крадіжка або підміна криптографічних ключів, витік сертифікатів;

– використання несертифікованого або віддаленого коду (remote code execution) у вбудованих системах.

Кожна з цих загроз має різний вплив на рівень інформаційної безпеки (табл. 8.2), проте кожна з них потребує

детального вивчення та аналізу з огляду на те, що сучасні організації відчувають значний влив загроз, їхня діяльність залежить від уміння на них реагувати і зменшувати їхній вплив.

Таблиця 8.2

Рівень впливу загроз на інформаційну безпеку організації

№ з/п	Категорія загроз	Короткий опис	Рівень впливу	Причини
1	*2*	*3*	*4*	*5*
1	Технічні та мережеві загрози (malware, ransomware, DDoS тощо)	Прямі атаки на ІТ-інфраструктуру, шифрування/ викрадення даних, відмови сервісів.	Високий	Може призвести до миттєвих зупинок роботи, фінансових втрат і втрати даних.
2	Людський фактор і соціальна інженерія (фішинг, інсайдери)	Маніпуляції працівниками, випадкові або навмисні помилки і зловживання.	Високий	Більшість інцидентів починаються з помилок/обману людей; складно повністю технічно нейтралізувати.
3	Загрози доступу та управління привілеями (компрометація акаунтів)	Неналежне надання прав, викрадення привілейованих облікових записів.	Високий	Привілейований доступ дає можливість масштабних атак і прихованих маніпуляцій.
4	Зовнішні й організаційні ризики (шпигунство, non-compliance, vendor risk)	Діяльність третіх сторін, правові проблеми, контрагенти з низьким рівнем безпеки.	Високий	Вплив постачальників і правових санкцій може бути системним і довготривалим.
5	Фізичні та інфраструктурні загрози (крадіжка пристроїв, саботаж, війна)	Фізичні ушкодження, втрата носіїв, руйнування інфраструктури під час криз.	Високий	Фізичні пошкодження можуть повністю знеструмити ІТ-сервіси; воєнні ризики особливо критичні.
6	Загрози ланцюга постачання (supply-chain)	Компрометація ПЗ/обладнання у постачальників, приховані бекдори.	Середній–Високий	Уразливість через сторонні компоненти може вразити багато клієнтів одночасно.

Завершення табл. 8.2

1	*2*	*3*	*4*	*5*
7	Загрози для приватності та персональних даних (витоки PII)	Неправомірний доступ або розголошення персональних даних клієнтів/ співробітників.	Середній–Високий	Штрафи, репутаційні втрати і правові наслідки; залежить від масштабів витоку.
8	Загрози, пов'язані з новими технологіями (IoT, хмара, ML-атаки)	Уразливості IoT, хмарні misconfigurations, атаки на ML-моделі.	Середній	Нові вектори зростають; ефект залежить від ступеня впровадження таких технологій.
9	Фінансові та економічні загрози (шахрайство, компрометація платіжних каналів)	Маніпуляції з платіжними даними, шахрайські операції.	Середній	Безпосередньо впливають на грошові потоки; масштаб залежить від інтеграції платіжних систем.
10	Операційні та процедурні загрози (відсутність BCP, резервування)	Провали у процесах, незадовільні резервні копії, слабке управління змінами.	Середній	Знижують здатність організації відновитись та мінімізувати наслідки інцидентів.
11	Соціально-політичні та геополітичні загрози (кібервійни, санкції)	Масштабні національні/ міждержавні операції проти інфраструктури.	Середній–Високий	Може бути катастрофічним для критичної інфраструктури; залежить від географії й галузі.
12	Репутаційні та інформаційні загрози (дезінформація, витоки)	Поширення компрометуючої інформації, «smear campaigns».	Середній	Довготривалий вплив на довіру клієнтів і партнерів; складно швидко повернути репутацію.
13	Інші технічні та спеціалізовані загрози (side-channel, ключі)	Екзотичні атаки на крипто-ключі, маніпуляції логами, side-channel.	Низький–Середній	Частіше спеціалізовані, менш імовірні, але вразливі висококритичні системи.

В умовах війни та цифровізації бізнесу на всіх рівнях найбільш поширеними є саме екзогенні загрози (фактори):

1. Кібератаки та шкідливе ПЗ (ШПЗ):

– віруси, «трояни» та шифрувальники (Ransomware) – програми, призначені для знищення, модифікації або блокування даних з метою викупу;

– DDoS-атаки – перевантаження мережевих ресурсів великою кількістю запитів, що призводить до відмови в обслуговуванні легітимних користувачів;

– фішинг та соціальна інженерія – методи обману, спрямовані на виманювання облікових даних, паролів чи фінансової інформації від співробітників.

2. Дії конкурентів – промислове шпигунство, спрямоване на викрадення комерційної таємниці, технологічних рішень або стратегічних планів.

3. Природні та техногенні катастрофи – повені, пожежі, землетруси, а також аварії в енергомережах, що призводять до фізичного знищення інформаційної інфраструктури.

8.4. Напрями запобігання інформаційним ризикам в організації та управління ними

Інформаційні технології сьогодні визнаються чи не найголовнішим рушієм розвитку національної економіки. Вони формують конкурентні переваги держави та окремих компаній на міжнародних ринках, створюють можливості для зростання продуктивності та ефективності, а також дають змогу органам влади забезпечувати громадян сучасними та якісними послугами. Завдяки розвитку інформаційних систем приватний і державний сектори можуть успішніше реалізовувати свої місії, виконувати бізнес-функції та підтримувати стабільність діяльності в умовах зростаючої цифровізації.

Водночас інформаційні системи є об'єктами підвищеного ризику, оскільки вони піддаються як технічним, так і організаційним загрозам. Ці загрози можуть призвести до серйозних наслідків для компаній: втрати репутації, зриву бізнес-процесів, порушення місії та завдань підприємства, а також негативно позначитися на безпеці активів, клієнтів і партнерів. Для цього зловмисники використовують як відомі,

так і нові вразливості інформаційної інфраструктури, аби порушити конфіденційність, цілісність чи доступність даних.

Саме тому управління ризиками інформаційної безпеки розглядається як важливий напрям сучасного менеджменту. Воно об'єднує знання і досвід різних учасників організації – від керівників і стратегічних планувальників до спеціалістів з безпеки й технічних відділів. Такий підхід забезпечує комплексну оцінку можливих ризиків і дозволяє своєчасно впроваджувати адекватні заходи реагування, зберігаючи баланс між безпекою та ефективністю бізнесу.

Не менш важливим елементом вважається архітектура інформаційної безпеки, яка має бути інтегрована в загальну корпоративну архітектуру підприємства. Вона не лише включає технічні рішення, але й враховує чинні норми законодавства, внутрішні політики та міжнародні стандарти. Така архітектура фактично виконує роль стратегічної «дорожньої карти», яка переводить загальні цілі компанії у конкретні рішення, процеси і технології захисту. Це створює умови для цілісного, узгодженого та довгострокового підходу до побудови інформаційної безпеки, яка є фундаментом стабільного розвитку сучасної організації.

Вимоги до забезпечення інформаційної безпеки реалізуються через управлінські, організаційні, операційні та технічні механізми, які спрямовані на комплексний захист інформаційних ресурсів організації. Управління ризиками в цій сфері включає визначення критеріїв для виявлення загроз, проведення оцінки їх імовірності та масштабів наслідків, аналіз ступеня небезпеки для бізнес-процесів, формування заходів реагування, а також систематичний перегляд і вдосконалення обраних рішень у міру зміни зовнішнього та внутрішнього середовища. Такий підхід дає можливість адаптувати систему інформаційної безпеки до нових викликів і підвищувати її стійкість.

Розв'язання проблем управління ризиками може бути реалізовано шляхом побудови чіткої структури, яка узгоджується зі стратегічними цілями організації. Необхідно визначати ті сфери діяльності, де швидке та ефективне реагування на ризики є критично важливим для досягнення місії компанії. У межах цієї структури слід закріплювати вимоги

до інформаційної безпеки, що формуються відповідно до загальної політики управління ризиками. Важливо також трансформувати вимоги у конкретні дії та інструменти захисту, які застосовуються як до ІТ-інфраструктури, так і до операційних процесів. При цьому управлінські, технічні та організаційні заходи мають бути чітко розподілені між відповідальними рівнями, що дозволить уникнути дублювання функцій і забезпечить ефективну координацію.

Документування усіх рішень із питань управління ризиками на різних рівнях управлінської структури має важливе значення, оскільки створює основу для прозорості та підзвітності. Це допомагає не лише фіксувати поточний стан безпеки, а й слугувати базою для подальшого аналізу, вдосконалення та прийняття більш ефективних рішень. У результаті формується система, яка поєднує стратегічні завдання, технологічні можливості та реальні потреби бізнесу, що створює умови для довготривалого захисту інформаційних активів.

Управління інформаційною безпекою організації – це системний, багаторівневий та безперервний процес, спрямований на захист інформаційних ресурсів, технологій та інфраструктури підприємства від внутрішніх і зовнішніх загроз, що можуть призвести до порушення конфіденційності, цілісності, доступності та правомірності використання інформації. Воно охоплює формування політики безпеки, визначення відповідальності та повноважень, застосування організаційних, правових, технічних і програмних засобів захисту, а також постійний моніторинг і вдосконалення системи.

Це поняття передбачає не лише використання сучасних технологій і методів захисту, а й управлінський підхід до мінімізації ризиків, пов'язаних з діяльністю персоналу, зовнішніми кібератаками чи форс-мажорними обставинами. Ефективне управління інформаційною безпекою інтегрується в загальну стратегію організації, узгоджується з її бізнес-цілями, враховує вимоги законодавства та міжнародних стандартів і передбачає створення адаптивної системи реагування на нові загрози. Таким чином, воно виступає важливим інструментом забезпечення конкурентоспроможності, стійкості та довіри з боку клієнтів, партнерів і держави.

Основні етапи управління подано в табл. 8.3.

Таблиця 8.3

Етапи управління інформаційною безпекою організації

Етап	Зміст і характеристика	Очікуваний результат
1. Ідентифікація інформаційних активів	Визначення всіх інформаційних ресурсів організації (бази даних, документи, програмне забезпечення, технічні системи, персонал, що працює з даними).	Формування переліку критично важливих активів, що потребують захисту.
2. Аналіз загроз і ризиків	Виявлення потенційних внутрішніх і зовнішніх загроз (кібератаки, витоки інформації, технічні збої, людський фактор, воєнні ризики). Оцінка ймовірності та масштабу можливих наслідків.	Карта ризиків із визначенням рівня небезпеки кожного фактора.
3. Розробка політики безпеки	Створення стратегічних і нормативних документів, які регламентують порядок обробки та захисту інформації, доступу до систем, відповідальність співробітників.	Затверджена політика інформаційної безпеки, що інтегрується в загальну стратегію управління.
4. Вибір і впровадження засобів захисту	Використання програмних, технічних та організаційних інструментів (системи контролю доступу, антивірусні програми, шифрування, навчання персоналу).	Зниження вразливості інформаційної системи та підвищення рівня захищеності активів.
5. Моніторинг і контроль	Постійне відстеження стану інформаційних систем, фіксація спроб несанкціонованого доступу, аналіз журналів подій, перевірка ефективності політики безпеки.	Виявлення відхилень у реальному часі та оперативне реагування на інциденти.
6. Реагування на інциденти	Розробка планів дій у випадку кібератак, витоків чи пошкоджень даних, включно з резервним копіюванням і відновленням роботи.	Мінімізація наслідків інцидентів і швидке відновлення стабільного функціонування.
7. Аудит та вдосконалення системи	Регулярні перевірки політики, технологій та процедур безпеки, виявлення недоліків і впровадження нових підходів (наприклад, з урахуванням міжнародних стандартів ISO/IEC 27001).	Підвищення стійкості системи безпеки, адаптація до нових умов та загроз.

Ефективне управління інформаційною безпекою має на меті створення системи, здатної гарантувати захист усіх даних організації на всіх етапах їх життєвого циклу. Йдеться не лише про запобігання зовнішнім загрозам, а й про усунення внутрішніх ризиків, що можуть виникати внаслідок людського фактора, організаційних помилок чи технічних збоїв. Сучасні компанії працюють у середовищі, де інформаційні потоки є основою управління, тому їхня безпека визначає стійкість бізнес-процесів, довіру партнерів і клієнтів, а також конкурентоспроможність на ринку.

Основна мета такого управління полягає у створенні цілісної політики, яка поєднує правові, організаційні, технічні та адміністративні заходи, спрямовані на збереження конфіденційності, цілісності та доступності інформації. Завдяки ефективному управлінню інформаційною безпекою організації можуть знизити ймовірність кіберінцидентів, мінімізувати фінансові втрати в разі атак чи витоків даних, а також гарантувати безперервність своєї діяльності навіть за умов кризових ситуацій, таких як війна, кіберзагрози чи масштабні техногенні ризики.

Основні напрями запобігання ризикам, що пов'язані з інформаційною безпекою організації, наведено на рис. 8.2.

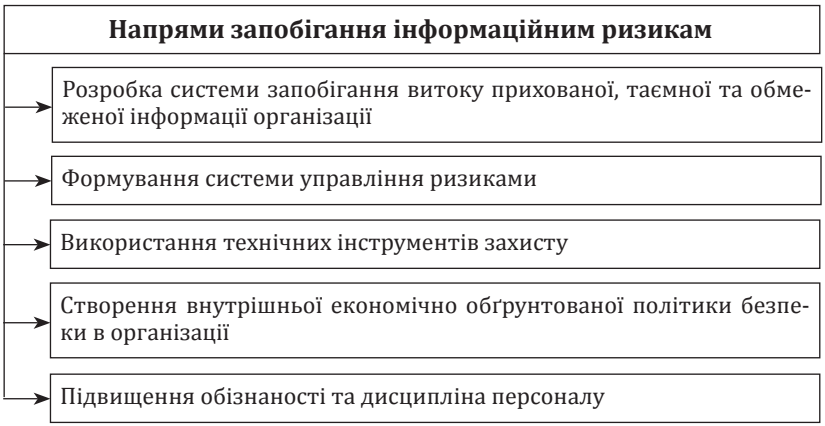


Рис. 8.2. Основні напрями запобігання інформаційним ризикам організації

Доцільно більш детально розглянути провідні напрями запобігання інформаційним ризикам в організаціях:

1. Розробка системи запобігання витоку прихованої або обмеженої інформації. Будь-яка організація працює з даними, які мають критичне значення для її функціонування, тому важливо створювати механізми, які не дозволять стороннім особам отримати доступ до такої інформації. Це може включати багаторівневий контроль доступу, застосування сучасних засобів шифрування, а також моніторинг використання інформаційних ресурсів. Такий підхід допомагає знизити ризик витоку даних і зберегти конкурентні переваги компанії.

2. Формування системи управління ризиками. Ефективне управління інформаційною безпекою базується на постійній оцінці та контролі ризиків. Важливо не лише виявляти можливі загрози, а й будувати систему, яка надає змогу прогнозувати їх появу та визначати найбільш уразливі місця. Для цього застосовують внутрішні аудити, аналіз ризиків, розробку планів реагування на надзвичайні ситуації. Завдяки цьому організація може діяти на випередження і мінімізувати можливі наслідки атак чи збоїв.

3. Використання технічних інструментів захисту. Технічна складова відіграє основну роль у забезпеченні інформаційної безпеки; це не лише антивірусні програми чи міжмережеві екрани, а й сучасні системи виявлення аномальної активності, резервного копіювання та захисту від DDoS-атак. Їхнє завдання – створити багаторівневий бар'єр, який унеможливлює як зовнішнє, так і внутрішнє втручання. Використання новітніх технологій допомагає реагувати на загрози оперативніше та з меншими витратами.

4. Створення економічно обґрунтованої політики безпеки. Фінансовий аспект у сфері безпеки часто недооцінюють, проте саме він дає можливість забезпечити оптимальний баланс між витратами та результатами. Не кожна компанія може дозволити собі дорогі системи, тому важливо правильно розставляти пріоритети: які загрози є найнебезпечнішими і які заходи потрібно профінансувати першочергово. Економічний підхід допомагає уникати надмірних витрат і водночас підтримувати високий рівень захисту.

5. Підвищення обізнаності та дисципліни персоналу. Жодна, навіть найдорожча система безпеки, не буде ефективною, якщо працівники не розуміють своєї ролі в її забезпеченні, тому важливо проводити навчання, тренінги, інструктажі, які формують у колективі культуру безпеки. Працівники мають знати, як правильно поводитися з конфіденційною інформацією, розпізнавати шахрайські схеми чи підозрілі дії. Коли люди стають відповідальними за безпеку так само, як і технічні системи, ризики зменшуються в рази.

Організація може застосовувати різні форми навчання персоналу для підвищення рівня інформаційної безпеки. Основними видами можна вважати:

– інструктажі та семінари – регулярні роз'яснювальні заняття, на яких працівникам пояснюють правила поводження з конфіденційною інформацією, політику безпеки організації та особливості реагування на підозрілі ситуації;

– онлайн-курси та вебінари – зручна форма навчання, яка надає можливості персоналу отримувати знання в будь-який час, включати сучасні кейси з інформаційної безпеки та приклади кібератак;

– тренінги з моделювання інцидентів – практичні заняття, під час яких імітуються різні сценарії загроз (наприклад, фішинг, витік даних, кібератака), щоби співробітники могли відпрацьовувати алгоритми дій у реальних умовах;

– психологічні тренінги та коучинг – спрямовані на формування культури відповідальності та уважності серед працівників, а також розвиток навичок критичного мислення;

– тестування знань та атестації – контрольні перевірки знань персоналу з основ інформаційної безпеки, що допомагають виявляти слабкі місця та планувати подальші освітні заходи;

– корпоративні інформаційні кампанії – розповсюдження пам'яток, плакатів, внутрішніх бюлетенів чи коротких відеоінструкцій для нагадування про основні правила безпеки;

– індивідуальне наставництво – залучення досвідчених працівників для консультування новачків щодо безпечної поведінки в інформаційному просторі.

Вибір стратегії управління інформаційними ризиками має неабияке значення для ефективності діяльності

будь-якої організації, адже він прямо впливає на здатність компанії захищати свої дані, підтримувати стабільність бізнес-процесів і формувати довіру серед клієнтів та партнерів. Продумана стратегія дозволяє не лише знижувати ймовірність виникнення інцидентів, але й мінімізувати їхні можливі наслідки, забезпечуючи безперервність роботи підприємства навіть у кризових умовах.

Крім того, стратегія управління ризиками створює основу для формування системного підходу до інформаційної безпеки, що охоплює технічні, організаційні, правові та кадрові заходи. Вона допомагає інтегрувати безпекові аспекти у загальну корпоративну культуру, зробити їх частиною повсякденної діяльності персоналу та управлінських рішень. Суттєво, що правильний вибір стратегії підсилює конкурентоспроможність організації на ринку, адже захищеність інформаційних ресурсів підвищує довіру інвесторів, сприяє укладенню нових угод і зміцнює репутацію компанії у довгостроковій перспективі.

Крім того, важливими напрямами запобігання інформаційним ризикам сучасних організацій та управління ними є:

– впровадження політики резервного копіювання та відновлення даних у разі збоїв чи атак;

– застосування систем багаторівневої автентифікації користувачів (MFA);

– регулярне оновлення програмного забезпечення та усунення вразливостей;

– аудит інформаційних систем і незалежна перевірка безпеки;

– сегментація мережі та обмеження доступу до критичних ресурсів;

– моніторинг кіберзагроз у режимі реального часу;

– впровадження систем виявлення та реагування на інциденти (SIEM, SOC);

– забезпечення юридичного супроводу та відповідності стандартам (compliance: ISO/IEC 27001, GDPR тощо);

– формування внутрішніх кодексів етики та правил використання інформації;

– розробка системи внутрішнього контролю за діями персоналу;

– взаємодія з державними структурами та правоохоронними органами у сфері кіберзахисту;

– використання шифрування даних під час їх зберігання та передачі;

– контроль доступу до мобільних пристроїв і захист корпоративних мереж у віддаленій роботі;

– застосування штучного інтелекту та машинного навчання для прогнозування атак;

– проведення стрес-тестування інформаційних систем (penetration testing);

– створення кризових планів реагування на кібератаки та катастрофи;

– інвестиції в кіберосвіту та підготовку персоналу до дій у нестандартних ситуаціях;

– формування культури відповідальності за інформаційну безпеку на всіх рівнях управління.

Питання для самоконтролю

1. Що таке інформаційна безпека організації та які її ключові складники?
2. Які принципи забезпечення інформаційної безпеки є найбільш важливими для сучасних підприємств?
3. Які об'єкти та суб'єкти інформаційної безпеки можна виділити в діяльності організації?
4. Як класифікують загрози інформаційній безпеці та які з них є найбільш актуальними в умовах воєнного стану?
5. Яку роль відіграє правове регулювання у сфері інформаційної безпеки організації?
6. У чому полягає значення управління інформаційними ризиками для сталого функціонування бізнесу?
7. Які основні методи та інструменти захисту інформації застосовують сучасні організації?
8. Як людський фактор впливає на рівень інформаційної безпеки та якими способами можна мінімізувати цей вплив?
9. Які етапи управління інформаційною безпекою організації можна виділити?
10. Чому важливо інтегрувати інформаційну безпеку в загальну систему корпоративної безпеки підприємства?

Тестові завдання

1. Під інформаційною безпекою організації розуміють:

а) виключно технічний захист від хакерських атак і вірусних програм;

б) комплексну систему заходів, що забезпечує конфіденційність, цілісність і доступність інформаційних ресурсів організації;

в) використання лиш антивірусного захисту для комп'ютерів і серверів;

г) лише дотримання трудової дисципліни працівниками компанії.

2. Які є основні цілі забезпечення інформаційної безпеки?

а) Тільки обмеження доступу до інформації для сторонніх осіб;

б) забезпечення цілісності, конфіденційності та доступності даних для авторизованих користувачів;

в) виключно захист серверного обладнання від пошкодження;

г) тільки регулярний контроль паролів у корпоративних системах.

3. Яку роль відіграє керівництво в системі інформаційної безпеки?

а) Лише забезпечує фінансування технічних засобів безпеки для ІТ-відділу;

б) формує стратегію і політику безпеки, контролює виконання рішень та відповідає за стратегічні напрями розвитку системи;

в) займається виключно юридичними питаннями, пов'язаними з інформацією;

г) має лише формальну функцію – підписання документів і наказів.

4. Які основні категорії загроз інформаційній безпеці виділяють?

а) Тільки зовнішні загрози, пов'язані з кібератаками чи економічною нестабільністю;

б) внутрішні, зовнішні та комбіновані загрози, що можуть поєднувати обидва джерела;

в) виключно природні фактори, як-от стихійні лиха чи пожежі;

г) лише організаційні проблеми, зумовлені управлінськими помилками.

5. Який принцип вважається основним у сфері інформаційної безпеки?

а) Принцип економічної вигоди, за яким витрати на безпеку мають бути мінімальними;

б) принцип законності, що вимагає дотримання національного та міжнародного законодавства;

в) принцип випадковості, де захист формується залежно від непередбачуваних загроз;

г) принцип автоматизації, який зводиться до встановлення технічних систем без втручання людини.

6. Які засоби забезпечення інформаційної безпеки застосовуються на практиці?

а) Виключно програмні засоби, зокрема антивірусні системи;

б) поєднання програмних, технічних, адміністративних, правових та етичних методів захисту;

в) лише морально-етичні підходи, пов'язані з корпоративною культурою поведінки;

г) тільки апаратні засоби, зокрема системи контролю доступу та сервери.

7. Підвищення обізнаності персоналу має вирішальне значення:

а) тому що це допомагає скоротити витрати компанії на дорогі технічні системи;

б) адже навчені працівники стають активними учасниками процесу захисту і вчасно реагують на загрози;

в) бо персонал завжди є головною причиною порушень і ризиків у сфері інформації;

г) оскільки проведення навчань є модною вимогою сучасних компаній і стандартів.

8. Об'єктами системи інформаційної безпеки є:

а) Виключно технічні пристрої, сервери та комп'ютерна техніка;

б) інформаційні ресурси, персонал, інфраструктура, бізнес-процеси і навіть репутація компанії;

в) тільки спеціалізовані приміщення, зокрема серверні кімнати;

г) виключно програмне забезпечення та бази даних.

9. Що відноситься до адміністративних методів інформаційної безпеки?

а) Використання антивірусного програмного забезпечення для робочих місць;

б) розробка правил взаємодії з інформацією, розподіл повноважень і контроль доступу до даних;

в) встановлення відеоспостереження і контроль за входом до приміщень;

г) виключно створення та підтримка програмного коду.

10. Чому управління ризиками інформаційної безпеки є безперервним процесом?

а) З часом ризики зникають і втрачають актуальність;

б) загрози постійно змінюються, тому необхідний регулярний аналіз і адаптація системи;

в) так вимагає законодавство у сфері захисту інформації;

г) безперервний аудит вигідний лише ІТ-відділу компанії.

Практичні завдання

Завдання 1.

ТОВ «Альфа-Софт» займається розробкою програмного забезпечення для банківського сектору. У компанії працює понад 200 осіб, більшість з яких мають доступ до клієнтських баз даних. В умовах війни підприємство перевело частину співробітників на дистанційний формат роботи, що призвело до активного використання хмарних сервісів. Протягом останніх двох місяців виявлено кілька спроб несанкціонованого доступу до внутрішніх систем компанії, а один зі співробітників повідомив про отримання підозрілого електронного листа з вкладенням, яке могло містити шкідливий код. Додатковою проблемою є відсутність у компанії єдиної політики керування паролями та багатофакторної автентифікації.

1. Оцініть, які основні ризики для інформаційної безпеки має компанія.

2. Визначте їх наслідки для клієнтів і самої організації.

3. Запропонуйте комплекс управлінських і технічних заходів для їх усунення.

Завдання 2.

Промислове підприємство «Бета-Маш» має власний відділ досліджень і розробок, де створюються унікальні інженерні рішення. У компанії працює близько 500 осіб, але рівень плинності кадрів останнім часом суттєво зріс. Під час аудиту виявлено, що кілька працівників відділу ІТ використовували персональні флешнакопичувачі для перенесення даних, а один зі співробітників завантажував конфіденційні файли на особисту електронну пошту. Також виявлено факти поширення внутрішньої документації у професійних спільнотах. Деякі працівники, що залишають компанію, переходять у конкурентні організації, маючи доступ до напрацювань підприємства.

1. Визначте основні вразливості системи інформаційної безпеки підприємства.

2. З'ясуйте, які внутрішні ризики є найнебезпечнішими.

3. Запропонуйте заходи кадрового, організаційного і технічного характеру для зменшення загроз витоку інформації.

Завдання 3.

Організація «Гамма-Телеком» є провайдером послуг інтернет-зв'язку та обслуговує понад 50 тисяч клієнтів у різних регіонах України. Через регулярні обстріли енергетичної інфраструктури та тривалі відключення електроенергії збої в роботі серверів і центрів обробки даних стають систематичними. Це призводить до порушення безперервності бізнес-процесів, затримки в обслуговуванні клієнтів і зниження довіри до компанії. При цьому резервні джерела живлення є лише в центральному офісі, а регіональні філії не обладнані відповідними системами. Інформаційна інфраструктура не має достатньо надійної системи резервного копіювання даних, і є ризик втрати критично важливої клієнтської інформації.

1. Проаналізуйте ситуацію з позицій інформаційної безпеки та безперервності бізнесу.

2. З'ясуйте, які загрози стоять перед компанією в умовах воєнного стану.

3. Визначте, які стратегічні та тактичні кроки варто впровадити, щоб мінімізувати ризики і забезпечити стабільність діяльності.

ТЕМА 9
МЕНЕДЖМЕНТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ

9.1. Сутність екологічної безпеки та її місце в системі корпоративної безпеки

9.2. Складові системи екологічної безпеки організації

9.3. Інструменти та стратегія менеджменту екологічної безпеки

Основні поняття і терміни: екологія, організація, екологічна безпека, менеджмент екологічної безпеки, природне середовище, глобальні виклики, техногенні катастрофи, природоохоронна діяльність, природний ресурс, загрози забруднення, ризики природних катастроф.

9.1. Сутність екологічної безпеки та її місце в системі корпоративної безпеки

Екологічна безпека є невід'ємною складовою сталого розвитку будь-якої організації, оскільки забезпечує гармонійне співіснування господарської діяльності з природним середовищем. В умовах сучасних глобальних викликів, таких як зміна клімату, вичерпання природних ресурсів, воєнні дії та техногенні катастрофи, питання екологічної безпеки набувають особливого значення. Організація, яка ігнорує екологічний фактор, ризикує не лише втратити економічну стабільність, а й зазнати репутаційних і правових втрат.

Сутність екологічної безпеки полягає у створенні системи заходів, спрямованих на попередження, зниження та ліквідацію негативного впливу виробничої чи іншої діяльності на довкілля. Вона охоплює як внутрішні процеси управління природоохоронною діяльністю, так і зовнішню взаємодію з державними органами, міжнародними інституціями та місцевими громадами. Тож екологічна безпека виступає не лише захисним бар'єром від потенційних загроз, а й стратегічним ресурсом, який визначає конкурентоспроможність і перспективи розвитку організації у довгостроковій перспективі.

Поняття «екологічна безпека» уперше почало вживатися у США в 1974 році в роботі генерала М. Тейлора «Законні вимоги національної безпеки», де автор акцентував увагу на тому, що головні виклики для безпеки держави формуються не лише у військовій площині, а й у невійськових сферах. Уже через кілька років, у 1978 році, президент аналітичного інституту «Worldwatch» Л. Браун у статті «Переглянути визначення національної безпеки» визначив серед ключових загроз не тільки енергетичну кризу, але й інфляцію, зростання міграційних потоків та екологічні ризики. Надалі, у 90-х роках XX століття, американські політологи дійшли висновку, що виснаження природних ресурсів і деградація довкілля посилюють соціально-економічні диспропорції, стаючи фактором, що впливає на стабільність розвитку суспільства. Як наслідок, поняття «екологічна безпека» закріпилося в офіційній концепції національної безпеки США.

У широкому розумінні екологічна безпека означає захист громадян і суспільства від небезпек, пов'язаних із впливом на довкілля, та є необхідною передумовою реалізації фундаментального права людини на безпечне і здорове середовище існування. Вона виступає важливим елементом національної, а подекуди й міжнародної безпеки, адже проблеми екології не мають кордонів. Як соціальна категорія, екологічна безпека формується у системі суспільних відносин і вважається пріоритетною цінністю під час взаємодії людини з природою, використання небезпечних речовин або технологій, що можуть завдати шкоди як природному середовищу, так і самому суспільству.

Досліджуючи сутність цього поняття, його можна розглядати на різних рівнях – від локального до глобального. Локальні проблеми можуть поступово поширюватися на регіональний і навіть світовий масштаб, а наслідки сучасних негативних екологічних процесів у майбутньому здатні стати незворотними. Це означає, що екологічна безпека завжди обмежена часом і простором, а своєчасні дії у цій сфері є запорукою збереження як природних ресурсів, так і умов існування людства.

Поняття екологічної безпеки не має єдиного визначення, адже воно багатогранне та охоплює різні підходи.

Найчастіше її трактують як стан захищеності від потенційних або реальних екологічних загроз, коли шкода довкіллю мінімізована, а природні ресурси використовуються раціонально. Йдеться про таку ситуацію, коли забезпечено належний рівень екологічного середовища, зведено до мінімуму антропогенний вплив на біосферу, відсутні загрози природним об'єктам, а екологічні ризики знижено до прийнятного рівня. Водночас екологічна безпека означає здатність відновлювати природно-ресурсний потенціал та підтримувати умови, необхідні для якісної життєдіяльності населення. Вона також передбачає задоволення екологічних потреб суспільства й гарантію проживання у здоровому та чистому середовищі.

Розглядаючи екологічну безпеку на рівні підприємства, доцільно виокремити дві взаємопов'язані позиції. Перша з них стосується захисту довкілля та населення від негативного впливу виробничої діяльності. Викиди в атмосферу, скиди у водні об'єкти, утворення відходів, порушення ландшафтів чи шкідливі умови праці – усе це приклади екологічних загроз, які можуть мати як соціальні, так і економічні наслідки. До них додається високий рівень зношеності обладнання, використання застарілих технологій, а також недостатнє фінансування природоохоронних заходів. Порушення технологічної дисципліни чи нехтування екологічними аспектами в управлінських рішеннях лише посилює ці проблеми. Як наслідок підприємство стикається з додатковими витратами: виплатою компенсацій, пільгами для працівників, сплатою зборів за спеціальне використання ресурсів чи за забруднення навколишнього середовища.

Друга позиція стосується захищеності самого підприємства від зовнішніх екологічних загроз. Тут вирішальну роль відіграють природно-кліматичні та ресурсні умови, відсутність стихійних лих і техногенних аварій, а також дотримання екологічних нормативів іншими суб'єктами господарювання. Для аграрного сектору, лісового господарства чи підприємств, що залежать від природних ресурсів, критичне значення має стабільність природного середовища; для сфери туризму та рекреації – чистота повітря, вода і збереження екосистем. Тому екологічна безпека підприємства у цьому вимірі асоціюється з доступом до якісних ресурсів, відсутністю

зовнішнього забруднення, наявністю ефективної правової бази та системи державного і корпоративного контролю.

У такому контексті екологічна безпека підприємства набуває двостороннього характеру: з одного боку, вона вимагає зниження негативного впливу на довкілля і створення безпечних умов праці, з іншого – передбачає стійкість підприємства до зовнішніх екологічних загроз, що формують середовище його функціонування. Баланс цих підходів дозволяє не тільки уникати штрафів та зменшувати витрати, а й створювати додаткові конкурентні переваги завдяки іміджу екологічно відповідальної компанії.

Отже, **екологічна безпека** розглядається як складна соціально-економічна та правова категорія, що поєднує завдання збереження природного середовища, захисту життя та здоров'я населення, а також підтримання стабільного розвитку підприємств і держави загалом. Її сутність полягає у створенні таких умов, за яких антропогенний вплив на довкілля не перевищує екологічно допустимих меж, забезпечується відтворення природно-ресурсного потенціалу та формуються належні умови для життєдіяльності людини.

Екологічна безпека вимагає системного підходу, де враховуються як внутрішні чинники діяльності підприємств (технології, виробничі процеси, організація праці), так і зовнішні умови (стан довколишнього природного середовища, наявність загроз природного чи техногенного походження). Вона є базисом сталого розвитку, оскільки поєднує економічні інтереси зі соціальною відповідальністю та потребою збереження довкілля для нинішніх і майбутніх поколінь.

Менеджмент екологічної безпеки – це система управлінських заходів, спрямованих на ідентифікацію, оцінку та мінімізацію екологічних ризиків у діяльності підприємств і організацій. Він включає планування, організацію, контроль і регулювання процесів, що пов'язані з охороною довкілля, раціональним використанням природних ресурсів та впровадженням екологічно безпечних технологій.

Цей напрям менеджменту поєднує економічні, правові, технічні та соціальні інструменти для забезпечення збалансованого розвитку підприємства без шкоди для навколишнього середовища і здоров'я населення. Його метою

є створення умов, за яких виробнича діяльність відповідає чинним екологічним нормам і стандартам, сприяє формуванню позитивного іміджу компанії та підвищує її конкурентоспроможність як на внутрішньому, так і на міжнародному ринку.

Роль екологічної безпеки у структурі корпоративної безпеки є надзвичайно важливою, оскільки вона забезпечує гармонійне поєднання економічної діяльності організації з вимогами охорони довкілля та захисту здоров'я населення. У сучасних умовах саме екологічний аспект визначає рівень соціальної відповідальності бізнесу, його здатність дотримуватися принципів сталого розвитку та формувати позитивний імідж серед партнерів і клієнтів. Порушення екологічної безпеки може призвести не лише до штрафів і санкцій, а й до значних фінансових втрат через зниження довіри з боку суспільства та інвесторів.

У структурі корпоративної безпеки екологічна складова виконує функцію своєрідного захисного бар'єра, що мінімізує ризики техногенних аварій, забруднення навколишнього середовища та пов'язаних із цим репутаційних і правових наслідків. Вона інтегрується з фінансовою, кадровою та інформаційною безпекою, оскільки екологічні ризики впливають на всі інші елементи корпоративної діяльності. Приміром, неефективне управління природоохоронними процесами може збільшити витрати підприємства, спровокувати конфлікти з громадськістю або викликати відтік кваліфікованих кадрів через небезпечні умови праці.

Суб'єктами менеджменту екологічної безпеки виступають усі учасники, які прямо чи опосередковано впливають на організацію природоохоронних заходів і контролюють дотримання екологічних стандартів у діяльності підприємства. Їх можна умовно поділити на кілька основних груп:

– держава в особі органів законодавчої та виконавчої влади. Вони формують нормативно-правову базу, встановлюють екологічні стандарти, правила природокористування та контролюють їх дотримання. Сюди належать Міністерство захисту довкілля та природних ресурсів, Державна екологічна інспекція, органи місцевого самоврядування, що відповідають за екологічну політику на регіональному рівні;

– власники підприємств, керівники і топменеджмент. Вони ухвалюють стратегічні рішення щодо пріоритетів екологічної безпеки, визначають політику використання ресурсів, виділяють фінансування на природоохоронні заходи, впроваджують нові технології та контролюють відповідність діяльності вимогам законодавства;

– структурні підрозділи підприємств (екологічні служби, відділи охорони праці, служби технічного контролю, юридичні відділи). Саме вони відповідають за реалізацію екологічної політики на практиці: організовують моніторинг викидів і скидів, здійснюють паспортизацію відходів, впроваджують системи екологічного менеджменту, проводять навчання персоналу;

– працівники організації, які безпосередньо виконують виробничі операції. Від їхнього рівня обізнаності, дисципліни та відповідального ставлення залежить ефективність системи екологічної безпеки;

– зовнішні інститути – міжнародні організації, неурядові та громадські об'єднання, науково-дослідні установи, інвестори. Вони впливають на формування стандартів, здійснюють експертизи, аудити, надають фінансову й технічну підтримку, а також можуть виступати «сторожовими псами» у питаннях екологічної відповідальності бізнесу.

Основні об'єкти менеджменту екологічної безпеки організації подано на рис. 9.1.

Серед наведених об'єктів екологічної безпеки ключове значення мають технологічні процеси та обладнання, оскільки саме вони є головним джерелом викидів, відходів і виробничих ризиків, що безпосередньо впливають на стан довкілля та здоров'я працівників. Не менш важливими об'єктами виступають природні ресурси, які залучаються у виробничу діяльність, адже їх раціональне використання визначає сталість функціонування підприємства та можливості для подальшого розвитку. Вирішальну ж роль відіграють працівники організації, оскільки рівень їхньої безпеки, професійного захисту та готовності дотримуватися екологічних норм прямо впливає на загальний рівень екологічної відповідальності та конкурентоспроможність компанії. Саме ці об'єкти формують основу екологічної безпеки та визначають її ефективність у довгостроковій перспективі.

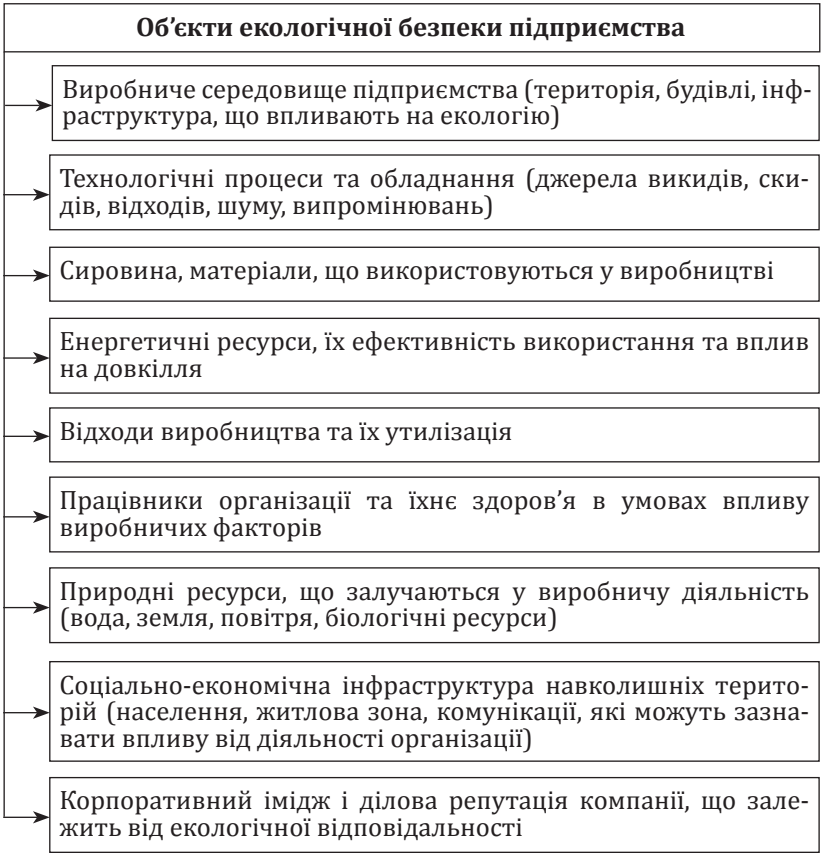


Рис. 9.1. Перелік основних об'єктів
екологічної безпеки організації

Збереження цих об'єктів вимагає впровадження системи екологічного менеджменту, яка поєднує контроль, регулювання та профілактику ризиків. Це дає змогу не лише знижувати витрати, пов'язані зі забрудненням чи компенсаційними виплатами, а й створює конкурентні переваги на ринку за рахунок дотримання екологічних стандартів. У результаті організація формує більш стійку модель розвитку, що поєднує економічну вигоду з екологічною та соціальною відповідальністю.

Функції екологічної безпеки організації можна розглядати як сукупність завдань і напрямів діяльності, що забезпечують гармонійне поєднання господарської діяльності та охорони довкілля. Вони спрямовані на зменшення негативного антропогенного впливу, дотримання екологічних стандартів і норм, формування умов для сталого розвитку та захисту життя і здоров'я людей. До основних функцій належать:

– превентивна – полягає у завчасному виявленні потенційних екологічних ризиків і загроз та розробці механізмів їх попередження;

– регуляторна – забезпечує дотримання вимог законодавства, міжнародних угод та внутрішніх стандартів підприємства у сфері охорони довкілля;

– контрольна – включає моніторинг стану природних ресурсів, рівня забруднення, використання енергії та ресурсів, контроль за виконанням екологічних заходів;

– відновлювальна – спрямована на відтворення та підтримку природно-ресурсного потенціалу, проведення рекультиваційних і відновлювальних робіт;

– інноваційна – полягає у впровадженні новітніх технологій та екологобезпечних методів виробництва;

– соціальна – забезпечує захист життя та здоров'я працівників і населення, створення безпечних умов праці та проживання;

– економічна – пов'язана зі зниженням витрат, що виникають через штрафи, компенсації, ліквідацію наслідків аварій та забруднень, а також з підвищенням конкурентоспроможності завдяки екологічній репутації;

– комунікаційна – налагоджує взаємодію підприємства з державними органами, місцевими громадами, міжнародними інституціями у сфері екологічної безпеки.

9.2. Складові системи екологічної безпеки організації

Екологічна безпека у сучасному розумінні позиціонується як стан довкілля та умов життєдіяльності, що забезпечують гармонію між природними процесами та господарською діяльністю людини. Вона передбачає підтримання

екологічної рівноваги, охорону біосфери, атмосфери, гідросфери, літосфери та космічного простору, збереження біорізноманіття і природних ресурсів, а також гарантію здоров'я та безпеки населення. Сутність цього поняття криється в тім, що воно має бути спрямоване як на стабільний розвиток у нормальних умовах, так і на здатність реагувати на кризові чи катастрофічні ситуації. Важливу роль відіграє прогнозування можливих подій, моделювання сценаріїв ризиків та розробка управлінських рішень, які дозволяють запобігати загрозам або мінімізувати їхні наслідки.

Система екологічної безпеки організації – це цілісна структура управління, яка поєднує механізми моніторингу, регулювання та реалізації природоохоронних заходів. Вона ґрунтується на трьох ключових складових: контроль, що передбачає систематичний нагляд за станом довкілля та відповідність діяльності підприємства екологічним стандартам; регулювання, яке включає правові, організаційні та економічні інструменти впливу для забезпечення дотримання екологічних норм; а також впровадження заходів безпеки, які охоплюють як традиційні методи охорони природи, так і розвиток інноваційних рішень, зокрема альтернативних джерел енергії та екологічно чистих технологій (табл. 9.1). Такий підхід допомагає сформувати багаторівневу і динамічну систему, здатну функціонувати в умовах змінного середовища та забезпечувати стійкість організації у довгостроковій перспективі.

Складова контроль у системі екологічної безпеки є однією з найважливіших, адже вона забезпечує постійне спостереження за станом довкілля та відповідність діяльності підприємства вимогам законодавства та екологічним стандартам. Контроль виконує роль «зворотного зв'язку» – він дає можливість виявляти відхилення від норм і своєчасно застосовувати коригувальні заходи, що знижує ризик виникнення екологічних катастроф чи штрафних санкцій.

Передусім контроль передбачає моніторинг природного середовища – вимірювання рівня викидів у повітря, скидів у водойми, утворення та утилізації відходів, рівня шуму чи радіації. Цей напрям вимагає використання сучасних приладів, лабораторних аналізів та інформаційних систем,

Таблиця 9.1

Складові системи екологічної безпеки організації

Складова системи	Характеристика та роль у забезпеченні екологічної безпеки
Контроль	Передбачає постійний моніторинг стану довкілля та рівня впливу підприємства на природне середовище. Включає регулярні вимірювання обсягів викидів, скидів, утворення відходів, а також перевірку дотримання екологічних стандартів і нормативів. Контроль забезпечує своєчасне виявлення порушень і дає змогу швидко реагувати на загрози.
Регулювання	Охоплює застосування правових, економічних та організаційних механізмів управління природоохоронною діяльністю. Це – впровадження екологічних стандартів, дотримання вимог національного та міжнародного законодавства, використання стимулів для екологобезпечної діяльності. Регулювання формує систему правил і норм, які спрямовують поведінку організації у сфері екологічної безпеки.
Заходи безпеки	Включають комплекс практичних дій і технологічних рішень, спрямованих на зниження негативного впливу підприємства на довкілля. Це впровадження екологічно чистих технологій, використання альтернативних джерел енергії, будівництво очисних споруд, утилізація та переробка відходів. Заходи безпеки забезпечують мінімізацію екологічних ризиків і створюють умови для сталого розвитку організації.

що допомагають швидко обробляти дані. Наступним елементом є внутрішній аудит екологічної діяльності підприємства, який проводиться спеціальними службами чи екологічними відділами організації. Він включає перевірку дотримання технологічних процесів, стану очисних споруд, ефективності використання ресурсів, відповідності нормативним актам і міжнародним стандартам, таким як ISO 14001.

Крім того, контроль охоплює правовий аспект – перевірку на відповідність чинному законодавству України у сфері охорони довкілля та міжнародним угодам. Особливо актуально це під час воєнних дій, коли підприємства можуть опинитися у надзвичайних умовах і ризик неконтрольованих викидів чи пошкодження екологічних систем значно зростає. Тому важливим є регулярний зовнішній контроль з боку державних органів (Міндовкілля, Держекоінспекція), а також незалежних аудиторських структур.

Ще однією складовою є управлінський контроль, коли керівництво організації систематично отримує звіти про стан екологічної діяльності та ухвалює рішення щодо вдосконалення технологій, модернізації обладнання чи інвестування в екологічні проєкти. Це дозволяє не лише уникати штрафів і санкцій, але й створювати позитивний імідж компанії як соціально відповідальної. Нарешті, контроль виконує профілактичну функцію – він формує культуру екологічної відповідальності серед працівників, адже кожен співробітник розуміє, що його дії відстежуються та оцінюються з точки зору безпеки довкілля.

Складова регулювання у системі менеджменту екологічної безпеки організації виконує роль координатора та «правил гри», які визначають рамки функціонування підприємства у сфері природоохоронної діяльності. Її сутність полягає у створенні механізмів впливу, що забезпечують дотримання екологічних норм і стандартів, запобігають порушенням та стимулюють відповідальне ставлення до навколишнього середовища.

До основних інструментів регулювання належать:

– правові механізми – закони, нормативні акти, міжнародні угоди, які встановлюють обов'язкові вимоги до природоохоронної діяльності, визначають відповідальність за шкоду довкіллю;

– економічні механізми – податки, збори, штрафи за забруднення, пільги і дотації для підприємств, що впроваджують екологічно безпечні технології, інвестиції в «зелені» проєкти;

– організаційні механізми – створення внутрішніх політик, процедур, стандартів та екологічного аудиту, що формують корпоративну екологічну культуру;

– ринкові механізми – участь у «зелених» сертифікаційних програмах, торгівля квотами на викиди, впровадження екологічного маркування.

Таким чином, регулювання формує систему правил, які впливають як на стратегічні рішення компанії, так і на щоденну діяльність її підрозділів. Воно забезпечує баланс між економічними інтересами підприємства та суспільною потребою у збереженні довкілля, а також створює передумови

для сталого розвитку і підвищення конкурентоспроможності на ринку.

Третя складова системи екологічної безпеки **заходи безпеки** відіграє ключову роль, оскільки саме вони забезпечують практичну реалізацію екополітики підприємства. Під цим розуміють комплекс організаційних, технічних і технологічних дій, спрямованих на зменшення негативного впливу виробничих процесів на довкілля. До таких заходів належить перехід на екологічно безпечні технології, модернізація обладнання, використання альтернативних і відновлюваних джерел енергії, запровадження систем енергоефективності та ресурсозбереження.

Важливим напрямом вважається створення і вдосконалення очисних споруд, систем збору, переробки та утилізації відходів, завдяки чому реально мінімізувати забруднення повітря, води й ґрунтів. Серед заходів також виділяють впровадження екологічного моніторингу для своєчасного виявлення ризиків та контроль відповідності господарської діяльності екологічним нормам. Додатково підприємства можуть застосовувати принципи «зеленої економіки» – це орієнтація на виробництво екологічно чистої продукції, скорочення шкідливих викидів та оптимізацію використання природних ресурсів.

Отже, заходи безпеки формують практичний фундамент екологічної безпеки підприємства, адже шляхом їх реалізації створюються умови для сталого розвитку, зменшення екологічних ризиків, підвищення соціальної відповідальності бізнесу та формування позитивного іміджу компанії на ринку.

Ефективне управління складовими системи екологічної безпеки має базуватися на таких **принципах**:

1. Принцип превентивності – передбачає випереджувальне реагування на потенційні екологічні загрози ще до того, як вони набудуть масштабного характеру. Йдеться про планування діяльності з урахуванням екологічних ризиків, впровадження технологій, що мінімізують можливі негативні наслідки для довкілля.

2. Принцип комплексності – включає інтеграцію екологічної складової в усі напрями діяльності організації: виробництво, інвестиції, логістику, управління персоналом.

Це дозволяє створити єдину узгоджену систему дій та уникнути фрагментарності у прийнятті рішень.

3. Принцип сталого розвитку – орієнтує підприємство на баланс між економічними вигодами, соціальною відповідальністю та охороною довкілля. Такий підхід формує довгострокову стратегію, яка враховує інтереси майбутніх поколінь.

4. Принцип законності – забезпечує дотримання чинного національного та міжнародного екологічного законодавства, стандартів і нормативів. Це мінімізує ризики штрафів, судових позовів та втрати ділової репутації.

5. Принцип відповідальності – передбачає персональну і колективну відповідальність керівників та працівників за дотримання екологічних вимог. Організація повинна формувати культуру безпечної поведінки та прозорості у своїй екологічній політиці.

6. Принцип адаптивності вимагає, щоб система екологічної безпеки була гнучкою, здатною до швидкого реагування на зміни у зовнішньому середовищі – природні катаклізми, воєнні загрози, зміни клімату чи нові екологічні нормативи.

7. Принцип економічної доцільності означає, що будь-які природоохоронні заходи мусять оцінюватися з точки зору витрат і результатів. Інвестиції в екологічну безпеку розглядаються як внесок у зниження довгострокових ризиків і підвищення конкурентоспроможності.

8. Принцип прозорості та відкритості – організації важливо забезпечувати інформування громадськості, органів влади та партнерів про результати своєї екологічної діяльності, оприлюднювати звіти, дотримуватися стандартів корпоративної соціальної відповідальності.

9. Принцип інноваційності – передбачає використання сучасних екотехнологій, цифрових систем моніторингу, альтернативних джерел енергії, що є запорукою ефективності системи екологічної безпеки в довгостроковій перспективі.

10. Принцип міжнародної співпраці – передбачає орієнтацію на кращі світові практики, участь у глобальних екологічних програмах та партнерство з міжнародними організаціями для вирішення проблем транскордонного характеру.

9.3. Інструменти та стратегія менеджменту екологічної безпеки

Сучасним українським організаціям необхідно дотримуватися високих стандартів екологічної безпеки насамперед тому, що це безпосередньо впливає на їхню репутацію, конкурентоспроможність і довіру з боку партнерів та споживачів. Умови євроінтеграції та вимоги міжнародних ринків змушують компанії дотримуватися екологічних стандартів, адже саме вони часто стають вирішальним фактором при укладенні контрактів чи виході на зовнішні ринки. Високий рівень екологічної безпеки перетворюється на інструмент не лише виживання, але й зростання підприємств у сучасному глобалізованому середовищі.

Другим вагомим аспектом є соціальна відповідальність бізнесу перед суспільством. Українські підприємства функціонують у складних умовах воєнного часу, коли екологічні ризики зростають у зв'язку з руйнуванням інфраструктури, забрудненням ґрунтів і водних ресурсів. Забезпечення екологічної безпеки допомагає зменшити шкоду для здоров'я працівників та місцевого населення, створює умови для безпечного виробництва і формує позитивний психологічний клімат. Організації, які піклуються про довкілля, демонструють готовність брати на себе відповідальність за майбутнє країни, що сприяє зміцненню їхнього іміджу.

Не менш важливим є економічний ефект. Недотримання екологічних стандартів тягне за собою штрафи, збільшення витрат на ліквідацію наслідків аварій та зниження інвестиційної привабливості. Водночас системне впровадження екологобезпечних технологій дозволяє підприємствам скорочувати витрати енергоресурсів, зменшувати втрати від забруднень і отримувати додаткові переваги завдяки зеленому брендуванню продукції. Це створює умови для сталого розвитку, що є принциповою вимогою як внутрішніх, так і міжнародних партнерів, а також відповідає стратегії відновлення економіки України у післявоєнний період.

З метою досягнення належного рівня забезпечення менеджменту екологічної безпеки організації важливо використовувати ефективні **інструменти**, до яких відносять:

1. Організаційні інструменти. До цієї групи належать політики безпеки, внутрішні регламенти, інструкції

та стандарти, які визначають правила поведінки співробітників і порядок реагування на надзвичайні ситуації. Організаційні інструменти включають створення спеціалізованих підрозділів безпеки, визначення відповідальних осіб, розподіл повноважень і контроль за дотриманням нормативів.

2. Правові інструменти. Це використання чинного законодавства, внутрішніх договорів, контрактів і угод, що регламентують права та обов'язки сторін у сфері безпеки. Сюди входять трудові договори з пунктами про нерозголошення, комерційна таємниця, угоди про відповідальність за збереження матеріальних та інформаційних ресурсів, а також співпраця з державними органами для правового захисту інтересів підприємства.

3. Економічні інструменти. Вони пов'язані з мотивацією персоналу дотримуватись вимог безпеки: система матеріальних стимулів, страхування персоналу, компенсації, інвестиції в охорону праці та довкілля. Економічні інструменти сприяють формуванню відповідального ставлення співробітників до захисту корпоративних ресурсів, адже порушення правил часто напряму впливає на фінансовий стан організації.

4. Технічні інструменти. Це сучасні системи охорони і контролю, які включають відеоспостереження, сигналізацію, системи контролю доступу, біометричну ідентифікацію, пожежогасіння, екологічний моніторинг. В інформаційній сфері це програмні комплекси для захисту даних, антивірусні системи, шифрування, брандмауери та системи резервного копіювання.

5. Соціально-психологічні інструменти. Ця група пов'язана із забезпеченням корпоративної культури безпеки, формуванням цінностей відповідальності та довіри. Вона охоплює тренінги, навчальні програми, корпоративні комунікації, заходи для формування командної роботи та підвищення лояльності персоналу. Важливим інструментом виступає розвиток «свідомості безпеки» у співробітників.

6. Інформаційно-аналітичні інструменти. До них належить моніторинг зовнішнього середовища, оцінка ризиків, проведення аудитів, аналіз фінансової та кадрової звітності, використання методів прогнозування загроз. Завдяки цим інструментам підприємство може вчасно виявляти

потенційні проблеми й адаптувати свою стратегію безпеки до змін у середовищі.

Окрім інструментів організаціям необхідно розробляти дієві стратегії управління екологічною безпекою, які розраховані на довгострокові перспективи, та враховувати циклічність економічних і природних процесів, викликів сучасності.

Стратегія менеджменту екологічної безпеки – це довгострокова система цілей, принципів і управлінських рішень, спрямованих на захист довкілля, раціональне використання природних ресурсів та зниження екологічних ризиків у діяльності організації. Вона визначає напрям дій підприємства щодо попередження негативного впливу на природу, мінімізації наслідків виробничої діяльності та впровадження екологічно безпечних технологій.

Сутність такої стратегії полягає у формуванні збалансованої політики, що поєднує економічні інтереси підприємства з потребами суспільства у безпечному середовищі. Вона включає розробку стандартів екологічного менеджменту, визначення пріоритетів природоохоронної діяльності, створення системи моніторингу та оцінки екологічних ризиків.

У практичному вимірі стратегія менеджменту екологічної безпеки проявляється у впровадженні альтернативних джерел енергії, використанні «зелених» технологій, оптимізації систем утилізації та переробки відходів, дотриманні національних та міжнародних екологічних норм. Вона також спрямована на підвищення конкурентоспроможності підприємства завдяки позитивному іміджу, соціальній відповідальності та сталому розвитку.

Основні етапи стратегії наведено в табл. 9.2.

При цьому реалізація стратегії управління екологічною безпекою організації включає певні напрями:

– впровадження системи екологічного моніторингу – створення комплексної системи відстеження стану довкілля, яка дає можливість своєчасно фіксувати рівень викидів, обсяг відходів та вплив виробничих процесів на природні ресурси;

– розробка і виконання програм екологічної модернізації – оновлення обладнання та технологій із урахуванням принципів енергоефективності, використання чистих

Таблиця 9.2

Характеристика основних етапів забезпечення екологічної безпеки організації в сучасних умовах

Етап	Зміст та характеристика
1. Аналіз середовища	Передбачає виявлення внутрішніх і зовнішніх факторів, що впливають на екологічну безпеку організації. Сюди входить оцінка рівня екологічних ризиків, аналіз виробничих процесів, дотримання екологічного законодавства, вивчення міжнародних стандартів і вимог.
2. Постановка цілей	Визначаються ключові стратегічні цілі у сфері екологічної безпеки: мінімізація шкідливого впливу на довкілля, зниження обсягів відходів, оптимізація використання ресурсів, розвиток «зелених» технологій, підвищення репутаційної цінності організації.
3. Вибір стратегії та заходів	Формуються конкретні напрями і програми дій для досягнення поставлених цілей. Це може включати впровадження систем екологічного менеджменту, інноваційних технологій, альтернативних джерел енергії, модернізацію очисних споруд, розвиток системи екологічного моніторингу.
4. Реалізація стратегії	Передбачає впровадження практичних рішень і управлінських механізмів, розподіл відповідальності між підрозділами, забезпечення фінансування екологічних проєктів, проведення навчання та підвищення кваліфікації персоналу у сфері екологічної безпеки.
5. Моніторинг і контроль	Здійснюється оцінка результатів виконання стратегії, аналіз ефективності заходів, перевірка відповідності екологічним стандартам і нормативам. Важливо виявляти відхилення та визначати напрями для вдосконалення.
6. Коригування та вдосконалення	На основі отриманих результатів проводяться коригувальні дії, впроваджуються нові рішення, враховуються зміни у законодавстві, технологіях та зовнішньому середовищі. Це забезпечує гнучкість стратегії та її актуальність у довгостроковій перспективі.

джерел енергії та мінімізації шкідливого впливу на навколишнє середовище;

– формування внутрішньої екологічної політики – створення корпоративних стандартів, інструкцій та регламентів, що регулюють поведінку персоналу у сфері природоохоронної діяльності;

– виконання законодавчих і міжнародних вимог – забезпечення дотримання норм чинного екологічного законодавства України, а також міжнародних угод і стандартів у сфері захисту довкілля;

– розвиток альтернативних джерел енергії – перехід на сонячні, вітрові та інші відновлювані ресурси для зменшення залежності від викопного палива та скорочення викидів вуглекислого газу;

– організація системи управління екологічними ризиками – проведення оцінки можливих загроз і розробка планів дій у кризових ситуаціях, пов'язаних із техногенними або природними катастрофами;

– підвищення екологічної обізнаності персоналу – навчання співробітників правил екологічної поведінки, формування культури екологічної відповідальності всередині організації;

– розширення співпраці з державними і громадськими структурами – участь у програмах екологічного партнерства, екологічних аудитах, взаємодія з органами влади та екологічними організаціями;

– впровадження технологій поводження з відходами – сортування, утилізація, переробка та повторне використання відходів з метою мінімізації негативного впливу на навколишнє середовище;

– створення системи прозорої екологічної звітності – регулярне оприлюднення результатів діяльності компанії у сфері екології, що формує довіру серед інвесторів, партнерів і суспільства.

Перелік українських підприємств, що забезпечують збереження екологічної безпеки, створюють умови для її покращення та демонструють ставлення до «зелених ініціатив», подано в додатку Л.

Питання для самоконтролю

1. У чому полягає сутність екологічної безпеки організації та як вона пов'язана зі загальною системою корпоративної безпеки?
2. Які основні об'єкти екологічної безпеки можна виділити на рівні підприємства та чому вони є важливими?
3. Назвіть головних суб'єктів менеджменту екологічної безпеки організації та охарактеризуйте їхні функції.
4. Які внутрішні та зовнішні загрози найбільше впливають на стан екологічної безпеки в сучасних умовах?
5. Які функції виконує система екологічної безпеки підприємства?
6. У чому полягає значення принципів екологічної безпеки та як вони забезпечують сталий розвиток компанії?
7. Розкрийте зміст основних складових системи екологічної безпеки: контроль, регулювання, заходи безпеки.
8. Які інструменти менеджменту екологічної безпеки застосовуються на сучасних підприємствах?
9. Що таке стратегія менеджменту екологічної безпеки і які напрями вона охоплює?
10. Чому для українських організацій у післявоєнний період важливо підтримувати високий рівень екологічної безпеки?

Тестові завдання

1. Яке з наведених визначень найповніше розкриває сутність екологічної безпеки організації?

а) Це система заходів, спрямованих на охорону навколишнього середовища;

б) це стан захищеності підприємства та суспільства від екологічних ризиків, що забезпечує баланс між виробничою діяльністю, використанням природних ресурсів та охороною довкілля;

в) це дотримання екологічних законів і стандартів;

г) це діяльність державних органів у сфері екології.

2. До основних об'єктів екологічної безпеки організації належать:

а) тільки природні ресурси, які використовує підприємство;

б) лише працівники підприємства, оскільки вони найбільше піддаються впливу;

в) природні ресурси, виробниче середовище, працівники, місцеві громади та довкілля загалом;

г) фінансові ресурси компанії, які виділяються на природоохоронну діяльність.

3. Яку роль виконує екологічна безпека у структурі корпоративної безпеки?

а) Вона є допоміжною і не впливає на інші види безпеки;

б) вона має стратегічне значення, адже порушення екологічних стандартів призводить до економічних втрат, репутаційних ризиків і соціальних конфліктів;

в) вона розглядається виключно як соціальний елемент охорони праці;

г) вона потрібна тільки у сфері промислового виробництва.

4. Основними суб'єктами управління екологічною безпекою організації є:

а) виключно керівництво підприємства;

б) державні контролюючі органи;

в) керівники, працівники, служби охорони довкілля, державні установи та громадські організації, які впливають на екологічну політику;

г) тільки спеціалізовані екологічні інспекції.

5. Яка головна мета функції «контроль» у системі екологічної безпеки?

а) Лише збір екологічних даних для звітності;

б) регулярне спостереження, оцінювання та своєчасне виявлення відхилень у діяльності підприємства з метою попередження негативних наслідків для довкілля і здоров'я людей;

в) покарання винних працівників;

г) формування бюджету для інвестицій у природоохоронні заходи.

6. Суть складової «регулювання» в системі екологічної безпеки полягає у:

а) забороні підприємствам вести діяльність, що шкодить довкіллю.

у впровадженні правових, економічних і організаційних механізмів, які формують правила та стандарти екологічної поведінки підприємств;

б) діяльності міжнародних організацій зі захисту довкілля;

в) створенні нових технологій очищення відходів.

7. Які заходи можна віднести до практичних складових екологічної безпеки?

а) Виключно розробку інструкцій із охорони довкілля;

б) використання екологічно чистих технологій, альтернативної енергетики, будівництво очисних споруд, впровадження програм утилізації та переробки відходів;

в) лише навчання персоналу правил екологічної безпеки;

г) виконання формальних вимог екологічного законодавства.

8. Яке місце займають принципи екологічної безпеки у діяльності організації?

а) Це формальні документи, які не мають реального впливу;

б) це основа всієї системи управління, адже принципи законності, комплексності, превентивності та безперервності визначають характер і якість екологічної політики;

в) це лише рекомендації для окремих відділів;

г) це набір міжнародних угод, що не стосується підприємства напряму.

9. Яке значення має стратегія менеджменту екологічної безпеки для підприємства?

а) Вона потрібна лише для великих підприємств;

б) вона визначає довгострокові напрями розвитку, інтегрує екологічні заходи в загальну стратегію бізнесу, знижує ризики і підвищує конкурентоспроможність організації;

в) вона служить виключно для звітності перед державою;

г) вона використовується тільки у кризових ситуаціях.

10. В умовах війни та післявоєнного відновлення екологічна безпека набуває особливого значення для українських підприємств, тому що:

а) це дозволяє уникнути міжнародних санкцій;

б) руйнування інфраструктури, обстріли, забруднення ґрунтів і води створюють нові виклики, і підприємства зобов'язані впроваджувати екологобезпечні технології, щоби зберегти природні ресурси та відновити довіру суспільства і партнерів;

в) це знижує витрати на виробництво;

г) цього вимагає лише міжнародне право.

Практичні завдання

Завдання 1.

Підприємство «ЕкоПром» здійснює виробництво будівельних матеріалів. У процесі діяльності утворюється велика кількість відходів, які частково складуються на території підприємства, а частково скидаються у місцеву річку після мінімальної очистки. Протягом останніх років громада висловлює численні скарги на забруднення води та ґрунтів. Крім того, у працівників почастішали випадки професійних захворювань, пов'язаних із пилом та хімічними домішками. Керівництво підприємства планує запровадити систему екологічної безпеки, але стикається з дилемою: обмежені фінансові ресурси не дають змого одночасно впровадити сучасні очисні споруди, замінити застаріле обладнання та підвищити стандарти охорони праці.

1. Визначте першочергові кроки менеджменту екологічної безпеки для підприємства.

2. Обґрунтуйте критерії вибору пріоритетів.

3. Оцініть імовірні наслідки ігнорування проблеми для репутації та фінансової стабільності компанії.

Завдання 2.

Агропромислове підприємство «ЗерноЛенд» активно розширює свої земельні площі. Для цього воно застосовує інтенсивні технології вирощування культур, які передбачають використання значних обсягів мінеральних добрив і пестицидів. Останнім часом місцева влада виявила перевищення допустимих норм вмісту нітратів у ґрунтових водах. Крім того, міжнародний партнер підприємства пригрозив розірванням контракту через порушення екологічних стандартів, які діють у країнах ЄС. Керівництво підприємства розуміє необхідність перегляду своєї стратегії, але побоюється зниження врожайності та доходів у разі зменшення використання добрив.

1. Сформуйте можливі підходи до управління екологічною безпекою підприємства, що допомогли би поєднати економічну ефективність із екологічними стандартами.

2. Оцініть, які довгострокові вигоди може отримати підприємство від екологізації своєї діяльності.

Завдання 3.

Машинобудівний завод «ТехноМаш» розташований у зоні підвищеного ризику, оскільки поряд знаходяться військові об'єкти, які часто стають мішенню для обстрілів. Підприємство має критично важливі для регіону виробничі потужності, але через військові дії виникають проблеми із забезпеченням стабільної роботи: пошкоджуються комунікації, відбуваються аварійні викиди мастил та хімічних речовин, зростає ризик забруднення територій і водних джерел. Додатково існує загроза руйнування сховищ відходів. Керівництво повинно терміново розробити план дій у кризових умовах.

1. Запропонуйте заходи менеджменту екологічної безпеки в умовах воєнних ризиків.

2. Визначте можливості мінімізації шкоди довкіллю.

3. Окресліть роль співпраці з місцевою владою і міжнародними організаціями у забезпеченні стійкості підприємства.

ТЕМА 10
ОЦІНКА ЕФЕКТИВНОСТІ МЕНЕДЖМЕНТУ БЕЗПЕКИ ОРГАНІЗАЦІЇ

10.1. Сутність оцінки ефективності менеджменту безпеки організації

10.2. Методи, підходи та інструменти оцінки ефективності менеджменту безпеки організації

10.3. Напрями удосконалення системи оцінки ефективності менеджменту безпеки організації

Основні поняття і терміни: організація, менеджмент безпеки, оцінка ефективності, прийняття рішень, політика безпеки організації, результати діяльності, оцінка загроз, аудит рівня безпеки, види ризиків, заходи безпеки, стійке функціонування організації.

10.1. Сутність оцінки ефективності менеджменту безпеки організації

Оцінка ефективності менеджменту безпеки організації вважається ключовим елементом сучасної системи управління, адже саме вона дає змогу з'ясувати, наскільки прийняті рішення, впроваджені заходи та використані ресурси забезпечують досягнення запланованих результатів у сфері безпеки. У реаліях постійних змін зовнішнього середовища, зростання ризиків і загроз організація не може обмежуватися лише формальним упровадженням політики безпеки – необхідним є системний підхід до контролю, аналізу та коригування управлінських дій.

Сутність такої оцінки полягає у вимірюванні співвідношення між цілями безпеки та фактичними результатами діяльності. Це дає можливість виявити не тільки рівень досягнення очікуваних результатів, але й визначити слабкі місця в системі захисту, оцінити ефективність витрат на безпекові заходи та обґрунтувати потребу в їх удосконаленні. Важливим є те, що аналіз ефективності менеджменту

безпеки охоплює як фінансові, так і нефінансові аспекти – від економічної доцільності інвестицій у захист до оцінки соціально-психологічного клімату в колективі.

Оцінка ефективності менеджменту безпеки організації стає не лише інструментом контролю, а й засобом стратегічного розвитку, що дозволяє адаптувати систему безпеки до нових викликів і формувати конкурентні переваги. Вона виступає основою для прийняття управлінських рішень, спрямованих на підвищення стійкості організації, зменшення ризиків та забезпечення стабільності функціонування у довгостроковій перспективі.

Оцінка ефективності менеджменту безпеки організації – це процес порівняння фактичних результатів реалізації заходів безпеки з установленими стратегічними і тактичними цілями, що дає можливість визначити ступінь раціональності управлінських рішень, адекватність використаних ресурсів і здатність системи безпеки забезпечувати стійке функціонування підприємства в умовах ризиків та загроз.

Під оцінкою ефективності менеджменту безпеки організації слід розуміти комплексний аналіз витрат і результатів, спрямований на встановлення економічної доцільності впроваджених заходів безпеки, а також виявлення їхнього впливу на фінансові показники, конкурентоспроможність і довгострокову стійкість підприємства.

Оцінка ефективності менеджменту безпеки організації – це процес визначення того, наскільки система безпеки відповідає очікуванням зацікавлених сторін, створює сприятливе середовище для персоналу, підтримує високий рівень корпоративної культури та довіри, а також сприяє зниженню соціальних, правових і репутаційних ризиків.

Оцінка ефективності менеджменту безпеки організації – це цілеспрямований процес аналізу та зіставлення фактичних результатів функціонування системи безпеки з попередньо визначеними цілями, критеріями та стандартами. Вона допомагає встановити, наскільки використані ресурси та управлінські рішення забезпечують належний рівень захищеності організації від зовнішніх і внутрішніх загроз.

Суть цього процесу полягає не лише у фіксації кількісних результатів, а й у визначенні якісних аспектів: рівня

надійності системи, швидкості реагування на ризики, довіри персоналу до безпекових заходів, а також відповідності функціонування системи безпеки стратегічним цілям підприємства. Тобто ефективність у сфері менеджменту безпеки має багатовимірний характер і не може зводитися лише до фінансових показників.

Важливою рисою оцінки є її інтегральність: вона включає економічні, організаційні, правові та соціальні елементи діяльності. Наприклад, поряд з аналізом витрат на заходи безпеки враховуються їхній вплив на репутацію організації, рівень задоволеності працівників умовами праці, а також здатність підприємства адаптуватися до нових викликів. Назагал оцінка ефективності менеджменту безпеки виконує три ключові функції:

– контрольну (дає змогу визначити ступінь досягнення поставлених завдань);

– аналітичну (виявляє сильні та слабкі сторони системи безпеки);

– прогнозну (слугує основою для формування нових управлінських рішень і стратегій розвитку).

Сутність оцінки ефективності менеджменту безпеки організації можна розглядати з боку стратегічного й оперативного управління (табл. 10.1).

До об'єктів, що задіяні в процесі оцінки ефективності менеджменту безпеки організації, відносяться:

1. Організаційні об'єкти:

– структура управління безпекою – підрозділи, служби, посадові особи, які забезпечують планування та реалізацію заходів безпеки;

– процеси управління – планування, контроль, аудит, координація та комунікації, що впливають на рівень безпеки.

2. Ресурсні об'єкти:

– фінансові ресурси – кошти, інвестовані у системи захисту, інформаційні технології, охорону праці, навчання персоналу;

– матеріально-технічні ресурси – обладнання, технічні системи захисту, програмне забезпечення, інфраструктура;

– людські ресурси – кваліфікація, мотивація і дисципліна персоналу, рівень їхньої обізнаності у сфері безпеки.

Таблиця 10.1

Стратегічна та оперативна роль оцінки ефективності менеджменту безпеки

Аспект	Стратегічне управління	Оперативне управління
Мета оцінки	Забезпечення відповідності системи безпеки довгостроковим цілям розвитку організації	Моніторинг та контроль поточного стану безпеки, реагування на зміни
Горизонт часу	Довгострокова перспектива (3–5 років і більше)	Короткострокова перспектива (дні, тижні, квартал)
Завдання	Визначення стратегічних пріоритетів, інвестицій у безпеку, формування політик і стандартів	Виявлення відхилень, локалізація проблем, коригування планів і процедур
Методи	Стратегічний аналіз, сценарне прогнозування, оцінка ризиків, бенчмаркінг	Оперативні індикатори, статистичний контроль, внутрішній аудит, інцидент-аналіз
Результати	Розробка стратегій безпеки, інтеграція безпекових цілей у загальну стратегію організації	Забезпечення безперервності діяльності, мінімізація втрат і загроз у реальному часі
Ключові користувачі інформації	Вищий менеджмент, власники, стратегічні інвестори	Керівники підрозділів, служби безпеки, оперативний персонал

3. Інформаційні об'єкти:

– документація – політики безпеки, інструкції, внутрішні регламенти;

– інформаційні потоки – канали передачі даних, корпоративні інформаційні системи;

– аналітичні дані – показники ризиків, звіти, аудиторські висновки.

4. Функціональні об'єкти:

– рівень захищеності від загроз – стан інформаційної, кадрової, економічної, правової та фізичної безпеки;

– якість виконання безпекових заходів – ступінь відповідності їх результатів встановленим цілям;

– ефективність реагування на інциденти – швидкість і результативність дій у разі виникнення небезпечних ситуацій.

5. Зовнішні об'єкти:

– регуляторне середовище – вимоги законодавства, нормативи, міжнародні стандарти;

– контрагенти та партнери – їхня надійність і безпековий вплив на організацію;

– суспільне середовище – імідж, репутація та рівень довіри з боку клієнтів, громадськості й державних органів.

У сучасному середовищі діяльності організацій, що характеризується високою динамікою ринкових змін, цифровізацією та посиленням зовнішніх і внутрішніх загроз, оцінка ефективності менеджменту безпеки набуває особливої актуальності. Підприємства змушені працювати в умовах невизначеності, підвищеної конкуренції та значних ризиків, які охоплюють фінансову, інформаційну, правову та кадрову сфери. Без системної оцінки ефективності заходів безпеки організація ризикує втратити конкурентоспроможність, стабільність функціонування та довіру партнерів і клієнтів.

Оцінка в таких умовах виконує роль інструмента контролю і стратегічного розвитку: вона дозволяє не лише фіксувати рівень досягнення поставлених цілей, а й виявляти проблемні зони, аналізувати доцільність використання ресурсів та коригувати управлінські рішення. Важливо, що завдяки оцінці підприємства здатні вчасно адаптуватися до нових викликів, знижувати витрати на ліквідацію наслідків ризиків та посилювати довгострокову стійкість.

Організація, впроваджуючи процедуру оцінки ефективності менеджменту безпеки, переслідує такі цілі:

– контроль досягнення стратегічних і тактичних завдань – перевірка відповідності фактичних результатів запланованим цілям безпеки;

– визначення рівня захищеності організації – оцінювання стійкості до загроз і здатності протистояти ризикам;

– оптимізація використання ресурсів – аналіз витрат на заходи безпеки та їх економічна доцільність;

– виявлення слабких місць у системі – ідентифікація проблемних процесів, що потребують удосконалення;

– підвищення якості управлінських рішень – формування надійної інформаційної основи для планування й коригування дій;

– зміцнення конкурентних позицій та репутації – забезпечення довіри партнерів, клієнтів і суспільства до організації;

– формування основи для інновацій та розвитку – адаптація системи безпеки до нових технологічних і соціально-економічних викликів.

10.2. Методи, підходи та інструменти оцінки ефективності менеджменту безпеки організації

Методологія оцінки ефективності менеджменту безпеки організації ґрунтується на використанні різних підходів, які відображають багатогранність цього процесу. Жоден з підходів не може повністю охопити всі аспекти безпеки, адже йдеться про складну систему, що включає економічні, організаційні, соціальні та технологічні компоненти. Саме тому сучасна практика передбачає застосування поєднання методів, що дає змогу сформувати більш об'єктивне уявлення про стан і результативність функціонування безпекових заходів.

Залежно від цілей і завдань оцінювання можна виділити чотири **ключові підходи**: системно-управлінський, економіко-аналітичний, соціально-функціональний та інтегральний. Вони відрізняються об'єктами аналізу, видами показників та інструментами, але всі спрямовані на досягнення основної мети – визначення реальної здатності організації забезпечувати належний рівень безпеки та стійкості в умовах ризиків:

1. Системно-управлінський підхід. Він розглядає систему менеджменту безпеки як комплекс взаємопов'язаних елементів – структури, функцій, процесів і ресурсів. Оцінювання відбувається шляхом аналізу ефективності управлінських процедур: планування, контролю, координації, комунікацій та реагування на загрози. Перевага підходу полягає в тому, що він допомагає виявити узгодженість між окремими елементами системи та їхній внесок у загальний результат.

2. Економіко-аналітичний підхід. Основою цього підходу є порівняння витрат на забезпечення безпеки з отриманими результатами. Він передбачає розрахунок фінансових

показників, аналіз економічної доцільності інвестицій у безпеку, визначення ефективності витрат на технічні засоби, персонал чи навчання. Такий підхід особливо актуальний у ринкових умовах, де кожна гривня має бути виправданою, а безпекові заходи повинні приносити вимірюваний економічний ефект.

3. Соціально-функціональний підхід. Цей підхід акцентує увагу на людському факторі та соціальних наслідках функціонування системи безпеки. Оцінка проводиться з огляду на задоволеність персоналу умовами праці, рівень корпоративної культури, психологічний клімат у колективі та довіру до заходів безпеки. Також враховується вплив безпеки на репутацію організації та її взаємини зі зацікавленими сторонами. Такий підхід показує, що безпека – це не лише фінанси і техніка, а й соціальна стабільність та довіра.

4. Інтегральний (комплексний) підхід. Інтегральний підхід поєднує елементи попередніх методологій і базується на використанні системи різнопланових показників – кількісних і якісних. Він передбачає застосування багатофакторного аналізу, моделювання ризиків та інтегральних індексів, завдяки чому можна комплексно оцінити стан безпеки. Такий підхід є найбільш наближеним до сучасної практики, адже він враховує економічні, організаційні та соціальні чинники одночасно, створюючи повну картину ефективності.

Для ефективної та прозорої оцінки ефективності управління безпекою організації сучасні організації можуть використовувати **показники**, які тією чи іншою мірою встановлюють ефективність, доцільність, напрями, які необхідні для визначення:

1. Кількісні показники. До цієї групи відносять економічні, фінансові та ризикові індикатори, які можна обчислити у числовому вираженні. Вони дають можливість чітко відстежити динаміку змін у рівні захищеності організації, порівняти результати в різні періоди та визначити ефективність витрачених ресурсів. Такі показники відрізняються високим рівнем об'єктивності, оскільки ґрунтуються на фактичних даних фінансової та управлінської звітності. Крім того, їх можна інтегрувати в аналітичні моделі, що допомагає

прогнозувати ймовірність виникнення загроз та оцінювати очікувані наслідки ризиків:

– економічні показники: співвідношення витрат на забезпечення безпеки та отриманих результатів. Формула:

$$E = \frac{R_b}{C_b}, \tag{10.1}$$

де E – економічна ефективність, R_b – результати, досягнуті від впровадження заходів безпеки (зменшення збитків, підвищення продуктивності), C_b – витрати на безпекові заходи;

– фінансові показники: зниження рівня втрат і збитків від інцидентів безпеки, зростання рентабельності підприємства, покращення ліквідності та фінансової стійкості. Наприклад:

$$\Delta Z = Z_{\text{до}} - Z_{\text{після}}, \tag{10.2}$$

де ΔZ – скорочення збитків, $Z_{\text{до}}$ – збитки до впровадження заходів, $Z_{\text{після}}$ – збитки після впровадження;

– ризикові показники: імовірність виникнення загроз та очікуваний розмір збитку. Формула ризику:

$$R = P \times L, \tag{10.3}$$

де R – рівень ризику, P – імовірність настання події, L – розмір можливих втрат.

2. Якісні показники. Ці показники не завжди піддаються точним вимірюванням, однак мають важливе значення. Вони відображають рівень організаційної культури, соціальної стабільності та довіри до системи безпеки з боку працівників і партнерів. На відміну від фінансових чи економічних індикаторів, якісні показники демонструють, наскільки заходи безпеки узгоджуються з цінностями, нормами та очікуваннями колективу. Саме вони формують довгостроковий вплив на репутацію організації, зміцнюють її імідж та підвищують конкурентоспроможність у взаєминах зі зовнішнім середовищем:

– організаційні – рівень узгодженості функцій безпеки з іншими управлінськими процесами, ефективність комунікацій, відповідність нормативним вимогам;

– соціальні – рівень задоволеності працівників умовами праці, довіра до системи безпеки, зниження кількості конфліктів чи інцидентів у колективі;

– репутаційні – імідж організації, оцінка її надійності з боку партнерів, клієнтів та громадськості; наявність чи відсутність негативних інформаційних приводів у медіа.

Якісні показники зазвичай оцінюють через експертні опитування, соціологічні дослідження, рейтингові оцінки.

3. Інтегральні критерії оцінювання. Для комплексної характеристики ефективності часто застосовують інтегральні індекси, що поєднують кількісні та якісні фактори. Такі критерії дозволяють отримати узагальнений показник, який відображає стан системи безпеки з урахуванням різних аспектів діяльності організації. Їхня перевага полягає в можливості порівняння різних періодів та виявлення тенденцій розвитку безпеки у динаміці. Крім того, інтегральні показники забезпечують зручність для прийняття управлінських рішень, оскільки спрощують складну багатофакторну інформацію до зрозумілого індикатора. Саме тому вони широко застосовуються в практиці стратегічного й оперативного управління, особливо у великих організаціях:

– індекс ефективності безпеки (*ІЕБ*):

$$ІЕБ = \sum_{i=1}^{n} w_i \times k_i, \qquad (10.4)$$

де w – ваговий коефіцієнт значущості i-го показника, k_i – нормалізоване значення показника, n – кількість показників;

– критерій збалансованості: співвідношення між витратами, рівнем ризику та досягнутими результатами. Формула:

$$K_{зб} = \frac{(E + S + R)}{3}, \qquad (10.5)$$

де E – економічна складова, S – соціальна складова, R – рівень зниження ризику.

У сучасних умовах підвищеної конкуренції, цифровізації та постійних змін у зовнішньому середовищі організації змушені приділяти особливу увагу системі безпеки. Проте сама наявність заходів захисту ще не гарантує їх дієвості – важливим є постійний аналіз і контроль їхньої результативності. Саме методи та інструменти оцінки ефективності допомагають виявити, наскільки витрачені ресурси,

обрані стратегії та управлінські рішення сприяють досягненню бажаного рівня захищеності та стабільності організації. Вони створюють інформаційну основу для прийняття зважених управлінських рішень і формують умови для розвитку підприємства в довгостроковій перспективі.

Використання різних методів оцінювання важливе ще й тому, що безпека має багатовимірний характер: вона включає економічні, фінансові, організаційні, соціальні й технологічні аспекти. Тому поєднання економіко-статистичних, експертних, багатофакторних і цифрових підходів забезпечує комплексний аналіз і дає змогу врахувати як кількісні, так і якісні фактори. Завдяки цьому оцінка ефективності перетворюється з формальної процедури на дієвий інструмент стратегічного та оперативного управління, що підвищує стійкість і конкурентоспроможність організації. До основних **методів** оцінки ефективності менеджменту безпеки можна віднести:

1. Економіко-статистичні методи. До цієї групи належать методи, що базуються на аналізі кількісних даних про діяльність організації. Найпоширенішим є аналіз витрат і результатів, який дозволяє зіставити ресурси, витрачені на заходи безпеки, з отриманим ефектом у вигляді зменшення ризиків, скорочення збитків чи підвищення продуктивності. Наприклад, використовується формула:

$$E = \frac{R_b}{C_b}, \tag{10.6}$$

де E – ефективність заходів безпеки, R_b – отриманий результат, C_b – понесені витрати.

Також застосовується коефіцієнтний аналіз, який передбачає розрахунок різних відносних показників – рівня збитковості, коефіцієнтів ліквідності, фінансової стійкості тощо. Ці показники відображають фінансовий вплив безпекових заходів і дають можливість порівнювати динаміку в часі чи з іншими підприємствами.

2. Експертні методи. У випадках, коли кількісні дані є обмеженими або важко піддаються точному вимірюванню, застосовуються експертні підходи.

З-поміж них виокремлюють:

– метод Delphi – колективне опитування групи експертів із кількома турами оцінювання, що допомагає досягти

узгодженості думок щодо рівня ефективності заходів безпеки;

– рейтингові оцінки – присвоєння вагових балів окремим аспектам безпеки (наприклад, рівню захисту інформації, кадровій стабільності, технічній готовності).

Експертні методи є незамінними для оцінки якісних показників, таких як репутація, корпоративна культура чи рівень довіри персоналу.

3. Методи багатофакторного аналізу та моделювання. Цей блок включає застосування математичних та економіко-математичних моделей для вивчення складних взаємозв'язків у системі безпеки. Використовуються такі інструменти, як:

– багатофакторна регресія – для визначення впливу різних змінних (витрати, рівень ризику, кадрові заходи) на загальний рівень безпеки;

– сценарне моделювання – прогнозування наслідків реалізації різних сценаріїв розвитку подій (приміром, кібератаки чи кадрових втрат);

– імітаційне моделювання – відтворення поведінки системи безпеки в умовах ризику та невизначеності, що допомагає оцінити потенційні наслідки прийнятих рішень.

Такі методи дають змогу будувати більш точні прогнози і враховувати вплив багатьох чинників одночасно.

4. Використання цифрових технологій у моніторингу ефективності. Сучасні організації дедалі частіше застосовують інформаційні системи та цифрові технології для постійного контролю рівня безпеки. До них належать:

– системи бізнес-аналітики (BI-системи), які дозволяють інтегрувати дані з різних джерел та формувати дашборди ефективності;

– технології Big Data, що забезпечують аналіз великих обсягів даних і допомагають виявляти приховані закономірності у сфері безпеки;

– системи моніторингу інформаційної безпеки (SIEM), що дають змогу відстежувати інциденти в реальному часі та швидко реагувати на них;

– штучний інтелект і машинне навчання, що використовуються для прогнозування ризиків та автоматизації управлінських рішень.

Завдяки цифровим інструментам оцінка ефективності стає безперервною, динамічною та більш об'єктивною, оскільки базується на актуальних даних у режимі реального часу.

10.3. Напрями удосконалення системи оцінки ефективності менеджменту безпеки організації

Система оцінки ефективності менеджменту безпеки має вирішальне значення для сучасних організацій, оскільки дозволяє перетворити управління безпекою з формального обов'язку на стратегічний інструмент розвитку. Вона забезпечує керівництво об'єктивною інформацією для прийняття рішень, допомагає оптимізувати витрати на захист, вчасно виявляти нові ризики та адаптуватися до змін у зовнішньому середовищі.

Удосконалення оцінки робить її більш комплексною, інтегрованою та технологічною, що дає змогу не лише підвищити рівень безпеки, а й зміцнити конкурентні позиції організації, забезпечити її стійкість і довіру з боку партнерів, клієнтів та суспільства.

Основні напрями вдосконалення системи оцінки ефективності менеджменту безпеки організації подано на рис. 10.1.

Розробка та впровадження єдиних стандартів оцінювання передбачає створення уніфікованих підходів і критеріїв, які дозволяють здійснювати об'єктивне порівняння результатів між різними організаціями та сферами діяльності. Єдині стандарти забезпечують прозорість процесу оцінки, спрощують аналіз даних і сприяють формуванню єдиної методологічної бази для управлінських рішень. Вони допомагають уникати суб'єктивізму та різночитань у тлумаченні показників, а також формують передумови для гармонізації національних і міжнародних практик у сфері безпеки. Крім того, стандартизація робить результати оцінки більш надійними для зовнішніх користувачів – інвесторів, партнерів, регуляторних органів. У довгостроковій перспективі це підвищує довіру до організації та забезпечує сталий розвиток системи безпеки.

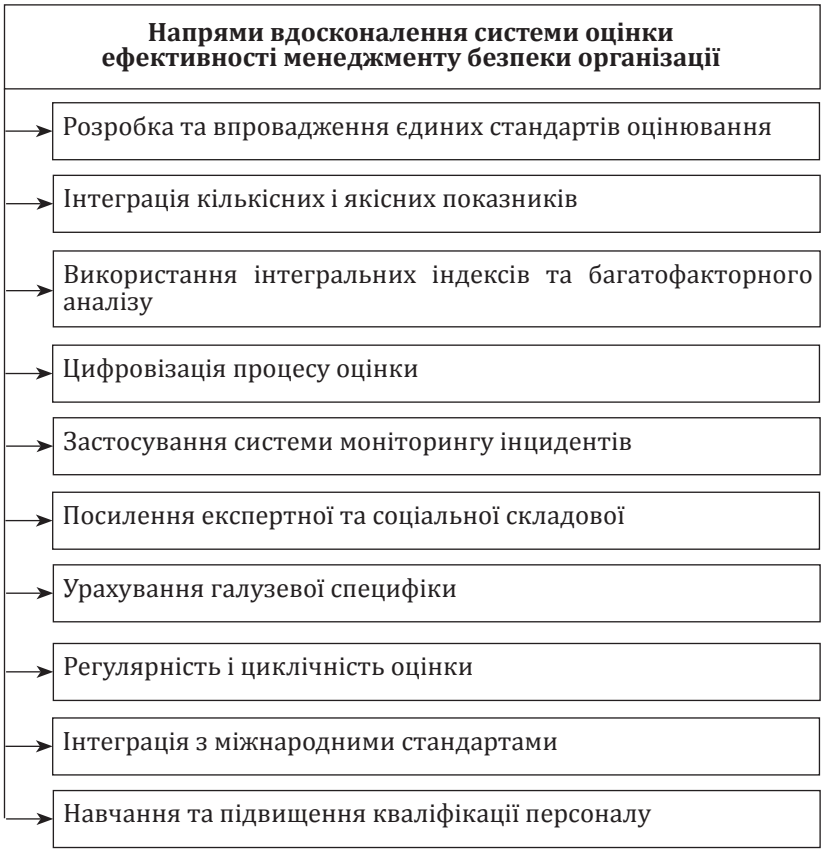


Рис. 10.1. Сукупність основних напрямів удосконалення системи оцінки ефективності менеджменту безпеки організації

Інтеграція кількісних і якісних показників передбачає поєднання об'єктивних даних, що виражаються у цифрах, зі суб'єктивно-експертними оцінками, які відображають соціальні, організаційні та репутаційні аспекти діяльності. Такий підхід дає змогу комплексно оцінити ефективність менеджменту безпеки, адже фінансові чи економічні результати без урахування соціальних факторів можуть створювати викривлену картину. Наприклад, зменшення витрат на безпеку може виглядати позитивним у кількісному вимірі,

але водночас негативно позначатися на довірі персоналу чи іміджі компанії. Інтеграція показників дозволяє отримати збалансований результат, що враховує як матеріальні, так і нематеріальні вигоди та ризики. Вона також забезпечує більшу точність у прогнозуванні, адже поєднання різних видів даних зменшує ймовірність однобічних висновків. У підсумку організація отримує більш повну інформацію для ухвалення стратегічних і оперативних рішень у сфері безпеки.

Використання інтегральних індексів та багатофакторного аналізу дає можливість отримати комплексну оцінку ефективності системи безпеки організації шляхом поєднання великої кількості показників у єдиний узагальнений критерій. Інтегральні індекси дозволяють звести різні кількісні та якісні дані до одного показника, що спрощує їх інтерпретацію та робить результати зрозумілими для керівництва. Багатофакторний аналіз, у свою чергу, дає змогу врахувати вплив одразу кількох змінних (фінансових, соціальних, організаційних) на загальний рівень безпеки, а також виявити приховані залежності між ними. Завдяки такому підходу можна визначити не лише факт досягнення певного результату, а й зрозуміти, які саме фактори зробили найбільший внесок у його формування. Крім того, інтегральні показники і моделі багатофакторного аналізу широко використовуються для прогнозування можливих сценаріїв розвитку ситуацій та оцінки ефективності управлінських рішень у довгостроковій перспективі. Внаслідок цього організація отримує більш обґрунтовану інформацію для стратегічного планування й оперативного реагування на загрози.

Цифровізація процесу оцінки означає перехід від традиційних паперових і ручних методів збору та обробки інформації до використання сучасних цифрових технологій. Такий підхід дозволяє здійснювати моніторинг ефективності системи безпеки в режимі реального часу, інтегрувати дані з різних джерел та оперативно реагувати на зміни у внутрішньому й зовнішньому середовищі. Застосування бізнес-аналітики, великих даних (Big Data), систем управління інцидентами та штучного інтелекту сприяє більш глибокому аналізу ризиків і виявленню прихованих закономірностей, які неможливо встановити традиційними методами.

Крім того, цифровізація забезпечує автоматизацію процесів оцінки, знижує ймовірність людських помилок і підвищує швидкість прийняття управлінських рішень. Вона створює можливості для формування інтерактивних дашбордів та індикаторів ефективності, доступних керівникам і фахівцям безпеки у зручному форматі. У довгостроковій перспективі цифрові технології допомагають підвищити точність прогнозів, оптимізувати витрати на безпекові заходи та забезпечити більш високий рівень прозорості управління. Таким чином, цифровізація стає не просто технічним нововведенням, а стратегічним інструментом удосконалення оцінки ефективності менеджменту безпеки організації.

Застосування систем моніторингу інцидентів. Сучасні організації дедалі активніше впроваджують автоматизовані системи моніторингу інцидентів, які базуються на технологіях SIEM (Security Information and Event Management) та комплексному кібермоніторингу. Їх використання допомагає в режимі реального часу відстежувати події, що можуть становити загрозу, і своєчасно виявляти відхилення від нормальної роботи системи. Такі інструменти не лише ідентифікують потенційні ризики, а й аналізують ефективність дій персоналу під час реагування на інциденти. Це створює можливості для вдосконалення внутрішніх регламентів, підвищення оперативності прийняття рішень та мінімізації негативних наслідків. У підсумку система безпеки стає більш гнучкою та здатною швидко адаптуватися до нових типів загроз.

Оцінювання ефективності менеджменту безпеки не може зводитися виключно до числових показників, оскільки значний вплив на результат має людський фактор. З цією метою дедалі активніше використовуються **експертні методики**, зокрема Delphi, а також анкетування й соціологічні опитування. Вони дають можливість з'ясувати рівень довіри персоналу до системи захисту, оцінити стан корпоративної культури та визначити внутрішні проблеми у взаємодії між працівниками й управлінцями. Залучення експертної та соціальної складової розширює межі оцінки, дозволяючи врахувати психологічні й поведінкові аспекти, які важко виміряти у фінансових чи економічних категоріях. Такий підхід робить оцінку більш комплексною та реалістичною, а також сприяє підвищенню довіри до управлінських рішень.

У перспективі це позитивно впливає на атмосферу в колективі, формує лояльність працівників і підтримує ділову репутацію організації.

Врахування галузевої специфіки означає адаптацію методик оцінювання ефективності менеджменту безпеки до особливостей конкретної сфери діяльності. У промисловості головний акцент робиться на техногенних ризиках та охороні праці, у фінансовій сфері – на кіберзагрозах та стабільності грошових потоків, у транспорті – на безпеці логістичних операцій. Завдяки такому підходу є можливість врахувати специфічні фактори ризику, характерні для певної галузі, та розробити релевантні індикатори оцінки. Внаслідок цього результати оцінювання стають більш точними та корисними для прийняття управлінських рішень, а система безпеки краще відповідає реальним умовам функціонування підприємства.

Регулярність і циклічність оцінки означає, що аналіз ефективності не повинен бути разовою дією, а має проводитися постійно у визначені проміжки часу. Це дає змогу відслідковувати зміни в динаміці, своєчасно виявляти нові загрози та запобігати накопиченню проблем. Циклічний підхід робить оцінку частиною управлінського процесу та забезпечує безперервність контролю. В результаті система безпеки стає більш стійкою і здатною швидко адаптуватися до змін зовнішнього середовища.

Інтеграція з міжнародними стандартами передбачає застосування у діяльності організації загальноприйнятих норм, таких як ISO 31000 (ризик-менеджмент), ISO 27001 (інформаційна безпека), COSO ERM та інші. Це дозволяє гармонізувати підходи до оцінки з провідними світовими практиками та зробити їх зрозумілими для зовнішніх партнерів. Дотримання міжнародних вимог підвищує довіру інвесторів, полегшує співпрацю з міжнародними структурами та сприяє відкритості бізнесу. У перспективі це зміцнює репутацію організації та створює передумови для масштабування на глобальних ринках.

Навчання та підвищення кваліфікації персоналу є важливим чинником ефективності системи оцінки безпеки. Підготовлені фахівці здатні правильно інтерпретувати результати оцінювання, використовувати сучасні методи

та застосовувати цифрові технології. Постійний розвиток знань і навичок підвищує рівень професійної відповідальності та зменшує ризик управлінських помилок. У кінцевому підсумку інвестиції в освіту персоналу підсилюють надійність системи безпеки та сприяють її сталому вдосконаленню.

Питання для самоконтролю

1. У чому полягає сутність оцінки ефективності менеджменту безпеки організації та чому вона є важливою в сучасних умовах?
2. Яку роль відіграє оцінка ефективності у стратегічному та оперативному управлінні організацією?
3. Які об'єкти задіяні в процесі оцінки ефективності менеджменту безпеки?
4. Які основні цілі переслідує організація, здійснюючи оцінювання результативності своєї системи безпеки?
5. У чому полягає зміст системно-управлінського, економіко-аналітичного, соціально-функціонального та інтегрального підходів до оцінки?
6. Які приклади кількісних показників ефективності можна навести та як вони розраховуються?
7. Чим якісні показники відрізняються від кількісних і чому їх використання є необхідним?
8. У чому перевага інтегральних критеріїв оцінювання та як вони поєднують різні аспекти безпеки?
9. Які основні методи та інструменти оцінки ефективності менеджменту безпеки застосовуються на практиці (економіко-статистичні, експертні, багатофакторні, цифрові)?
10. Які напрями удосконалення системи оцінки ефективності можна виділити і як вони впливають на розвиток організації?

Тестові завдання

1. Під оцінкою ефективності менеджменту безпеки організації розуміють:

а) процес перевірки фінансової звітності організації;

б) систематичний аналіз досягнутих результатів у сфері безпеки з урахуванням витрат, ризиків та цілей;

в) формальну перевірку виконання інструкцій;

г) встановлення штрафних санкцій за порушення окремих аспектів (видів) економічної безпеки організації.

2. Оцінка ефективності має важливе значення для стратегічного управління, тому що:

а) дозволяє перевірити документи служби безпеки;

б) формує базу для розробки довгострокових стратегій і визначення інвестицій у сферу безпеки;

в) виконує лише контрольні функції;

г) дає можливість карати відповідальних осіб.

3. Які об'єкти охоплює процес оцінювання ефективності менеджменту безпеки?

а) Лише фінансові ресурси, які знаходяться у довготривалому розпорядженні організації;

б) тільки технічні засоби;

в) організаційну структуру, ресурси (фінансові, матеріальні, кадрові), інформаційні потоки та зовнішнє середовище;

г) виключно нормативні документи, які регулюють фінансово-економічну діяльність організації.

4. Яка головна мета проведення оцінки ефективності системи безпеки?

а) Лише фіксація виконаних заходів;

б) виявлення невідповідностей у звітності;

в) оптимізація використання ресурсів, підвищення рівня захищеності та формування основи для нових управлінських рішень;

г) забезпечення покарання винних у порушеннях.

5. Який підхід передбачає аналіз управлінських процесів, планування, координації та контролю у сфері безпеки?

а) Економіко-аналітичний;

б) системно-управлінський;

в) соціально-функціональний;

г) інтегральний.

6. Економіко-аналітичний підхід до оцінки ефективності полягає у:

а) розробці стратегій комунікації з персоналом;

б) зіставленні витрат на заходи безпеки з економічними результатами та зниженням ризиків;

в) використанні соціологічних опитувань;

г) визначенні корпоративної культури.

7. Якісні показники оцінювання включають:

а) лише рівень збитків;

б) лише обсяг інвестицій;

в) організаційні, соціальні та репутаційні характеристики;

г) виключно кількість інцидентів.

8. Суть інтегральних критеріїв оцінювання полягає у:

а) фіксації витрат на безпекові заходи;

б) створенні узагальненого індикатора, що поєднує кількісні та якісні фактори для комплексної оцінки;

в) проведенні одноразових перевірок;

г) збиранні анкет від персоналу.

9. Які методи відносять до експертних у процесі оцінювання ефективності?

а) Delphi, рейтингові оцінки, соціологічні опитування;

б) аналіз витрат і результатів, коефіцієнтний аналіз;

в) сценарне моделювання та імітаційні моделі;

г) виключно використання SIEM-систем.

10. Який напрям удосконалення системи оцінки найбільше пов'язаний із впровадженням сучасних інформаційних технологій?

а) Використання кількісних показників;

б) інтеграція з міжнародними стандартами;

в) цифровізація процесу оцінки;

г) регулярність і циклічність аналізу.

Практичні завдання

Завдання 1.

ТОВ «Альфа-Логістик» у 2024 році інвестувало значні кошти у систему безпеки: впроваджено відеоспостереження, систему контролю доступу та програмне забезпечення кіберзахисту. Загальні витрати на ці заходи склали 2,5 млн грн. До впровадження системи середньорічні збитки компанії від крадіжок, кіберінцидентів та аварій становили близько 3,2 млн грн. За результатами року після модернізації безпеки втрати скоротилися до 1,1 млн грн.

1. Розрахуйте економічну ефективність заходів безпеки.

2. Визначте, чи виправдані інвестиції у безпекові технології.

3. Поясніть, які ще показники (крім фінансових) слід врахувати для комплексної оцінки ефективності.

Завдання 2.

У банківській установі «ФінКапітал» було проведено внутрішнє соціологічне опитування серед працівників щодо рівня довіри до системи безпеки. Виявлено, що 60% персоналу позитивно оцінюють організацію процесів кіберзахисту, але лише 40% вважають ефективними заходи кадрової безпеки. Крім того, було зафіксова-

но збільшення кількості конфліктів у колективі через недостатню комунікацію між службою безпеки та іншими підрозділами.

1. Визначте, які якісні показники необхідно вдосконалити для підвищення ефективності менеджменту безпеки.

2. Запропонуйте, які методи (експертні чи соціологічні) можна застосувати для більш точного вимірювання цих показників.

3. Обґрунтуйте, як поліпшення соціальної складової вплине на загальний рівень безпеки банку.

Завдання 3.

Компанія «ЕнергоТех» працює у сфері енергетики та стикається з численними ризиками: техногенні аварії, кібератаки, екологічні загрози і тиск з боку конкурентів. Керівництво вирішило провести оцінку ефективності системи безпеки, використовуючи методологію, яка поєднує кількісні, якісні та інтегральні критерії. Для цього були зібрані дані: фінансові витрати на безпеку, рівень втрат, показники соціальної довіри персоналу та оцінки зовнішніх експертів.

1. Поясніть, чому важливо застосовувати інтегральний підхід у цій галузі.

2. Запропонуйте приклад інтегрального індексу для оцінки ефективності та поясніть його структуру.

3. Визначте, як результати такої оцінки можуть вплинути на стратегічні рішення компанії.

ТЕМА 11
ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ БЕЗПЕКИ ОРГАНІЗАЦІЇ

11.1. Нормативно-правова база забезпечення безпеки організацій

11.2. Організаційна структура управління безпекою та її правове регламентування

Основні поняття і терміни: безпека, організація, економічна безпека, нормативно-правова база, положення, регламенти, підтримка безпеки організації, сфера безпеки, забезпечення безпеки, стандарти.

11.1. Нормативно-правова база забезпечення безпеки організацій

Нормативно-правова база – це сукупність законів, підзаконних актів, стандартів і внутрішніх положень, що створюють юридичне підґрунтя для організації, функціонування та контролю системи безпеки в організації. Вона формує юридичні межі діяльності, визначає права, обов'язки та відповідальність органів управління, служб безпеки й окремих працівників, а також закладає процедури, за якими здійснюється захист від загроз. Без чіткої правової бази система безпеки ризикує стати декларативною: недостатньо формалізованою, необґрунтованою та вразливою перед зовнішніми чи внутрішніми ризиками.

В Україні на сьогодні основним законом у цій галузі є Закон України «Про національну безпеку України», який визначає стратегічні засади, об'єкти захисту (людина, держава, суспільство), а також встановлює принципи демократичного цивільного контролю та верховенства права в секторі безпеки й оборони. Крім цього, важливим є законодавство щодо захисту персональних даних, інформаційної безпеки, охорони праці, цивільного захисту, а також нормативи, що встановлюють вимоги до критичної інфраструктури, –

всі вони разом створюють правове поле, в якому організація вибудовує свою внутрішню систему безпеки.

Організація, формуючи власну систему безпеки, повинна враховувати як загальнонаціональні нормативи, так і спеціалізовані акти, що стосуються сфер її діяльності. Наприклад, для підприємства, яке працює в об'єкті критичної інфраструктури або в галузі інформаційних технологій, буде актуальне виконання не лише базових законів про безпеку, але й спеціалізованих нормативів щодо кіберзахисту чи техногенної безпеки. Впровадження таких нормативів у внутрішні документи (політики, положення, процедури) дозволяє забезпечити не лише відповідність вимогам, але й ефективну правозастосовність: тобто щоб у разі перевірки або інциденту можна було чітко показати, що система безпеки має підґрунтя у вимогах закону.

Нормативно-правова база забезпечення безпеки організації виступає головним елементом (табл. 11.1), який допомагає перетворити управління безпекою із набору факультативних заходів у скоординований, документований і контрольований процес. Вона дає змогу деталізувати ролі, встановити процедури, формалізувати контроль і відповідальність, а також створити умови для аудиту, перевірки і вдосконалення системи безпеки.

Розвиток законодавчої бази України у сфері безпеки відбувається доволі повільними темпами, а наявні правові акти не завжди відповідають вимогам сучасного бізнес-середовища. Чинні норми часто мають узагальнений характер і лише поверхово регламентують питання організації охоронної діяльності на підприємствах. Додатковою проблемою є відсутність деталізованого переліку спеціальних засобів, якими може користуватися персонал охорони, що призводить до неоднозначності у практичному застосуванні законодавства.

Водночас державні інституції відіграють провідну роль у створенні безпечного середовища для суб'єктів господарювання та захисті їх економічних інтересів. Це реалізується через:

– формування правових механізмів захисту підприємств, включаючи охорону приватної власності та регулювання господарських відносин;

Таблиця 11.1

Нормативно-правова база забезпечення безпеки організації

Назва нормативного акта	Основні положення	Значення для організацій
Закон України «Про національну безпеку України»	Визначає основи та принципи національної безпеки, об'єкти захисту, повноваження суб'єктів сектору безпеки	Служить стратегічною рамкою для організацій, що діють у сфері безпеки та оборони; закладає принципи цивільного контролю
Закон України «Про основні засади забезпечення кібербезпеки України»	Встановлює правові засади кіберзахисту, функції держорганів та вимоги до суб'єктів критичної інфраструктури	Зобов'язує організації впроваджувати системи кіберзахисту та взаємодіяти з Нацкоординаційним центром кібербезпеки
Закон України «Про захист персональних даних»	Регламентує правила збору, зберігання й обробки персональних даних, права суб'єктів та обов'язки володільців	Організації повинні створювати політики захисту даних, призначати відповідальних осіб та вести реєстри обробки
Закон України «Про інформацію»	Встановлює принципи доступу до інформації, її класифікацію, захист та обмеження поширення	Організації отримують правила роботи з комерційною, службовою і таємною інформацією
Закон України «Про охорону праці»	Гарантує безпечні і здорові умови праці, визначає обов'язки роботодавця та права працівників	Організації зобов'язані забезпечувати інструктажі, оцінку ризиків та створювати системи охорони праці
Кодекс цивільного захисту України	Регламентує захист населення і територій від надзвичайних ситуацій техногенного і природного характеру	Організації мають розробляти плани евакуації, створювати системи оповіщення та проводити навчання персоналу
Правила пожежної безпеки в Україні (наказ МВС № 1417)	Встановлюють обов'язкові вимоги до пожежної безпеки на об'єктах	Організації повинні обладнувати будівлі протипожежними засобами, проводити інструктажі та перевірки
Закон України «Про критичну інфраструктуру»	Визначає основи захисту об'єктів критичної інфраструктури, принципи взаємодії державних і приватних суб'єктів	Організації, що належать до КІ, зобов'язані впроваджувати комплекс заходів безпеки та звітувати державі
Міжнародні стандарти (ISO 31000, ISO/IEC 27001)	Визначають принципи управління ризиками та побудови системи інформаційної безпеки	Використовуються як добровільна, але загальновизнана основа для організацій, що прагнуть міжнародної інтеграції

– протидію зловживанням монопольним становищем, запобігання недобросовісній конкуренції та контроль за цінами з метою збереження ринкової стабільності;

– правове врегулювання питань охорони інтелектуальної власності й захисту комерційної таємниці для гарантування інтелектуальної та інформаційної безпеки.

Забезпечення безпеки організації в правовому полі вимагає чіткого розподілу обов'язків і персональної відповідальності. Відповідальні особи – це не лише формальні керівники, а й уповноважені працівники, які мають конкретні функції у сфері правового регулювання безпеки, як-от:

1. Керівник організації:

– несе загальну відповідальність за стан безпеки та дотримання законодавства;

– затверджує внутрішні політики, положення та інструкції;

– забезпечує ресурсами службу безпеки і створює умови для її роботи.

2. Служба безпеки (керівник служби / CISO / начальник відділу безпеки):

– організовує виконання вимог законів і внутрішніх регламентів;

– здійснює моніторинг ризиків, веде реєстри інцидентів, контролює відповідність стандартам;

– відповідає за підготовку звітів керівництву та взаємодію з державними контролюючими органами.

3. Юридичний відділ / юрист:

– забезпечує правову експертизу внутрішніх документів;

– стежить за змінами у законодавстві та пропонує оновлення політик;

– бере участь у підготовці договорів із партнерами з урахуванням вимог безпеки (NDA, SLA, DPA).

4. HR-служба (кадрова безпека):

– відповідає за дотримання трудового законодавства у сфері охорони праці та безпеки;

– організовує інструктажі й навчання персоналу;

– здійснює контроль за дотриманням правил доступу та дисциплінарних норм.

5. Відповідальні особи за напрями (інформаційна безпека, пожежна безпека, охорона праці):

– призначаються наказом керівника;

– ведуть спеціальні журнали та реєстри (пожежна безпека, охорона праці, кіберзахист тощо);

– несуть персональну відповідальність у разі порушення вимог нормативних актів.

6. Кожен працівник організації:

– зобов'язаний дотримуватися внутрішніх інструкцій та правил;

– повідомляти про інциденти чи загрози;

– проходити обов'язкові навчання та перевірку знань з охорони праці, пожежної та інформаційної безпеки.

Правове забезпечення є фундаментом функціонування будь-якої системи безпеки, адже воно визначає межі допустимих дій, закріплює процедури захисту та встановлює відповідальність за їх порушення. Виконання вимог законодавства створює передумови для стабільної та прозорої діяльності організації, а також захищає її від штрафних санкцій, судових позовів і репутаційних втрат.

Дотримання правових норм дозволяє організації бути легітимним учасником ринку та підтверджує її надійність у відносинах із партнерами, клієнтами та державними структурами. Це особливо важливо в умовах інтеграції України у світові економічні й політичні процеси, де міжнародні стандарти безпеки та комплаєнсу мають першорядне значення.

Крім того, правове забезпечення відіграє ключову роль у захисті прав працівників та збереженні їхнього життя і здоров'я. Воно гарантує реалізацію принципів безпечних умов праці, захист персональних даних і прав на конфіденційність. Таким чином, правові механізми не лише обмежують, але й створюють можливості для розвитку культури безпеки в організації.

У довгостроковій перспективі системне дотримання правових вимог підвищує стійкість компанії до ризиків, зміцнює її ділову репутацію та формує конкурентні переваги. Це перетворює правове забезпечення із формальної вимоги на стратегічний ресурс, який забезпечує не лише захист, а й сталий розвиток організації.

Важливість дотримання правового забезпечення:

1. Захист від юридичної відповідальності – виконання норм законодавства знижує ризик накладення штрафів, кримінальних чи адміністративних санкцій.

2. Забезпечення легітимності діяльності – організація демонструє партнерам, клієнтам і державним органам прозорість і відповідність вимогам.

3. Зміцнення репутації та довіри – дотримання правових стандартів підвищує імідж компанії й робить її більш привабливою для інвесторів.

4. Захист прав працівників та клієнтів – правові норми гарантують безпечні умови праці, охорону здоров'я та захист персональних даних.

5. Зменшення ризиків і втрат – чітко прописані правила та процедури допомагають уникати помилок і своєчасно реагувати на загрози.

6. Інтеграція у міжнародний простір – дотримання українських законів у поєднанні з міжнародними стандартами (ISO, GDPR) сприяє виходу на глобальні ринки.

11.2. Організаційна структура управління безпекою та її правове регламентування

Організаційна структура управління безпекою – це система підрозділів, посад і функцій, які взаємопов'язані між собою та забезпечують комплексне виконання завдань зі захисту організації. Вона створює чіткий розподіл ролей і відповідальності, визначає канали підпорядкування та механізми координації дій у сфері безпеки. Її правове регламентування відбувається через внутрішні нормативні документи (статути, положення, інструкції, регламенти) та на основі чинних законів і стандартів України.

До структури управління безпекою входить:

1. Керівництво організації – формує загальну політику безпеки, затверджує положення й забезпечує ресурсами.

2. Служба безпеки (відділ/департамент) – здійснює оперативну реалізацію політики безпеки, координує роботу інших підрозділів, відповідає за моніторинг ризиків і реагування на інциденти.

3. Юридичний відділ – забезпечує правову експертизу, стежить за дотриманням законодавчих норм та бере участь у договорах, що містять безпекові умови.

4. HR-служба – відповідає за кадрову безпеку, навчання та інструктажі персоналу, контроль за дотриманням трудового законодавства.

5. IT-відділ / підрозділ кібербезпеки – займається захистом інформаційних систем, впроваджує заходи кіберзахисту та взаємодіє з національними структурами кібербезпеки.

6. Відповідальні особи за спеціальні напрями (охорона праці, пожежна безпека, цивільний захист, екологічна безпека) – діють на підставі наказів керівника, ведуть журнали обліку і несуть персональну відповідальність.

Кожен елемент структури повинен діяти в межах законодавчих вимог (закони України «Про охорону праці», «Про основні засади забезпечення кібербезпеки», «Про критичну інфраструктуру», Кодекс цивільного захисту тощо) та внутрішніх документів підприємства. Важливою складовою є також застосування міжнародних стандартів (ISO 31000, ISO / IEC 27001), які допомагають гармонізувати роботу підрозділів і роблять систему безпеки прозорою та зрозумілою для зовнішніх партнерів.

Сучасним організаціям для забезпечення високого рівня безпеки доцільно не лише дотримуватися вимог чинного законодавства, а й формувати власну внутрішню нормативну базу. Наявність внутрішніх актів, положень, інструкцій та регламентів дозволяє закріпити конкретні правила поведінки, визначити відповідальних осіб та чітко розподілити обов'язки у сфері безпеки. Такі документи роблять систему управління безпекою прозорою, контрольованою та зрозумілою для всіх працівників. Крім того, вони створюють основу для дисципліни, формують корпоративну культуру безпеки та допомагають швидше реагувати на потенційні загрози.

Внутрішні акти і документи для забезпечення безпеки в організації:

1. Положення про службу безпеки:

– визначає статус, функції, повноваження та підпорядкування підрозділу безпеки;

– регламентує взаємодію служби безпеки з іншими структурними підрозділами.

2. Політика безпеки організації:

– стратегічний документ, що окреслює цілі та принципи безпеки;

– містить загальні вимоги до інформаційної, фізичної, кадрової та фінансової безпеки.

3. Накази та розпорядження керівника:

– про призначення відповідальних осіб за пожежну, інформаційну, кадрову чи технічну безпеку;

– про затвердження планів охорони об'єктів, інструкцій та програм навчання персоналу.

4. Інструкції та правила внутрішнього порядку:

– інструкції з охорони праці та пожежної безпеки;

– правила доступу до приміщень, режиму секретності, збереження комерційної таємниці;

– інструкції з користування технікою, обладнанням та інформаційними системами.

5. Регламенти роботи з інформацією та даними:

– порядок зберігання, обробки та передачі конфіденційної інформації;

– правила роботи з персональними даними відповідно до Закону України «Про захист персональних даних»;

– процедури шифрування, резервного копіювання та знищення інформації.

6. Плани та програми реагування на надзвичайні ситуації:

– план евакуації працівників у разі пожежі чи техногенної аварії;

– порядок дій у разі кібератаки, витоку інформації чи інших інцидентів;

– інструкції щодо комунікації з державними органами у випадку надзвичайних подій.

7. Колективний договір та правила внутрішнього трудового розпорядку:

– містять норми щодо безпечних умов праці, відповідальності за порушення правил безпеки;

– закріплюють права працівників на захист та механізми вирішення конфліктних ситуацій.

8. Журнали обліку та звітні документи:

– журнал реєстрації інструктажів з охорони праці та пожежної безпеки;

– журнал реєстрації інцидентів і заходів реагування;
– акти перевірок, протоколи навчань і тренувань.

Організаційна структура управління безпекою є ключовим елементом ефективного функціонування підприємства, оскільки саме вона визначає порядок розподілу ролей, обов'язків і відповідальності між підрозділами та окремими працівниками. Чітко вибудувана структура дає змогу уникнути дублювання функцій, забезпечує координацію дій та створює умови для своєчасного реагування на можливі ризики чи загрози. Наявність структурованої системи підпорядкування підвищує рівень дисципліни, формує прозорі канали комунікації та допомагає зменшити невизначеність у прийнятті управлінських рішень.

Важливість структури також полягає в тому, що вона забезпечує єдність організаційних і правових механізмів безпеки. Завдяки формалізації у внутрішніх положеннях, інструкціях та регламентах структура управління стає інструментом правового захисту та контролю за виконанням вимог законодавства. Це дає змогу не лише підвищити захищеність персоналу і матеріальних ресурсів, а й забезпечити стійкість організації до зовнішніх викликів та конкурентного тиску. Тобто організаційна структура виступає не формальністю, а практичним інструментом зміцнення корпоративної безпеки та розвитку всієї системи управління.

Правове регламентування організаційної структури управління безпекою полягає у визначенні нормативних засад, на яких базується її функціонування. Воно включає як зовнішні джерела права – закони, кодекси, державні стандарти, так і внутрішні документи організації – положення, інструкції, накази та правила. Наявність таких регламентів забезпечує законність діяльності підрозділів безпеки, створює чітку систему відповідальності та підзвітності, а також сприяє інтегруванню вимог законодавства у повсякденну роботу організації.

Завдяки правовому регламентуванню досягається узгодженість між внутрішньою структурою управління та державними нормами, що гарантує легітимність управлінських рішень. Це також дозволяє мінімізувати правові ризики, уникати конфліктів із контролюючими органами

та забезпечувати дотримання міжнародних стандартів у сфері безпеки. До основних аспектів варто віднести:

1. Зовнішнє правове регулювання:

– закони України («Про національну безпеку», «Про охорону праці», «Про основні засади забезпечення кібербезпеки», «Про критичну інфраструктуру» тощо);

– кодекси (Цивільний, Господарський, Кодекс цивільного захисту України);

– державні стандарти та міжнародні норми (ISO 31000, ISO/IEC 27001).

2. Внутрішнє правове регламентування:

– положення про службу безпеки та інші підрозділи;

– накази та розпорядження керівника організації;

– інструкції з охорони праці, пожежної, кадрової, інформаційної безпеки;

– колективний договір, правила внутрішнього трудового розпорядку.

3. Функціональне регламентування:

– закріплення посадових обов'язків і відповідальності у посадових інструкціях;

– створення механізмів підзвітності та контролю;

– визначення процедур моніторингу, звітності та реагування на інциденти.

4. Комплаєнс та аудит:

– перевірка відповідності діяльності внутрішнім і зовнішнім нормам;

– документування процедур і ведення журналів обліку;

– регулярні аудити для підтвердження відповідності законодавству та стандартам.

Питання для самоконтролю

1. У чому полягає сутність організаційно-правового забезпечення системи безпеки організації?
2. Які основні законодавчі акти України регулюють питання безпеки підприємств та установ?
3. Чому нормативно-правова база є основою функціонування внутрішньої системи безпеки?

4. Які внутрішні документи (положення, інструкції, накази) формують правове підґрунтя безпеки організації?

5. Які основні елементи входять до організаційної структури управління безпекою?

6. У чому полягає важливість правового регламентування діяльності служби безпеки?

7. Які принципи доцільно враховувати при формуванні структури управління безпекою організації?

8. Яку роль відіграють державні органи у правовому забезпеченні економічної безпеки підприємств?

9. Які ризики може мати організація у разі недотримання вимог законодавства у сфері безпеки?

10. Як міжнародні стандарти (ISO, GDPR, NIST тощо) впливають на вдосконалення правового регламентування безпеки в українських організаціях?

Тестові завдання

1. Який документ визначає загальні засади національної безпеки України?

а) Закон України «Про охорону праці»;

б) Закон України «Про національну безпеку України», що встановлює принципи, об'єкти захисту та систему державних органів у сфері безпеки;

в) Господарський кодекс України;

г) Наказ МВС про пожежну безпеку.

2. Основою організаційної структури управління безпекою на підприємстві є:

а) лише кадрова служба;

б) служба безпеки та внутрішні регламенти, які визначають права, обов'язки та відповідальність усіх підрозділів у сфері безпеки;

в) бухгалтерія та фінансовий відділ;

г) тільки накази керівника підприємства.

3. Які документи належать до внутрішніх актів з безпеки?

а) Конституція України;

б) положення про службу безпеки, інструкції з охорони праці, правила пожежної безпеки, накази керівника про призначення відповідальних осіб;

в) міжнародні стандарти ISO;

г) господарський договір із контрагентом.

4. Який принцип лежить в основі побудови організаційної структури управління безпекою?

а) Випадковий розподіл функцій між підрозділами;

б) системність та ієрархічність, що забезпечують взаємопов'язаність усіх елементів і чітке підпорядкування;

в) виключно економічна вигода;

г) відсутність чітких правил підпорядкування.

5. Яку роль відіграють державні органи у забезпеченні правової основи безпеки підприємств?

а) Лише контролюють пожежну безпеку;

б) формують правовий захист бізнесу, запобігають зловживанням монополістів, регламентують захист інтелектуальної власності та комерційної таємниці;

в) виключно займаються фінансовим аудитом;

г) не мають впливу на діяльність приватних компаній.

6. Які ризики виникають у разі недотримання правових норм у сфері безпеки?

а) Лише дрібні організаційні проблеми;

б) штрафи, кримінальна чи адміністративна відповідальність, втрата репутації, відмова партнерів від співпраці та зростання внутрішніх загроз;

в) нічого серйозного, усі ризики можна уникнути;

г) тільки зниження продуктивності праці.

7. Які міжнародні стандарти найчастіше застосовуються для посилення системи правового забезпечення безпеки?

а) ISO 9001, що стосується менеджменту якості;

б) ISO 31000 з управління ризиками та ISO/IEC 27001 з інформаційної безпеки, які встановлюють вимоги для організацій різних галузей;

в) лише внутрішні стандарти підприємства;

г) будь-які локальні правила, які вигадує керівник.

8. Які документи регулюють порядок роботи з персональними даними в організації?

а) Закон України «Про інформацію» без деталізації;

б) Закон України «Про захист персональних даних» у поєднанні з внутрішніми регламентами та політиками захисту інформації;

в) Господарський кодекс України;

г) тільки наказ керівника підприємства.

9. За моніторинг інцидентів і реагування на загрози відповідає такий елемент структури безпеки, як:

а) бухгалтерія;

б) служба безпеки або спеціальний департамент, що займається захистом організації та координує роботу інших підрозділів;

в) юридичний відділ;

г) відділ маркетингу.

10. Чому важливим є поєднання зовнішнього та внутрішнього правового регламентування системи безпеки?

а) Тому що це збільшує кількість документів для перевірок;

б) тому що забезпечується одночасна відповідність вимогам державного законодавства та внутрішнім правилам організації, що робить систему безпеки легітимною і практично дієвою;

в) бо так простіше вести кадрову документацію;

г) це дає можливість уникати контролюючих органів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акімова Н. С., Кирильєва Л. О., Наумова Т. А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. *Підприємництво і торгівля*. 2023. Вип. 35. С. 510. URL: https://doi.org/10.32782/2522-1256-2023-35-01
2. Ареф'єва О. В., Кузьменко Т. Б. Економічні основи формування фінансової складової економічної безпеки. *Актуальні проблеми економіки*. 2013. №1 (91). С. 98.
3. Балицька М., Паржицька М. Сучасні методи оцінки кредитоспроможності позичальників-юридичних осіб банками України. *Herald of Khmelnytskyi National University. Economic sciences.* 2022. Т. 306. № 3. С. 36–42.
4. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення): монографія. Київ : Київський національний торгово-економічний університет, 2014. 759 с.
5. Бланк І. А. Управління фінансовою безпекою підприємства. Київ : Ніка-Центр, 2014. 784 с.
6. Босак А. О., Далик В. П., Мазник Ю. І., Туліка С. К., Мацевко Б. В., Прокопів М. В., Старецький А. О. Кадрова безпека у системі економічної безпеки підприємства. *Інтернаука : міжнародний науковий журнал. Серія: Економічні науки*. 2023. № 10. URL: doi: https://doi.org/10.25313/2520-2294-2023-10-9165
7. Васильєва С. Аналіз сутності системи інвестиційної безпеки підприємства. *Цифрова економіка та економічна безпека*. 2022. № 3 (03). С. 3-7. URL: https://doi.org/10.32782/dees.3-1.
8. Васькова Ю. І. Фінансова безпека підприємства – провідна складова економічної безпеки та засіб попередження кризи підприємств. *Наука й економіка*. 2017. Вип. 1. С. 230–239.
9. Воронка О. З., Шевченко Н. В. Формування інвестиційної стратегії в умовах кризових ситуацій для забезпечення інноваційно-безпекового потенціалу підприємства. *Актуальні питання економічних наук.* 2025. № 14. URL: https://doi.org/10.5281/zenodo.16971013
10. Гармаш С. Кадрова безпека як економічна категорія в аспекті економічної безпеки підприємства (понятійний апарат та функції). *Вісник Національного технічного університету*

«Харківський політехнічний інститут». Серія: Економічні науки. 2022. №. 4. С. 44–49.

11. Гудзь О. Є. Інвестиційна безпека та кібердипломатія: шлях до економічного відновлення України. *Актуальні проблеми сталого розвитку*. 2025. Т. 2. №. 2. С. 136–144.
12. Гуменюк О. Г. Використання SWOT-аналізу як основного інструменту стратегічного управління. Глобальні та національні проблеми економіки. 2017. № 17. С. 281–285.
13. Гунченко О. М., Волошкіна О. С., Кравченко М. В., Корінний В. І. Система управління екологічною безпекою – як одна зі складових енергоефективності. *Екологічна безпека та природні ресурси*. 2020. № 36 (4). С. 5–19. URL: https://doi.org/10.32347/2411-4049.2020.4.5-19
14. Дейнега О. В. Інформаційна безпека підприємств в умовах глобалізації 4.0. *Економіка та суспільство*. 2019. Вип. 20. С.70-79.
15. Дем'янчук О., Хохонік К. Механізм управління фінансовою безпекою підприємства. *Таврійський науковий вісник. Серія: Економіка*. 2023. № 15. С. 167–171. URL: https://doi.org/10.32782/2708-0366/2023.15.20
16. Дем'янчук О., Дзюрах Ю., Лещенко Д. Оцінка рівня фінансової безпеки України. *Scientific Notes of Ostroh Academy National University. «Economics» Series*. 2024. №. 32 (60). С. 75–80.
17. Живко З. Б., Томаневич Л. М., Дудюк В. С., Копитко М. І. Менеджмент безпеки персоналу : конспект лекцій. Львів : Ліга-Прес, 2012. 204 с.
18. Загорельська Т. Ю. До проблеми формування системи управління фінансовою безпекою на підприємстві. *Вісник ДНУ. Серія В: Економіка і право*. Вип. 2. 2013. С. 247–253.
19. Ілляшенко О. В., Будрик О. І. Еколого-економічна безпека підприємства: теоретичні аспекти. *Економічна стратегія і перспективи розвитку сфери торгівлі та послуг*. 2017. Вип. 1 (25). С. 72–82.
20. Інформаційна безпека в умовах воєнного стану / Д. В. Смотрич, Л. Бріалко // *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 77. С. 121–127.
21. Караїм О. А. Менеджмент безпеки та екологічний менеджмент: інтеграція для сталого розвитку. *Сучасні технології менеджменту :* матеріали Міжнародної наук.-практичної конференції (18–20 жовтня 2024 р.). Луцьк, 2024. С. 136–139.
22. Кицюк В. М., Пупинін О. С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*. 2024. №. 2. С. 103–108.

23. Кодекс цивільного захисту населення від 02.10.2012 р. № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text
24. Комплексне забезпечення економічної безпеки підприємств : монографія / С. М. Лаптєв, В. Г. Алькема, В. С. Сідак, М. І. Копитко ; за ред. М. І. Копитко Київ : ВНЗ «Університет економіки та права «КРОК», 2017. 508 с.
25. Копитко М. І., Мойса Т. В. Інвестиційна безпека підприємства в умовах актуалізації зовнішньоекономічних ризиків і євроінтеграційних процесів. *Наукові інновації та передові технології*. 2024. Т. 2. С. 30.
26. Копитко М. І., Барановський О. І., Барилюк М.-М. Р. Використання методу таксономії для оцінки рівня фінансової безпеки комерційного банку. *Фінансово-кредитна діяльність: проблеми теорії та практики :* збірник наукових праць, 2018. Т. 1. № 24. С. 4–14.
27. Копитко М. І. Вплив факторів кадрової сфери на економічну безпеку підприємств з виробництва транспортних засобів. *Вчені записки Університету «КРОК».* 1997. Вип. 1. Вип. 38. Київ, 2014. С. 86–98.
28. Копитко М. І., Левків Г. Я. Вплив корпоративної культури на рівень лояльності працівників у процесі забезпечення економічної безпеки підприємств. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна : збірник наукових праць / голов. ред. В. В. Середа. Львів : ЛьвДУВС, 2016. Вип. 2. С. 187–200.
29. Копитко М. І., Ільків Ю. І. Основи безпекової діяльності підприємства: теоретичний аспект. *Вчені записки Університету «КРОК».* 2020. № 4 (60). С. 75–81.
30. Копитко М. І., Бабій Л. І., Співак С. І., Сарана А. О. Фінансово-безпекова та інвестиційна складові вибору інноваційно орієнтованого підприємства-аналога при розрахунку вартості бізнесу в умовах глобалізації, діджиталізації та управління змінами. *Формування ринкових відносин в Україні.* 2022. № 7–8 (254–255). С. 68–73. URL: https://doi.org/10.5281/zenodo.7323307
31. Копитко М. І., Мойса Т. В. Маркетингові інструменти формування інноваційно-безпекового потенціалу підприємства. *Актуальні питання в сучасній науці*. 2023. № 9 (15). С. 25–33. URL: https://doi.org/10.52058/2786-6300-2023-9(15)-25-33
32. Копитко М. І. Економічна безпека підприємств з виробництва транспортних засобів : монографія. Львів : Ліга-Прес, 2015. 556 с.
33. Копитко М. І. Економічна безпека промислових підприємств у процесі здійснення інноваційної діяльності. *Systemy i środki*

transportu samochodowego. Wybrane zagadnienia. Seria: Transport : monografia Politechniki Rzeszowsk'ej im. Ignacego Łukasiewicza. № 4 / pod redakcją naukową Kazimierza Lejdy. Poland, Rzeszów : Politechnika Rzeszowska, 2013. С. 457–472.

34. Копитко М. І. Моделювання впливу персоналу на рівень економічної безпеки підприємств з виробництва транспортних засобів. *Problems of social and economic development of busines :* collective monograph. Montreal, Canada : Publishing house «BREEZE», 2014. С. 293–298.
35. Копитко М. І. Організаційно-управлінський механізм гарантування економічної безпеки промислових підприємств в Україні. Сучасні тенденції управління розвитком організаційно-економічних систем (новий погляд) : кол. монографія / за заг. ред. Р. Р. Тімірталєєвої ; Республіканський ВНЗ «Кримський гуманітарний університет». Сімферополь : ВД «АРІАЛ», 2014. С. 523–538.
36. Копитко М. І. Соціально-економічна безпека підприємств в постіндустріальній економіці: національний та європейський аспект. Вплив війни на соціально-економічні системи: безпековий аспект : кол. монографія / за заг. ред. М. І. Копитко., З. Р. Кісіль. Львів : ЛьвДУВС, 2024. С. 142–176. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/7280 https://doi.org/10.32782/2311-844X/2024-monograph
37. Копитко М. І. Менеджмент інформаційних ресурсів та інформаційна безпека підприємств : навчально-методичний посібник. Львів : Ліга-Прес, 2016. 172 с.
38. Копитко М. І. Основи економічної безпеки : курс лекцій. Львів : ЛьвДУВС, 2024. 346 с.
39. Копчак Ю., Лобунець Т., Луковський Р. Swot-аналіз як важливий інструмент у розробці стратегії бізнесу. Еконо*міка та суспільство.* 2024. № 61. URL: https://doi.org/10.32782/2524-0072/2024-61-146
40. Кравченко В. О. Кадрова безпека – основа економічної безпеки підприємства. *Соціально-трудові відносини: теорія та практика.* 2014. № 1. С. 301–305.
41. Кравчук П. Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. *Науковий вісник Волинського державного університету ім. Лесі Українки*. 2005. № 1. С. 165–170.
42. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. *Збірник наукових праць ДВНЗ «КНЕУ ім. Вадима Гетьмана».* 2021. С. 26–28.
43. Малій О. Г., Широкорад Р. А. Ризик-менеджмент в кредитній діяльності банків. *Bulletin of the Black Sea Littoral*. 2024. Т. 63. С. 71.

44. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика : монографія. Львів : Растр-7, 2020. 384 с.

45. Мельник С. І., Шевченко Н. В., Висоцька І. Б. Банківська система : навчальний посібник у схемах і таблицях. Львів : Львівський державний університет внутрішніх справ, 2023. 184 с.

46. Мехеда Н. Г., Маренич А. І. Соціально-мотиваційні складові кадрової безпеки. *Фінансовий простір*. 2012. № 2(6). С. 38–45.

47. Національний банк України. *Офіційний сайт*. URL: https://bank.gov.ua

48. Національна комісія з цінних паперів та фондового ринку. *Офіційний сайт*. URL: https://www.nssmc.gov.ua

49. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського університету*. 2012. Вип. 18. С. 170–173.

50. Організація наукових досліджень у сфері менеджменту та безпеки організації : підручник / В. Бліхар, О. Омельчук, В. Вовк, М. Бліхар, М. Копитко, М. Верескля, Н. Михаліцька. Хельницький : Видво ХУУП імені Леоніда Юзькова, 2022. 443 с.

51. Ортинський В. Л., Керницький І. С., Живко З. Б., Керницька М. І., Живко М. О. Економічна безпека підприємств, організацій, установ : навчальний посібник. Київ : Правова єдність, 2009. 544 с.

52. Ортинський В. Л., Керницький І. С., Живко З. Б., Копитко М. І., Гук О. В., Шимечко Г. І., Живко М. О. Економічна безпека підприємств : підручник. Київ : Алерта, 2011. 704 с.

53. Подра О. П., Левків Г. Я., Копитко М. І. Теоретичні засади формування системи економічної безпеки підприємства. *Вісник Хмельницького національного університету*. 2019. № 3. С. 136–140.

54. Пушак Я. Я., Шевченко Н. В. Особливості формування та управління ресурсами банків в сучасних умовах. *Економічний Вісник Донбасу*. 2022. Вип. 3 (69). С. 36–41. URL: https://doi.org/10.12958/1817-3772-2022-3(69)-36-40

55. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

56. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

57. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

58. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
59. Про охорону праці : Закон України від 14.10.1992 р. № 2694-XII. URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text
60. Про затвердження Правил пожежної безпеки в Україні : Наказ МВС України від 30.12.2014 р. № 1417. URL: https://zakon.rada.gov.ua/laws/show/z0252-15#Text
61. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-XI. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
62. Савіцька С. І. Інвестиційна складова економічної безпеки України в умовах війни. *Подільський вісник: сільське господарство, техніка, економіка*. 2023. № 38. С. 150–153.
63. Ситник О. О. Методи оцінки кредитоспроможності підприємства. *Economic Synergy*. 2024. №. 4. С. 269-285.
64. Ситник Н. С., Репета М. М. Інвестиційна безпека України: стан і перспективи вдосконалення. *Бізнес Інформ*. 2018. № 11. С. 100–106.
65. Солодовнік О. О., Докуніна К. І. Оцінка кредитоспроможності позичальника: аналіз основних підходів. *Інфраструктура ринку.* 2021. № 53. С. 140-145.
66. Черчик Л. М. Екологічна безпека в системі менеджменту підприємства. *Економічний часопис Волинського національного університету імені Лесі Українки*. № 1 (17). 2019. 55–61. URL: https://doi.org/10.29038/2411-4014-2019- 01-55-61.
67. Федина В. В. Кредитний ризик банку: сутність та причини виникнення. *Підприємництво і торгівля*. 2023. № 39. С. 223–228.
68. Фінансовий менеджмент : електронний навчальний посібник / І. А. Бігдан, Л. І. Лачкова, В. М. Лачкова, О. В. Жилякова. Харків : ХДУХТ, 2017. 197 с.
69. Хома І., Лук'янський О. Теоретико-методологічні аспекти вдосконалення управління кредитним ризиком в банку. *Сталий розвиток економіки*. 2024. № 2 (49). С. 295–301.
70. Шевченко Н., Копитко М., Мігус І. Напрями зниження рівня корупції в Україні в умовах кризових явищ та підвищення необхідності легалізації доходів. *Вчені записки Університету «КРОК».* 2023. № 1 (69). С. 21–28. URL: https://doi.org/10.31732/2663-2209-2022-70-21-28
71. Шевченко Н., Копитко М., Захаров О. Роль міжнародної співпраці державних органів у сфері зниження та управління рівнем корупції в Україні. *Вчені записки Університету «КРОК».* 2023.

№ 3 (71). С. 38–45. URL: https://doi.org/10.31732/2663-2209-2022-71-38-45

72. Шевченко Н., Леськів Г., Горбан І., Марченко О. Інноваційні підходи до управління корпоративною безпекою підприємств в сучасних умовах. *Ефективна економіка*. 2024. № 11. URL: https://www.nayka.com.ua/index.php/ee/article/view/5096
73. Шевченко Н., Копитко М. Проблеми управління ризиками і кредитною безпекою в умовах формування війни та економічної нестабільності. *Вчені записки Університету «КРОК».* 2024. № 4 (76). С. 287–294. URL: https://doi.org/10.31732/2663-2209-2024-76-287-294
74. Шевченко Н. В., Пушак Я. Я. Управління операційною стратегією підприємства як складова забезпечення його безпеки та прибутковості: теоретичний аспект. *Вісник економічної науки України*. 2024. № 2 (47). С. 83–88.
75. Шевченко Н., Копитко М. Управління проєктами як складова операційного менеджменту та забезпечення достатнього рівня фінансової безпеки підприємства. *Соціальна економіка*. 2025. № 70 (2). URL: https://doi.org/10.26565/2524-2547-2025-70-08
76. Шевченко Н. В. Управління кризовими ситуаціями та ризиками в організації: безпековий аспект. *Актуальні питання економічних наук*. 2025. № 14. URL: https://doi.org/10.5281/zenodo.16938196
77. Шевченко Н. В. Зміцнення економічної безпеки роздрібних торговельних підприємств у контексті легалізації їх діяльності. Легалізація економіки в забезпеченні економічної безпеки суб'єктів господарювання та держави : кол. монографія / за ред. І. О. Ревак. Львів : СПОЛОМ, 2021. С. 93–102.
78. Шевченко Н. В., Огірко О. І. Напрями забезпечення лістингу цінних паперів на вітчизняному фондовому ринку оцінки економічних ризиків для прийняття рішень щодо інвестування. *Інфраструктура ринку*. 2021. № 53. URL: http://www.market-infr.od.ua/uk/2021
79. Шевченко Н. В., Галайко Н. В. Напрями оцінки факторів, що впливають на рівень корупції в Україні. *Вісник Одеського Національного Університету. Серія економічна.* 2022. Т. 2. Вип. 2 (92). С. 67–73. URL: https://doi.org/10.32782/2304-0920/2-92-11
80. Шевченко Н. В., Мельник С. І. Фінансовий менеджмент : навчальний посібник у схемах і таблицях. Львів : Львівський державний університет внутрішніх справ, 2022. 224 с.
81. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ. *Актуальні проблеми економіки*. 2004. № 1. С. 220–225.

82. Шира Т. Б. Корпоративна безпека підприємств в Україні: визначення ключових загроз. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Економіка і управління*. 2018. Т. 29 (68). № 6. С. 93–96.
83. Шостак Л. В. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека : науково-практичний журнал*. 2024. № 5 (14). С. 160–165. URL: https://doi.org/10.32782/dees.14-25.
84. Шульга В. І. Сучасні підходи до трактування поняття «інформаційна безпека». *Ефективна економіка*. 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514
85. Якименко Ю. М., Савченко В. А., Легомінова С. В. Системний аналіз інформаційної безпеки: сучасні методи управління : підручник. Київ : Державний університет телекомунікацій, 2022. 308 с.
86. Яковенко Р. В. Тлумачний англо-український словник економічних термінів з елементами теорії та проблематики. *Дидактичний довідник*. Вид. 2-ге, випр. Кіровоград : Видавець Лисенко В. Ф., 2015. 130 с.
87. Яременко О. Ф. Кадрова безпека підприємства: концептуальні основи забезпечення. *Вісник Хмельницького національного університету.* 2016. № 2. Т. 1. С. 29–32.
88. Altomonte L. The best SWOT analysis software of 2024. Safety Culture. 2024. URL: https://safetyculture.com/app/swot-analysis-software
89. Blikhar M., Vovk V., Shevchenko N., Kokhaniuk T. & Dobosh Z. Directions of offense prevention in the stock market of Ukraine. *Financial and credit activity: problems of theory and practice*. 2021. № 3 (38). С. 437–446. URL: https://doi.org/10.18371/fcaptp.v3i38.237476
90. Blikhar M., Vinichuk M., Patsula O., Shevchenko N. Methods of Assessing the level of Market capitalization of joint-stock companies: economic and managerial aspect. *Economic. Ecology. Socium*. 2022. Vol. 6. No. 4. Pp. 65–75. URL: https://ees-journal.com/index.php/journal/article/view/205/167
91. Blikhar V., Kopytko M., Lychenko I., Vinichuk M., Polishchuk R. Assessment of the level of economic security of innovative enterprises: economic and legal aspect. *Financial and Credit Activity: Problems of Theory and Practice*. 2021. 3(38). С. 240–248. URL: https://doi.org/10.18371/fcaptp.v3i38.237453
92. Kopytko M., Ilkiv Yu. Mechanism of Enterprise Security Activity Management of Innovation-Active Enterprise: Summary and Structure. *Social and Legal Studios*. 2020 3(2). С. 119–129. URL: https://doi.org/10.32518/2617-4162-2020-2-119-129

93. Kopytko M., Fleychuk M., Veresklia M., Petryshyn N., Kalynovskyy A. Management of security activities at innovative-active enterprises. *Business: Theory and Practice*. 2021. Vol. 22. P. 299–309.
94. Kopytko M., Górska M. Management of innovative development at the enterprise, taking into account ensuring a high level of personnel security. *Zeszyty naukowe*. 2025. № 50. Pp. 43–51.
95. Kopytko M., Liubokhynets L., Panchenko V., Moysa T., Malanchuk A. Formation of a personnel management system as a factor of increasing competitiveness and the enterprise security level in the context of digital transformation and new legal challenges. *Social & Legal Studios.* 2024. № 7(1). Pp. 210–220.
96. Kopytko M., Liubokhynets L., Kalinin A., Sai L., Bala O. Personnel management in the system of ensuring safety and security of the engineering enterprise in the conditions of industry 4.0. *International Journal of Safety and Security Engineering*. 2023. Vol. 13. № 3. Pp. 547–554. URL: https://doi.org/10.18280/ijsse.130317
97. Kotler P., Keller K. L. Marketing management (Global Edition, 15th ed.). 2021. URL: https://www.edugonist.com/wp-content/uploads/2021/09/Marketing-Management-by-Philip-Kotler-15th-Edition.pdf
98. Mihus I., Koval Ya., Laptev S., Bala O., Kopytko M. Monitoring in the system of state anti-crisis management of economic security of the banking institution of Ukraine. *Business: Theory and Practice*. 2020. № 21(2). Pp. 804–812. URL: https://doi.org/10.3846/btp.2020.12985
99. Shevchenko N., Marchenko O., Horban I., Leskiv H., Voronka O. Directions of profitability management of Ukrainian insurance companies in the process of minimizing risks and ensuring economic security. *Polish journal of science*. 2025. № 85. URL: https://doi.org/10.5281/zenodo.15253975
100. Shevchenko N., Kopytko M. Bank profitability management in the context of financial risk management in the context of industry 4.0. *Economics, Finance and Management Review*. 2025. № 2 (22). Pp. 153–162. URL: https://doi.org/10.36690/2674-5208-2025-2-153-162
101. SWOT-аналіз соціо-економіко-екологічного стану підприємств : конспект лекцій / уклад. І. Ю. Аблєєва. Суми : Сумський державний університет, 2020. 233 с.

ДОДАТКИ

Додаток А

Порівняння різних видів аналізу безпеки організації

№	Назва	Опис	Сильні сторони	Слабкі сторони
1	*2*	*3*	*4*	*5*
1	SWOT Analysis	Аналіз сильних та слабких сторін, можливостей та загроз. Дозволяє компаніям оцінити внутрішні ресурси та зовнішні виклики.	Простота у використанні, визначення внутрішніх і зовнішніх факторів, що впливають на успіх.	Суб'єктивність оцінок, може не відображати всі ключові загрози чи можливості без глибокого аналізу.
2	PESTEL Analysis	Аналіз політичних, економічних, соціокультурних, технологічних, екологічних та правових факторів, що впливають на організацію.	Охоплення широкого спектру зовнішніх факторів, допомагає організаціям адаптуватися до макроекономічних змін.	Може бути часозатратним, не враховує внутрішні ресурси компанії.
3	Porter's 5 Forces	Аналіз п'яти конкурентних сил, які формують галузь: конкуренція, загроза нових учасників, загроза замінників, переговорна сила покупців та постачальників.	Допомагає розуміти структуру галузі, ідентифікувати основні джерела конкурентної боротьби.	Менш ефективний у швидкозмінних або інноваційних галузях, може недооцінювати роль нових технологій.
4	McKinsey 7S	Фреймворк (набір інструментів), який аналізує сім ключових елементів компанії: стратегію, структуру, системи, спільні цінності, стиль, персонал, навички.	Охоплює внутрішню координацію і взаємозв'язок всіх аспектів організації.	Складність у впровадженні, потребує детального аналізу всіх компонентів.
5	Porter's Value Chain	Аналіз внутрішніх активностей компанії для ідентифікації джерел створення цінності та конкурентних переваг.	Покращує розуміння внутрішніх процесів, сприяє оптимізації та зниженню витрат.	Може бути обмеженим при змінах зовнішнього середовища, оскільки зосереджений лише на внутрішніх процесах.
6	Business Model Canvas	Візуальне представлення ключових аспектів бізнес-моделі, включаючи ціннісні пропозиції, клієнтів, канали, відносини та джерела доходів.	Легко використовувати для ітеративного планування та стратегічних змін.	Може бути занадто спрощеним для складних бізнес- структур.

1	*2*	*3*	*4*	*5*
7	Boston Consulting Group Matrix	Аналіз портфеля продуктів або бізнес-одиниць на основі ринкового зростання та частки для визначення стратегічних пріоритетів	Чітко визначає пріоритетні напрямки для інвестицій та ресурсів.	Може не враховувати зміни в ринкових умовах або конкурентних діях.
8	Pareto Analysis	Використовує принцип 80/20 для ідентифікації критичних проблем, які впливають на результати.	Допомагає визначити ключові фактори успіху або проблеми.	Може вести до ігнорування менш видимих, але важливих проблем.
9	Strategy Canvas	Візуалізація конкурентного позиціонування компанії порівняно з ринковими гравцями на основі різних факторів цінності.	Покращує розуміння стратегічного становища компанії, допомагає виділити унікальні аспекти.	Потребує глибоких знань ринку та конкурентних стратегій.
10	Scenario Analysis	Розробка різних можливих майбутніх сценаріїв і планування відповідей на них.	Допомагає підготуватися до непередбачених змін, забезпечує гнучкість стратегічного планування.	Може бути ресурсозатратним і вимагати значних зусиль для розробки реалістичних сценаріїв.

Додаток Б

Баланс підприємства (Форма № 1)

Дата (рік, місяць, число)

Підприємство_____ за ЄДРПОУ

Територія_____ за КАТОТТГ[1]

Організаційно-правова форма господарювання_____ за КОПФГ

Вид економічної діяльності_____ за КВЕД

Середня кількість працівників[2]_____

Адреса, телефон_____

Одиниця виміру: тис. грн. без десяткового знака (окрім розділу IV Звіту про фінансові результати (Звіту про сукупний дохід) (форма № 2), грошові показники якого наводяться в гривнях з копійками)

Складено (зробити позначку «v» у відповідній клітинці):
за національними положеннями (стандартами) бухгалтерського обліку
за міжнародними стандартами фінансової звітності

Баланс (Звіт про фінансовий стан)
на _____ 20__ р.

Актив	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	2	3	4
I. Необоротні активи			
Нематеріальні активи	1000		
первісна вартість	1001		
накопичена амортизація	1002		
Незавершені капітальні інвестиції	1005		
Основні засоби	1010		
первісна вартість	1011		
знос	1012		
Інвестиційна нерухомість	1015		
Довгострокові біологічні активи	1020		
Довгострокові фінансові інвестиції: які обліковуються за методом участі в капіталі інших підприємств	1030		
інші фінансові інвестиції	1035		
Довгострокова дебіторська заборгованість	1040		
Відстрочені податкові активи	1045		
Інші необоротні активи	1090		
Усього за розділом I	**1095**		

1	2	3	4
II. Оборотні активи			
Запаси	1100		
Поточні біологічні активи	1110		
Дебіторська заборгованість за продукцію, товари, роботи, послуги	1125		
Дебіторська заборгованість за розрахунками: за виданими авансами	1130		
з бюджетом	1135		
у тому числі з податку на прибуток	1136		
Інша поточна дебіторська заборгованість	1155		
Поточні фінансові інвестиції	1160		
Гроші та їх еквіваленти	1165		
Витрати майбутніх періодів	1170		
Інші оборотні активи	1190		
Усього за розділом II	**1195**		
III. Необоротні активи, утримувані для продажу, та групи вибуття	**1200**		
Баланс	**1300**		

Пасив	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	2	3	4
I. Власний капітал			
Зареєстрований (пайовий) капітал	1400		
Капітал у дооцінках	1405		
Додатковий капітал	1410		
Резервний капітал	1415		
Нерозподілений прибуток (непокритий збиток)	1420		
Неоплачений капітал	1425	( )	( )
Вилучений капітал	1430	( )	( )
Усього за розділом I	**1495**		
II. Довгострокові зобов'язання і забезпечення			
Відстрочені податкові зобов'язання	1500		
Довгострокові кредити банків	1510		
Інші довгострокові зобов'язання	1515		

1	2	3	4
Довгострокові забезпечення	1520		
Цільове фінансування	1525		
Усього за розділом II	**1595**		
III. Поточні зобов'язання і забезпечення			
Короткострокові кредити банків	1600		
Поточна кредиторська заборгованість за:			
довгостроковими зобов'язаннями	1610		
товари, роботи, послуги	1615		
розрахунками з бюджетом	1620		
у тому числі з податку на прибуток	1621		
розрахунками зі страхування	1625		
розрахунками з оплати праці	1630		
Поточні забезпечення	1660		
Доходи майбутніх періодів	1665		
Інші поточні зобов'язання	1690		
Усього за розділом III	**1695**		
IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття	**1700**		
Баланс	**1900**		

Керівник

Головний бухгалтер

Звіт про фінансові результати

	КОДИ
Дата (рік, місяць, число)	01
за ЄДРПОУ	

Підприємство _____
(найменування)

Звіт про фінансові результати (Звіт про сукупний дохід)
за _____ 20__ р.

Форма № 2 | Код за ДКУД | 1801003

І. Фінансові результати

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000		
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	( )	( )
Валовий:			
прибуток	2090		
збиток	2095	( )	( )
Інші операційні доходи	2120		
Адміністративні витрати	2130	( )	( )
Витрати на збут	2150	( )	( )
Інші операційні витрати	2180	( )	( )
Фінансовий результат від операційної діяльності:			
прибуток	2190		
збиток	2195	( )	( )
Дохід від участі в капіталі	2200		
Інші фінансові доходи	2220		
Інші доходи	2240		
Фінансові витрати	2250	( )	( )
Втрати від участі в капіталі	2255	( )	( )
Інші витрати	2270	( )	( )
Фінансовий результат до оподаткування:			
прибуток	2290		

1	2	3	4
збиток	2295	( )	( )
Витрати (дохід) з податку на прибуток	2300		
Прибуток (збиток) від припиненої діяльності після оподаткування	2305		
Чистий фінансовий результат:			
прибуток	2350		
збиток	2355	( )	( )

II. Сукупний дохід

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Дооцінка (уцінка) необоротних активів	2400		
Дооцінка (уцінка) фінансових інструментів	2405		
Накопичені курсові різниці	2410		
Частка іншого сукупного доходу асоційованих та спільних підприємств	2415		
Інший сукупний дохід	2445		
Інший сукупний дохід до оподаткування	**2450**		
Податок на прибуток, пов'язаний з іншим сукупним доходом	2455		
Інший сукупний дохід після оподаткування	**2460**		
Сукупний дохід (сума рядків 2350, 2355 та 2460)	**2465**		

III. Елементи операційних витрат

Назва статті	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Матеріальні затрати	2500		
Витрати на оплату праці	2505		
Відрахування на соціальні заходи	2510		
Амортизація	2515		
Інші операційні витрати	2520		
Разом	**2550**		

IV. Розрахунок показників прибутковості акцій

Назва статті	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Середньорічна кількість простих акцій	2600		
Скоригована середньорічна кількість простих акцій	2605		
Чистий прибуток (збиток) на одну просту акцію	2610		
Скоригований чистий прибуток (збиток) на одну просту акцію	2615		
Дивіденди на одну просту акцію	2650		

Керівник

Головний бухгалтер

Звіт про рух грошових коштів

	КОДИ
Дата (рік, місяць, число)	
Підприємство _____	
(найменування) за ЄДРПОУ	

Форма № 3 Код за ДКУД 1801004

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
I. Рух коштів у результаті операційної діяльності			
Надходження від:			
Реалізації продукції (товарів, робіт, послуг)	3000		
Повернення податків і зборів	3005		
у тому числі податку на додану вартість	3006		
Цільового фінансування	3010		
Інші надходження	3095		
Витрачання на оплату: Товарів (робіт, послуг)	3100	( )	( )
Праці	3105	( )	( )
Відрахувань на соціальні заходи	3110	( )	( )
Зобов'язань з податків і зборів	3115	( )	( )
Інші витрачання	3190	( )	( )
Чистий рух коштів від операційної діяльності	**3195**		
II. Рух коштів у результаті інвестиційної діяльності			
Надходження від реалізації:			
фінансових інвестицій	3200		
необоротних активів	3205		
Надходження від отриманих: відсотків	3215		

1	2	3	4
дивідендів	3220		
Надходження від деривативів	3225		
Інші надходження	3250		
Витрачання на придбання: фінансових інвестицій	3255	( )	( )
необоротних активів	3260	( )	( )
Виплати за деривативами	3270	( )	( )
Інші платежі	3290	( )	( )
Чистий рух коштів від інвестиційної діяльності	**3295**		
III. Рух коштів у результаті фінансової діяльності			
Надходження від:			
Власного капіталу	3300		
Отримання позик	3305		
Інші надходження	3340		
Витрачання на: Викуп власних акцій	3345	( )	( )
Погашення позик	3350		
Сплату дивідендів	3355	( )	( )
Інші платежі	3390	( )	( )
Чистий рух коштів від фінансової діяльності	**3395**		
Чистий рух грошових коштів за звітний період	**3400**		
Залишок коштів на початок року	3405		
Вплив зміни валютних курсів на залишок коштів	3410		
Залишок коштів на кінець року	3415		

Звіт про власний капітал (форма 4)

Стаття	Код рядка	Зареєстрований (пайовий) капітал	Капітал у дооцінках	Додатковий капітал	Резервний капітал	Нерозподілений прибуток (непокритий збиток)
1	2	3	4	5	6	7
Залишок на початок року	**4000**					
Коригування: Зміна облікової політики	4005					
Виправлення помилок	4010					
Інші зміни	4090					
Скоригований залишок на початок року	**4095**					
Чистий прибуток (збиток) за звітний період	**4100**					
Інший сукупний дохід за звітний період	**4110**					
Розподіл прибутку:	4200					
Виплати власникам (дивіденди)						
Спрямування прибутку до зареєстрованого капіталу	4205					
Відрахування до резервного капіталу	4210					
Внески учасників: Внески до капіталу	4240					
Погашення заборгованості з капіталу	4245					
Вилучення капіталу: Викуп акцій (часток)	4260					

1	2	3	4	5	6	7
Перепродаж викуплених акцій (часток)	4265					
Анулювання викуплених акцій (часток)	4270					
Вилучення частки в капіталі	4275					
Інші зміни в капіталі	4290					
Разом змін у капіталі	**4295**					
Залишок	**4300**					

Керівник

Головний бухгалтер

Баланс банківської установи

У млн грн	Прим.	31 грудня 2025	31 грудня 2026 (як перераховано)
АКТИВИ			
Грошові кошти та їх еквіваленти			
Кредити та аванси банкам			
Кредити та аванси клієнтам			
Інвестиційні цінні папери в т.ч.:			
– за справедливою вартістю через прибуток чи збиток			
– за справедливою вартістю через інший сукупний дохід			
– за амортизованою собівартістю			
Поточні податкові активи			
Інвестиційна нерухомість			
Основні засоби			
Нематеріальні активи за винятком гудвілу			
Відстрочені податкові активи			
Інвестиції в дочірні підприємства, спільні підприємства та асоційовані підприємства			
Інші фінансові активи			
Інші нефінансові активи			
Непоточні активи або групи вибуття, класифіковані як утримувані для продажу або як утримувані для виплати власникам			
Загальна сума активів			
ЗОБОВ'ЯЗАННЯ			
Кошти клієнтів			
Інші залучені кошти			
Поточні податкові зобов'язання			
Інші фінансові зобов'язання			
Забезпечення у т.ч.:			
– резерви за кредитними зобов'язаннями та контрактами фінансової гарантії			
– інше забезпечення			
Інші нефінансові зобов'язання			
Загальна сума зобов'язань			

ВЛАСНИЙ КАПІТАЛ			
Статутний капітал			
Емісійний дохід			
Інші резерви			
Результат від операцій з акціонером			
Резервні та інші фонди банку			
Накопичений дефіцит			
Загальна сума власного капіталу			
Загальна сума власного капіталу та зобов'язань			

Балансовий (розрахунок по балансу) –
загальний коефіцієнт ризику банкрутства (Altman Z-score):

$$Z = 1.2 \times A + 1.4 \times B + 3.3 \times C + 0.6 \times D + 1.0 \times E,$$

де:

$$X_1 = \frac{\text{Оборотні активи – Поточні зобов'язання}}{\text{Валюта балансу}}$$

$$X_2 = \frac{\text{Нерозподілений прибуток}}{\text{Валюта балансу}}$$

$$X_3 = \frac{EBIT}{\text{Валюта балансу}}$$

$$X_4 = \frac{\text{Власний капітал}}{\text{Зобов'язання}}$$

$$X_5 = \frac{\text{Виручка}}{\text{Валюта балансу}}$$

– Якщо Z < 1,8 – високий ризик банкрутства.

Модель Альтмана (Z-score) для банків (адаптований варіант)

$$Z = 6{,}56\, X_1 + 3{,}26\, X_2 + 6{,}72 X_3 + 1{,}05\, X_4,$$

де:

$$X_1 = \frac{\text{Власний капітал}}{\text{Активи}}$$

$$X_2 = \frac{\text{Нерозподілений прибуток}}{\text{Активи}}$$

$$X_3 = \frac{EBIT}{\text{Активи}}$$

$$X_4 = \frac{\text{Власний капітал}}{\text{Зобов'язання}}$$

– Якщо Z < 1,2 – висока ймовірність банкрутства банку.

Додаток Д

Основні порогові орієнтири для NPL/NPE у різних країнах

Регіон / країна	Типовий поріг «критичного рівня» NPL	Фактичний рівень / ситуація	Джерело / коментар
ЄС / ЕВА	≈ 5 % брутто-кредитів як орієнтир для банків з «високим рівнем NPL»	У IV кварталі 2024 року середній рівень NPL у значущих банках склав **2,28 %**	ECB/SSM статистика
Україна	–	У грудні 2024 року показник NPL в Україні – **30,3 %** портфеля кредитів	CEIC, дані НБУ
Єврозона / загально-європейський контекст	–	Середній NPL у ЄС в 2017 році – **3,7 %**	Дані за минулі роки
Україна (2025)	–	У другому кварталі 2025 року частка NPL знизилась до **27 %**	Публікації НБУ / преса

Додаток Е

Класифікація грошового потоку підприємства

Ознака класифікації	Склад класифікації
1. За розмірами обслуговування господарської діяльності (процесу)	– грошовий потік підприємства (загального структурного елементу); – грошовий потік за окремими структурними підрозділами підприємства).
2. За фінансовою звітністю (господарською діяльністю) підприємства	– грошовий потік від операційної діяльності; – грошовий потік від фінансової діяльності; – грошовий потік від інвестиційної діяльності.
3. За цілеспрямованістю руху грошових потоків підприємства	– позитивний грошовий потік, який визначає сукупність усіх доходів підприємства; – негативний грошовий потік, який включає всі сукупні витрати підприємства.
4. За стратегічним методом обчислення грошового потоку	– валовий грошовий потік; – чистий грошовий потік.
5. За рівнем достатності на підприємстві	– надлишковий грошовий потік – надходження коштів перевищують видатки; – дефіцитний грошовий потік – видатки перевищують надходження грошових коштів.
6. За методом оцінки у часі	– теперішній грошовий потік (поточний); – майбутній грошовий потік (очікуваний).
7. За процесом формування грошових потоків на підприємстві (регулярністю)	– регулярний грошовий потік – постійний незалежно від обсягів реалізованої продукції та здійснених витрат; – дискретний грошовий потік – відбувається декілька раз за звітниій період (нерегулярний).
8. За періодичністю та інтервальністю формування на підприємстві	– регулярний грошовий потік; – нерегулярний грошовий потік.
9. За валютним розподілом надходження та видатків	– грошовий потік у національній валюті; – грошовий потік у іноземній валюті (групування за видами валют).
10. За значимістю у фінансовій діяльності підприємства	– пріоритетні грошові потоки; – другорядні грошові потоки; – обслуговуючі (періодичні) грошові потоки.

Додаток Ж

Класифікація цінних паперів та їх характеристика

Вид цінного папера	Характеристика
Акції	Дає право власності на частку в статутному капіталі підприємства; власник отримує дивіденди та право голосу на загальних зборах акціонерів. Можуть бути іменними або на пред'явника, простими або привілейованими.
Облігації	Борговий цінний папір, що підтверджує зобов'язання емітента повернути інвестору номінальну вартість у визначений строк та виплачувати відсотки (купон). Використовується для залучення довгострокового фінансування.
Вексель	Письмове боргове зобов'язання встановленої форми, яке передбачає безумовну сплату визначеної суми у зазначений строк. Використовується у розрахунках між підприємствами.
Депозитні сертифікати	Папери, які банки видають вкладникам на підтвердження внесених коштів; передбачають повернення вкладу та відсотків у визначений строк.
Інвестиційні сертифікати	Цінні папери, що випускаються інвестиційними фондами або компаніями, підтверджують право власності інвестора на частку у фонді та отримання доходів від інвестиційної діяльності.
Державні цінні папери (ОВДП, казначейські зобов'язання)	Гарантовані державою папери, що засвідчують залучення коштів до бюджету. Вважаються надійними інструментами з низьким ризиком.
Опціони та ф'ючерси	Похідні цінні папери (деривативи), які дають право (але не зобов'язання) купити чи продати актив у майбутньому за зафіксованою ціною. Використовуються для хеджування ризиків або спекулятивних операцій.
Заставні	Папери, що підтверджують право власника на отримання боргу, забезпеченого іпотекою на нерухоме майно.
Приватизаційні папери (історично в Україні)	Використовувалися для передачі державного майна у власність громадян у процесі приватизації.

Додаток 3

Виробництво: погіршення результатів та очікувань

Результати (вересень до серпня)

- % підприємств, які **нарощували обсяги виробництва зменшився** (із 28,5% у серпні до 24,4% у вересні)
- % підприємств, що **скоротили обсяги виробництва без істотних змін** (17% у серпні vs 18,8% у вересні)

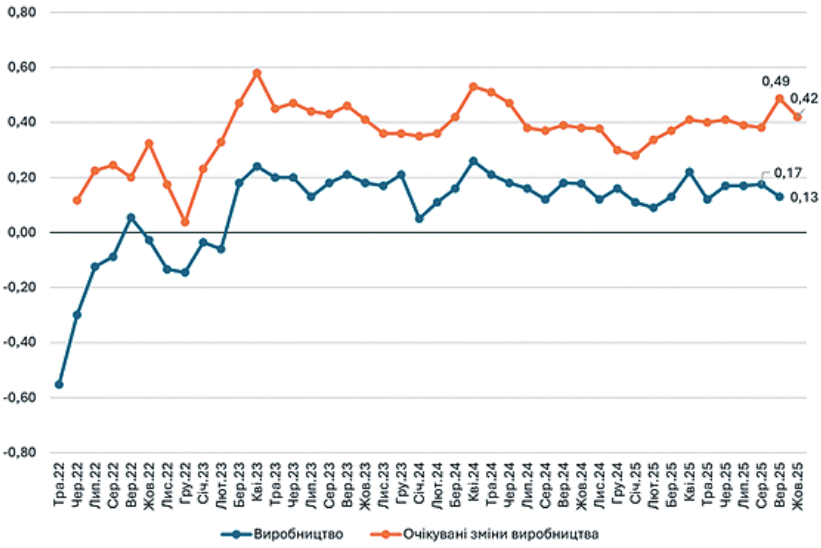
Індекс змін зменшився та становить 0,13 (було 0,17 три місяці поспіль)

Очікування на 3 місяці

- % підприємств, які **планують збільшувати обсяги виробництва** в найближчі 3-4 місяці, **зменшився** (із 46,8% у серпні до 42,2% у вересні)
- % підприємств, які **очікують скорочення обсягів виробництва не змінився** (4,2% як і у серпні)

Індекс очікуваних змін виробництва суттєво зменшився, із 0,49 до 0,42

Виробництво, балансові показники



Експорт: погіршення результатів та очікувань

Результати (вересень до серпня)

- % підприємств, що **повідомляють про зростання експорту, зменшився** (із 30,2% у серпні до 28,3% у вересні)
- % підприємств, що **повідомляють про скорочення експорту, без суттєвих змін** (14,3% у серпні vs 15% у вересні)

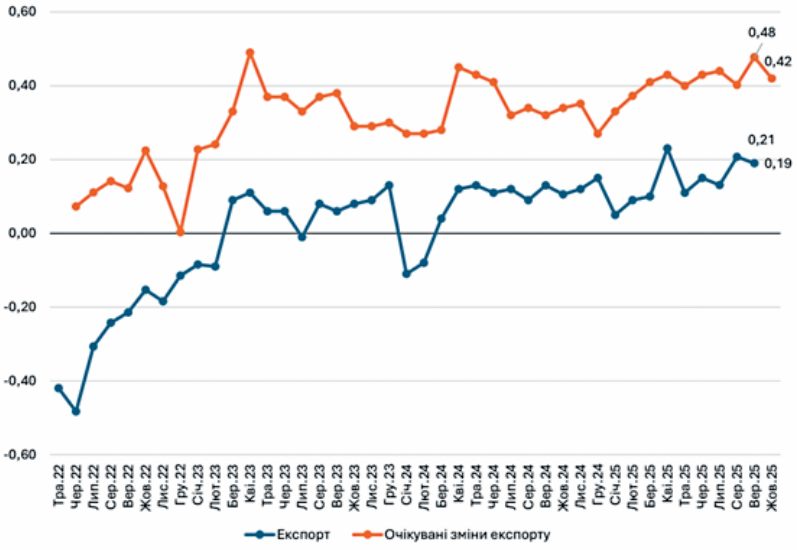
Індекс змін незначним чином зменшився (із 0,21 до 0,19)

Очікування на 3 місяці

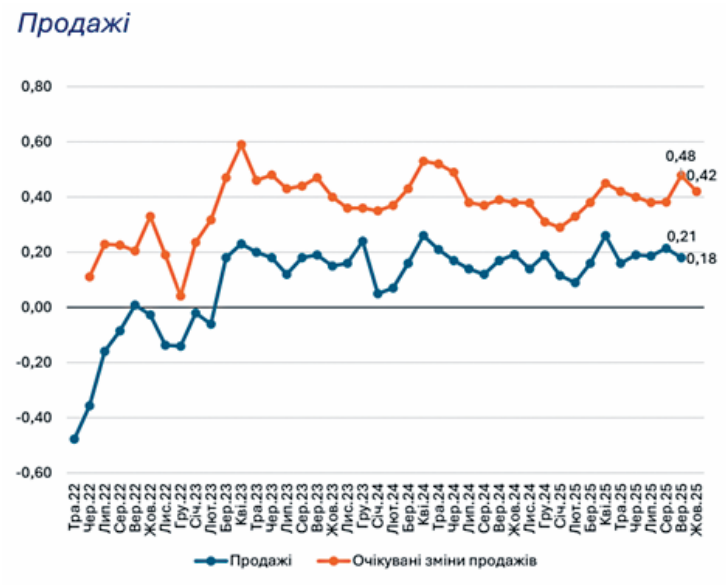
- % підприємств, які **очікують зростання експорту зменшився** (із 48,8% у серпні до 44,8% у вересні)
- % підприємств, які **планують скоротити експорт без суттєвих змін** (4,4% у серпні vs 5% у вересні)

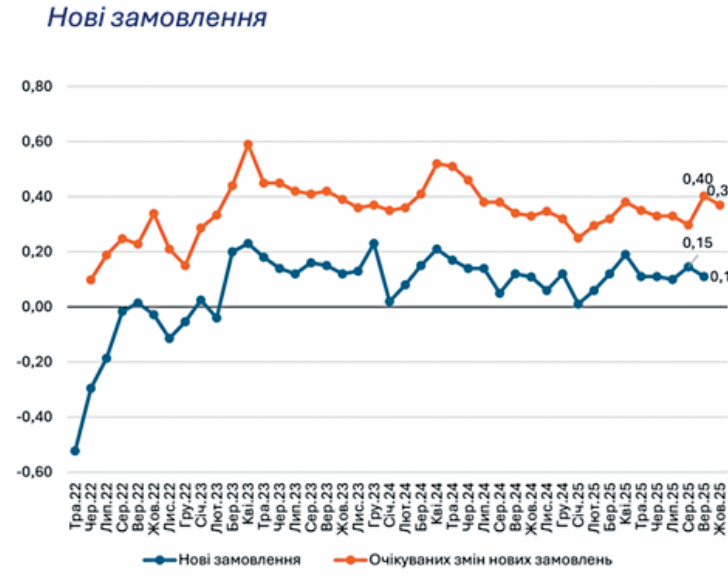
Індекс очікуваних змін експорту зменшився, із 0,48 до 0,42

Експорт, балансові показники



Продажі та нові замовлення:
погіршення результатів та очікувань





Ціни на готову продукцію: результати без змін, очікування зросли

Результати (вересень до серпня)

- % підприємств, що **повідомляють про зростання цін на готову продукцію дещо збільшився** (із 36,7% до 38,5%)
- % підприємств, які вважають, що **ціни на готову продукцію знизились, без істотних змін** (1,3% у серпні та липні vs 1,7% у вересні)

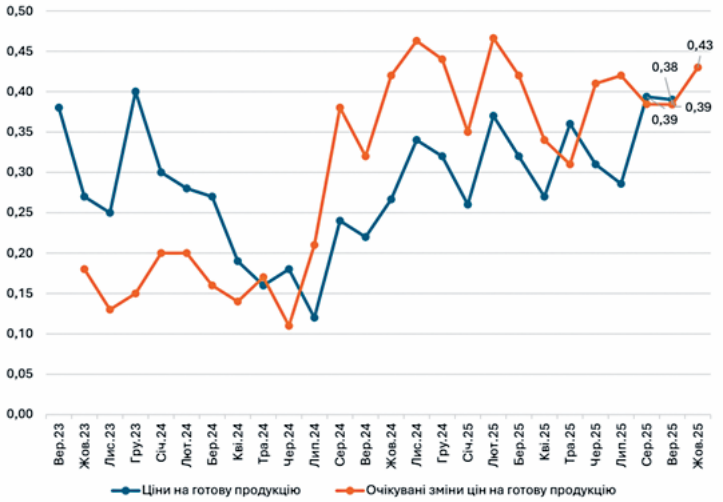
Індекс змін цін на готову продукцію не змінився 0,39, як і у серпні

Очікування на 3 місяці

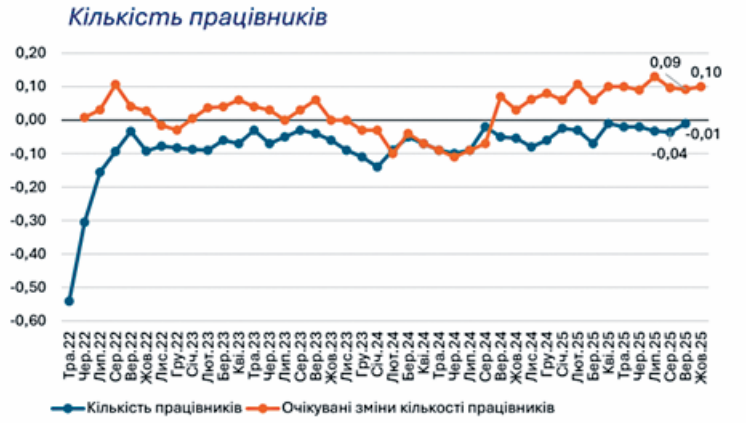
- % підприємств, які **очікують зростання цін збільшився** (із 40% у серпні до 45,6% у вересні)
- % підприємств, які **очікують на зниження цін суттєво не змінився** (1,1% у вересні та 0,07 у серпні та липні)

Індекс очікуваних змін цін на готову продукцію збільшився із 0,38 до 0,43

Ціни на готову продукцію, балансові показники



Зайнятість:
кількість працівників незначним чином збільшилась, очікування без істотних змін



Очікування на 3 місяці

- % підприємств, що **планують зростання зайнятості в найближчі 3-4 місяці, істотно не змінився** (16,4% у серпні vs 15,5% у вересні)
- % підприємств, які **мають намір скоротити чисельність працівників також без істотних змін** (7,4% у серпні vs 6,6% у вересні)

Індекс очікуваних змін суттєво не змінився та становить 0,10, (було 0,09)

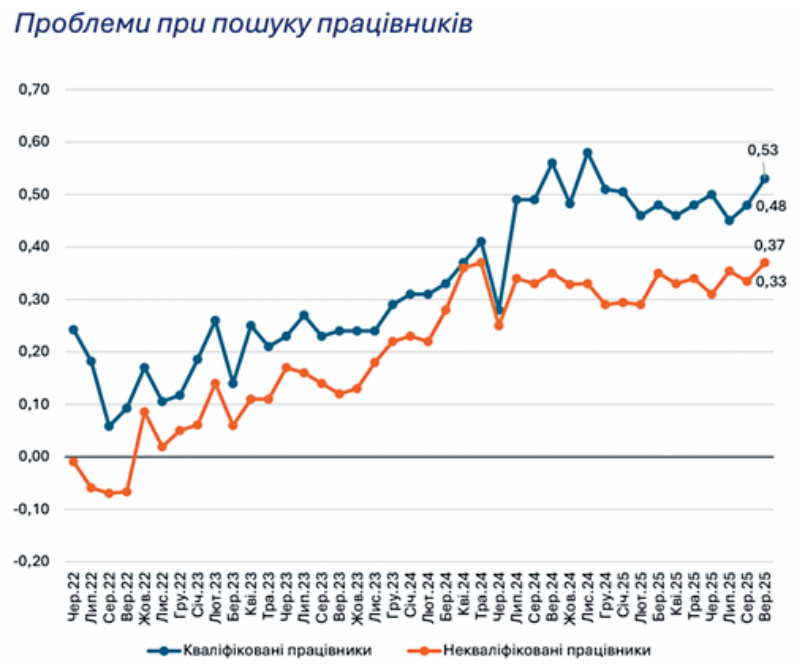
Кількість працівників у вимушених відпустках

Очікування на 3 місяці

- % підприємств, які **планують збільшити кількість працівників у вимушених відпустках дещо зріс** (із 10,1% до 12,7%)
- % підприємств, які **планують скоротити працівників у вимушених відпустках, без істотних змін** (0,3% у серпні vs 1,7% у вересні)

Індекс очікуваних змін без істотних змін та становить 0,10 (було 0,09)

Проблеми з пошуком працівників збільшились



У вересні 2025 року спостерігається посилення проблем при пошуку і для кваліфікованих, і для некваліфікованих працівників

Кваліфіковані працівники:

- % тих, хто повідомив, що **таких працівників знайти складніше, збільшився** (із 50,1% у серпні до 52,8% у вересні)
- % тих, хто вважає що **кваліфікованих працівників стало легше знайти відсутній** (було 1,6% у серпні)

Індекс труднощів зростає другий місяць поспіль, та у вересні **збільшився** із 0,48 до 0,53

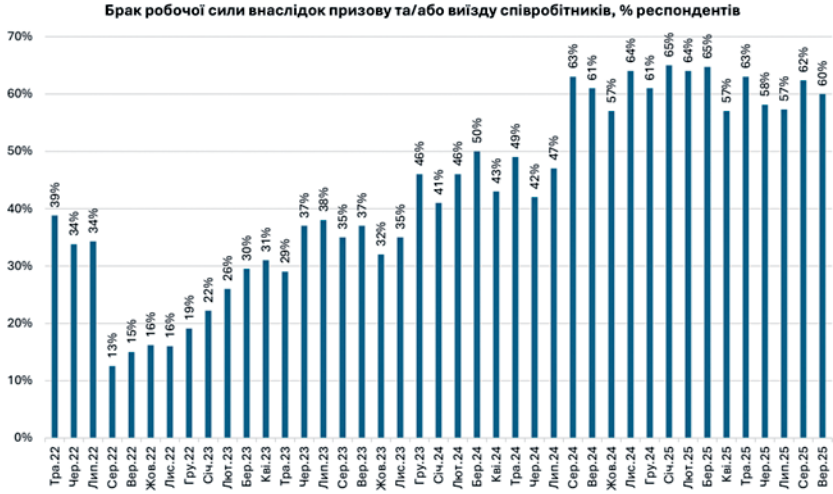
Некваліфіковані працівники:

- % тих, кому їх **важче шукати збільшився** (із 36,3% до 39,6%)
- % тих, хто повідомив, що їх **легко знайти, істотно не змінився** (4,1% у серпні vs 3% у вересні)

Індекс труднощів збільшився, із 0,33 до 0,37

«Брак робочої сили» зберігає лідерство у переліку перешкод із незначним зменшенням у значенні

- Частка підприємств, які вказали на **«брак робочої сили» як на перешкоду,** незначним чином зменшився (із 62% у серпні до 60% у вересні)
- **У переліку перешкод «брак робочої сили» залишається на першій позиції**



Основні перешкоди для ведення бізнесу у воєнний час, % респондентів

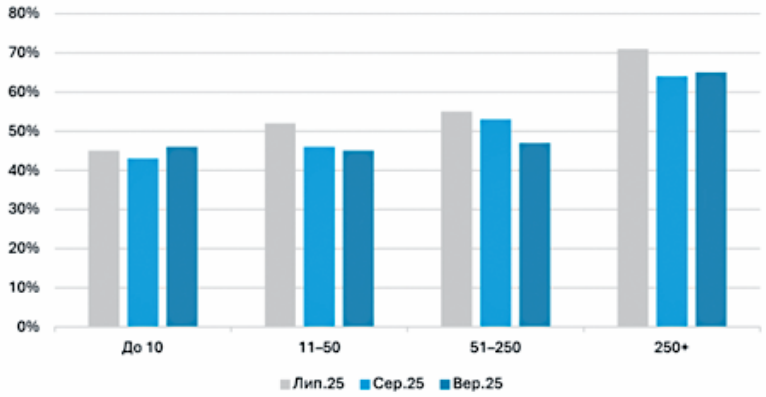
У вересні 2025 року перелік у трійці лідерів перешкод розвитку бізнесу залишається незмінним, водночас відбуваються зміни у відсотковому розподілі

- **«Брак робочої сили»** із незначним зменшенням значення (із 62% у серпні до 60% у вересні) **зберігає лідируючу позицію**
- **Перешкода «зростання цін на сировину та товари» збільшенням значення** (із 52% до 55%) **залишається на 2-гу сходинці** (у серпні перешкода розділяла її із «небезпечно працювати»)
- **«Небезпечно працювати» із майже незмінним значенням** (52% у серпні vs 51% у вересні) **опускається із 2-ої на 3-тю сходинку**
- **«Зменшення попиту»** не дивлячись на незначне зменшення значення (із 28% у серпні до 25% у вересні) **залишається на 4-му місці**
- **«Перебої з електроенергією»** із незначним зменшенням значення (із 6% до 4%) **опускається з 9-го на 11-те місце, розділяючи сходинку із «пошкодженням майна»**
- **Корупція та тиск з боку правоохоронних органів не є суттєвими проблемами**


Сер.25
Вер.25
Брак робочої сили внаслідок призову та/або виїзду співробітників
62
60
Зростання цін на сировину/матеріали/товари
52
55
Небезпечно працювати
52
51
Зменшення попиту на продукцію/послуги
28
25
Складнощі з перевезенням сировини чи готових товарів територією України
23
18
Розрив ланцюжків постачання
15
17
Брак обігових коштів
12
14
Блокування податкових накладних
6
8
Корупція
7
6
Державне регулювання курсу валют
5
5
Перебої з електро-, водо- або тепло-постачанням
6
4
Пошкодження майна або товару внаслідок бойових дій
3
4
Неправомірні вимоги або тиск з боку контролюючих чи правоохоронних органів
2
3
Не було проблем
3
3
Брак палива
1
0
Created with Datawrapper

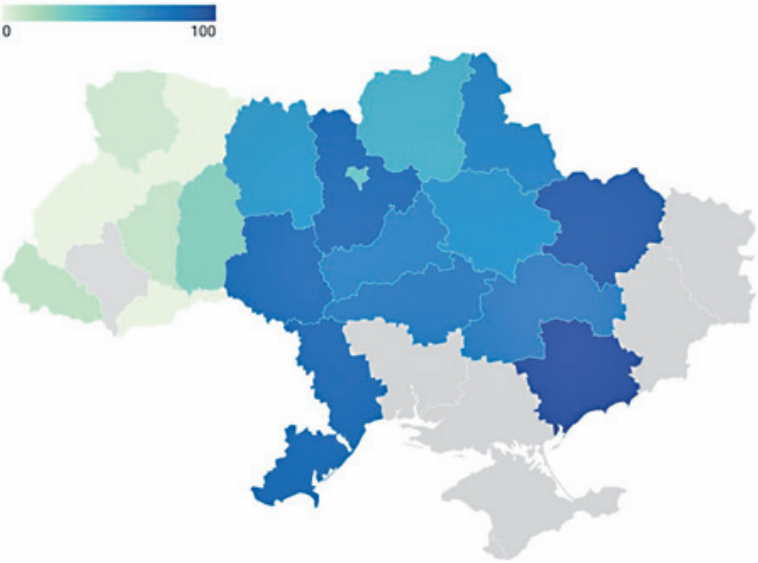
«Небезпечно працювати» у різних вимірах

«Небезпечно працювати» за розміром підприємств, % респондентів



- % підприємств, які обрали «небезпечно працювати» як перешкоду, є найвищим для великих підприємств (із майже незмінним значенням) та приблизно однаковим для мікро-, малих та середніх підприємств
- 80+% опитаних у Вінницькій, Київський, Одеській, Харківській та Запорізькій областях вважають небезпечні умови перешкодою для ведення бізнесу

«Небезпечно працювати» за регіоном, % респондентів

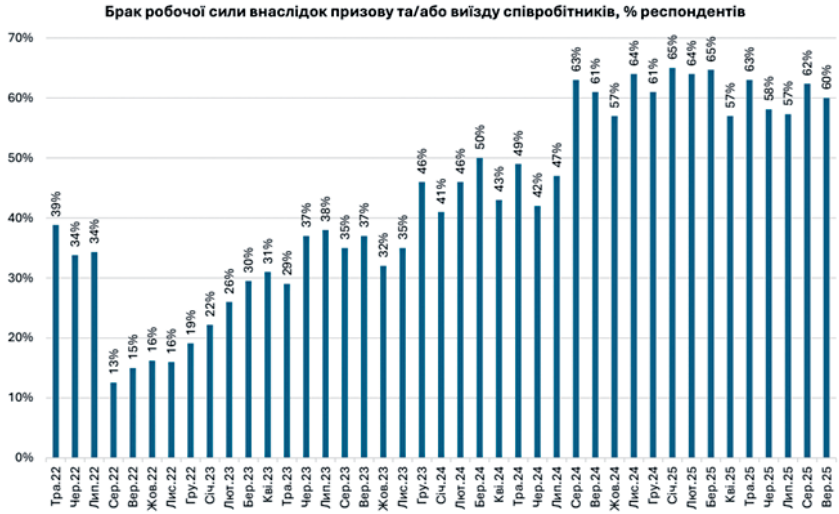


Created with Datawrapper

Примітка. Кількість респондентів в Івано-Франківській області була недостатньою для аналізу цього питання

«Зростання цін» зберігає другу позицію у рейтингу перешкод

- Частка підприємств, для яких **«зростання цін на сировину та матеріали»** є перешкодою **несуттєво зменшилась** із 62% до 60%
- У переліку перешкод «зростання цін» **зберігає за собою 2-гу сходинку**



Додаток К

Роль суб'єктів у забезпеченні інформаційної безпеки

Суб'єкти інформаційної безпеки	Їхня роль у забезпеченні інформаційної безпеки
Керівництво організації	Формує політику інформаційної безпеки, визначає стратегію захисту даних, забезпечує ресурси та контроль за її реалізацією.
IT-відділ (системні адміністратори, технічні спеціалісти)	Відповідає за технічний захист інформації: налаштування систем контролю доступу, шифрування, моніторинг та ліквідацію кіберзагроз.
Служба безпеки підприємства	Проводить аналіз ризиків, здійснює моніторинг інцидентів, організовує розслідування випадків порушень інформаційної безпеки.
Юридичний відділ	Забезпечує відповідність дій організації вимогам законодавства, розробляє внутрішні нормативні документи та договори про нерозголошення.
Працівники організації	Виконують правила та інструкції щодо захисту інформації, дотримуються політики конфіденційності, повідомляють про підозрілі випадки.
Відділ кадрів (HR)	Проводить перевірку кандидатів, інструктажі та навчання персоналу, формує культуру безпеки в колективі.
Зовнішні партнери та підрядники	Зобов'язані дотримуватися умов контрактів і правил безпечного обміну інформацією при взаємодії з організацією.
Державні органи (Кіберполіція, СБУ, НКЦК)	Здійснюють контроль, нагляд, розробляють стандарти та нормативи, а також надають допомогу в разі серйозних інцидентів.
Клієнти та користувачі послуг	Дотримуються правил користування сервісами, захищають свої облікові записи, взаємодіють з організацією у межах інформаційної безпеки.

Додаток Л

Українські компанії в системі «зелені ініціативи»

Компанія	Галузь	Ключові «зелені» ініціативи 2023–2025	Останнє публічне підтвердження
DTEK (ДТЕК)	Енергетика	Розвиток ВДЕ, зокрема вітрової генерації; інвестиції в «зелену» відбудову енергосистеми	Інтерв'ю CEO про розширення вітрових проєктів (2025), корпоративні матеріали зі сталого розвитку.
Metinvest	Металургія	Зниження викидів, екопроєкти в ланцюгу створення вартості, ESG-цілі	Консолідований звіт зі сталого розвитку 2023.
Nova (Nova Poshta)	Логістика / пошта	«Зелена» логістика, енергоефективність відділень, прозора нефінзвітність (GRI)	Огляд сталого розвитку групи Nova/GRI-підхід (2025).
Kyivstar (VEON)	Телеком	Інвестиції в енергостійкість мережі, «озеленення» інфраструктури, розвиток ESG	Звітність VEON 2024 та інтерв'ю про інвестпрограму в Україні до 2027 р.
MHP (МХП)	Агро/харчова	Політика «нульової вирубки», управління викидами (Scope 1–2), кліматичні ризики	Річний звіт 2024 з екополітикою і показниками викидів.
Ukrzaliznytsia	Транспорт	Екологічна політика до 2030 р., оновлення рухомого складу, партнерські «зелені» проєкти	Сторінка для інвесторів із політикою довкілля; проєкти EBRD.
Fozzy Group / Silpo	Ритейл	Програми підтримки локальних виробників, відповідальне споживання, екоініціативи мережі	Звіт сталого розвитку Silpo; публікації про сталий ритейл.
Vodafone Ukraine	Телеком	Системна нефінзвітність, підходи до мінімізації впливу на довкілля	Звіт зі сталого розвитку (англ.), політика екологічної безпеки.
Astarta-Kyiv	Агро	Перехід на звітність за ESRS, екопрактики у виробництві	Аналітика про впровадження ESRS в Україні (2025) з прикладами компаній.
Kernel (приклад ESG-кейсу)	Агро	Інтеграція ESG-рішень у практичний менеджмент та «зелену» трансформацію	Академічна публікація з кейсом Kernel в контексті воєнного часу.

Додаток М

Технології в системі покращення оцінки менеджменту безпеки організації

Технологія	Завдання	Результат
BI-системи (Business Intelligence)	Інтеграція даних з різних джерел, побудова звітів та дашбордів	Візуалізація ключових показників безпеки у зручному форматі, швидкий доступ до аналітики
Big Data	Обробка великих обсягів різнорідної інформації (фінансові операції, логи, комунікації)	Виявлення прихованих закономірностей, тенденцій і ризиків, які неможливо визначити вручну
SIEM-системи (Security Information and Event Management)	Моніторинг подій інформаційної безпеки, збір логів у режимі реального часу	Своєчасне виявлення інцидентів та швидке реагування на загрози
AI та ML (штучний інтелект і машинне навчання)	Автоматичний аналіз ризиків, прогнозування сценаріїв, виявлення аномалій	Підвищення точності прогнозів, зменшення людських помилок, проактивне управління безпекою
Хмарні технології	Забезпечення доступу до систем оцінки та аналітики з будь-якої точки	Гнучкість у використанні, зменшення витрат на IT-інфраструктуру
IoT-рішення (Internet of Things)	Збір даних із сенсорів та пристроїв безпеки	Постійний моніторинг фізичної безпеки та стану інфраструктури

НАВЧАЛЬНЕ ВИДАННЯ

Шевченко Наталія Володимирівна,
кандидат економічних наук, доцент
Копитко Марта Іванівна,
доктор економічних наук, професор

Менеджмент безпеки організації

Навчальний посібник

Редагування *Оксана Шмиговська*
Макетування *Галина Шушняк*
Друк *Назарій Ганущак*

Підписано до друку 30.12.2025.
Формат 60×84/16. Папір офсетний. Умовн. друк. арк. 18,83.
Тираж 45 прим. Зам № 98-25.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.