Міністерство освіти і науки України
Національний університет «Запорізька політехніка»
Кафедра Бізнесу та управління

Пожуєва Т.О.

Економічна безпека

Навчальний посібник

м. Запоріжжя, 2025

УДК 658:005.922.1
П46

Рекомендовано до друку вченою радою
Національного університету «Запорізька політехніка»
(протокол №1 від 28.08.2025)

Рецензенти:

Філюк Ганна Михайлівна, завідувач кафедри економіки підприємства Київського національного університету імені Тараса Шевченка, заслужений економіст України, доктор економічних наук, професор

Андрющенко Катерина Анатоліївна, професор кафедри бізнес-економіки та підприємництва Київського національного економічного університету імені Вадима Гетьмана, доктор економічних наук, професор

Іванова Марина Іллівна, професор кафедри менеджменту НТУ «Дніпровська політехніка», доктор економічних наук, професор

Автор: Т.О. Пожуєва, д.е.н, проф. каф. бізнесу та управління

П46 Економічна безпека. Навчальний посібник для здобувачів вищої освіти спеціальності 073 «Менеджмент» та 076 «Підприємництво та торгівля» усіх форм навчання / Автор Т.О. Пожуєва – Запоріжжя: НУ «Запорізька політехніка», 2025 – 304 с.

ISBN 978-617-529-530-4

Навчальний посібник «Економічна безпека» є комплексним дослідженням теоретичних засад, сучасних викликів та практичних підходів до забезпечення економічної безпеки підприємств. Особлива увага приділяється ключовим аспектам, таким як фінансова, інформаційна, кадрова, екологічна безпека та стратегічне управління ризиками.

Рекомендовано для використання у навчальному процесі закладів вищої освіти, а також для самостійного опрацювання.

УДК 658:005.922.1

ISBN 978-617-529-530-4

ЗМІСТ

Розділ 2. Аналіз ризиків та захист основних активів підприємства

ВСТУП

Економічна безпека промислового підприємства – це складний і багатогранний процес, що охоплює захист підприємства від внутрішніх та зовнішніх загроз, збереження його стійкості та конкурентоспроможності в умовах нестабільного ринкового середовища. У сучасному світі, де глобалізація, технологічні зміни та економічні кризи постійно змінюють бізнес-середовище, питання економічної безпеки виходять на перший план. Здатність підприємства своєчасно реагувати на загрози та виклики, зберігати свою фінансову стабільність, захищати активи та інтелектуальну власність, забезпечує його виживання та процвітання.

Актуальність теми економічної безпеки для промислових підприємств зростає з кожним днем. У сучасних умовах бізнесу підприємства стикаються з безліччю загроз: від фінансових труднощів та нестабільних ринків до інформаційних витоків та конкурентної боротьби. Саме тому для керівників та фахівців підприємств критично важливо мати глибокі знання у сфері економічної безпеки, щоб знижувати ризики та ефективно протистояти викликам.

Ця дисципліна не лише навчить вас виявляти загрози та аналізувати їх вплив на діяльність підприємства, але й забезпечить інструменти для розробки стратегічних рішень, спрямованих на забезпечення стабільності та стійкості компанії в умовах жорсткої конкуренції. Знання, отримані під час вивчення цієї дисципліни, дадуть вам змогу ефективно планувати розвиток підприємства, уникати критичних помилок і створювати умови для його довгострокового процвітання.

Метою цього посібника є надання читачам практичних знань та навичок, необхідних для забезпечення економічної безпеки промислових підприємств. Він допоможе вам навчитися ідентифікувати та оцінювати загрози, розробляти заходи щодо їх нейтралізації, а також планувати та впроваджувати стратегії захисту підприємства. Завдяки цьому посібнику, ви зможете:

- зрозуміти основні принципи та механізми забезпечення економічної безпеки підприємства;
- освоїти методики аналізу ризиків та загроз для підприємства;
- навчитися використовувати інструменти для управління фінансовою, інформаційною та кадровою безпекою;
- розробляти стратегії для підвищення стійкості підприємства в умовах мінливого ринкового середовища.

Посібник побудований таким чином, щоб забезпечити максимально практичний підхід до вивчення теми. Кожен розділ містить теоретичні матеріали, практичні кейси та рекомендації, які допоможуть вам ефективно застосовувати отримані знання у повсякденній роботі. Ви дізнаєтесь, як створити комплексну систему безпеки, що захищатиме ваше підприємство на всіх рівнях: від фінансових операцій до захисту конфіденційної інформації та інтелектуальної власності.

Цей посібник є не лише навчальним матеріалом, а й потужним інструментом для тих, хто прагне зробити свій бізнес більш захищеним, ефективним та успішним.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

ТЕМА 1. ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

1.1 Визначення та сутність економічної безпеки.

1.2 Ключові показники економічної безпеки.

1.3 Основні аспекти забезпечення економічної безпеки на підприємстві.

1.4 Види загроз економічній безпеці.

1.1 Визначення та сутність економічної безпеки

Економічна безпека підприємства є однією з ключових складових його стабільної та успішної діяльності на ринку. В умовах сучасної економіки, що характеризується постійними змінами, конкуренцією та ризиками, важливо не лише ефективно управляти виробничими процесами, але й забезпечувати захист від потенційних загроз. Саме тому поняття "економічна безпека" виходить на передній план у стратегіях управління будь-якого промислового підприємства.

Визначення економічної безпеки

Економічна безпека промислового підприємства – це комплексна характеристика, що відображає здатність підприємства забезпечити стабільність свого функціонування, захист від внутрішніх і зовнішніх загроз, а також зберігати конкурентні переваги та фінансову стійкість в умовах ринкової нестабільності. Вона включає не лише фінансові показники, але й аспекти управління людськими ресурсами, інформаційними потоками та взаємодією з зовнішнім середовищем.

На рисунку 1.1 проілюстровано, як із підвищенням рівня економічної безпеки підприємство покращує свої конкурентні позиції та фінансові показники

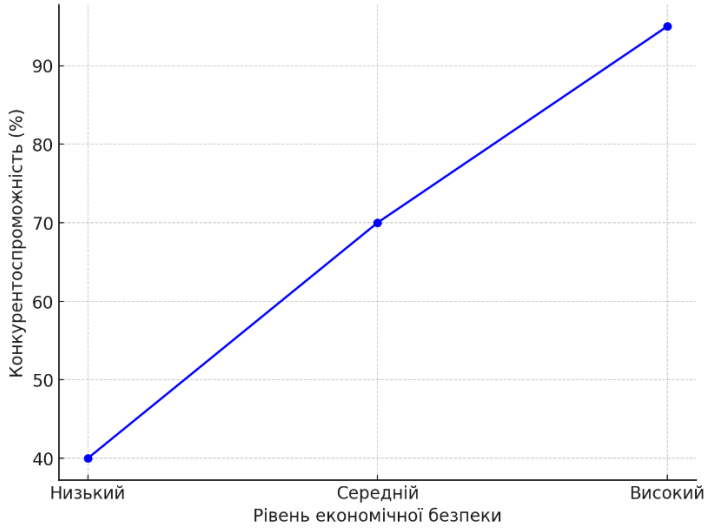

Рисунок 1.1 – Залежність конкурентоспроможності підприємства від рівня економічної безпеки

Основною метою економічної безпеки є підтримка довгострокової стійкості та конкурентоспроможності підприємства, забезпечення його розвитку навіть у несприятливих умовах. Це означає, що підприємство повинно мати здатність швидко адаптуватися до нових викликів, зберігаючи при цьому фінансову стабільність та можливість ефективного управління ресурсами.

Сутність економічної безпеки

Виходячи з ключової та функціональної мети економічної безпеки промислового підприємства, вона повинна містити, перш за все, елементи, які окреслені на рисунку 1.2

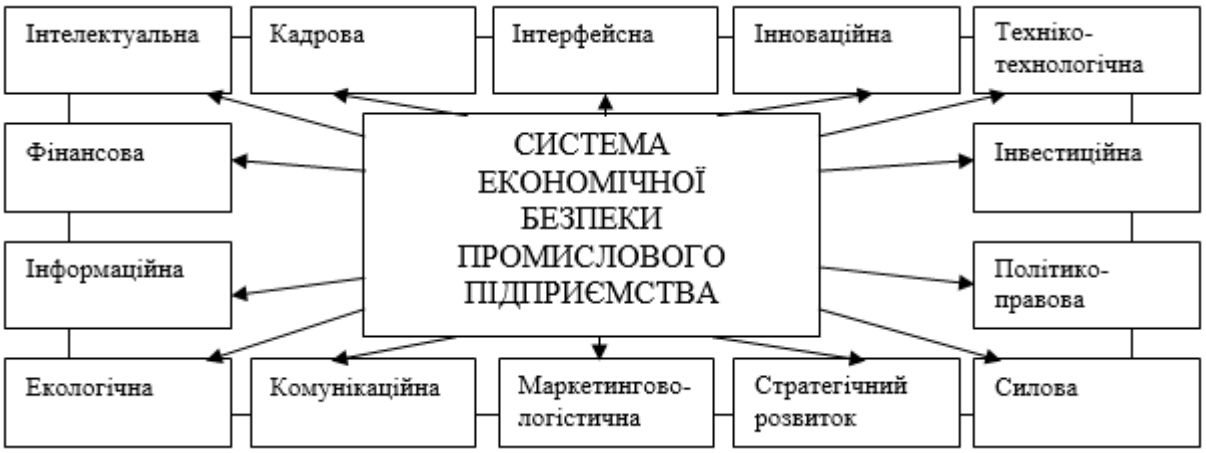

Рисунок 1.2 – Основні складові економічної безпеки суб'єкта господарювання

Основні компоненти комплексного забезпечення економічної безпеки:

1. **фінансова безпека:**
   - управління фінансовими потоками, забезпечення стабільної платоспроможності та фінансової стійкості підприємства;
   - мінімізація фінансових ризиків, пов'язаних із банкрутством, заборгованістю, шахрайськими діями чи неефективним використанням ресурсів.
2. **інтелектуальна безпека:**
   - охорона об'єктів інтелектуальної власності: патентів, авторських прав, ноу-хау;
   - формування системи захисту інноваційних розробок та унікальних знань підприємства.
3. **кадрова безпека:**
   - ефективне управління персоналом, підвищення мотивації, лояльності та кваліфікації працівників;
   - запобігання загрозам з боку персоналу, таким як витік інформації, недобросовісні дії чи кадрові конфлікти.
4. **інтерфейсна безпека:**
   - гармонізація взаємодії між внутрішніми підрозділами підприємства та зовнішніми структурами;
   - забезпечення узгодженості інформаційних, виробничих і управлінських процесів.
5. **інноваційна безпека:**
   - створення умов для безпечного впровадження інновацій і збереження інноваційного потенціалу;

- захист інновацій від копіювання конкурентами та підтримка їх комерційної цінності.

6. **техніко-технологічна безпека:**
   - модернізація виробничого обладнання, підтримка його технічної справності;
   - впровадження сучасних технологій для зменшення ризику аварій і збоїв у виробництві.
7. **інвестиційна безпека:**
   - захист інвестиційних ресурсів від зовнішніх і внутрішніх загроз;
   - забезпечення ефективного управління інвестиційними проектами та їх відповідності стратегічним цілям.
8. **політико-правова безпека:**
   - моніторинг і дотримання чинного законодавства, захист прав підприємства у правовому полі;
   - недопущення адміністративного тиску, юридичних конфліктів і регуляторних ризиків.
9. **силова безпека:**
   - забезпечення фізичного захисту об’єктів підприємства, охорона майна та працівників;
   - запровадження системи відеоспостереження, пропускного режиму та охоронних заходів.
10. **безпека стратегічного розвитку:**
    - розробка довгострокової стратегії підприємства з урахуванням потенційних ризиків;
    - адаптація до змін зовнішнього середовища, забезпечення конкурентоспроможності у перспективі.
11. **маркетингово-логістична безпека:**
    - контроль за ринковою ситуацією, дії конкурентів та постачальників;
    - забезпечення безперебійної логістики, захист каналів збуту та постачання.
12. **комунікаційна безпека:**
    - підтримка ефективної комунікації між працівниками, підрозділами і зовнішніми партнерами;
    - захист комунікаційних каналів від маніпуляцій, дезінформації та зовнішніх втручань.
13. **екологічна безпека:**
    - впровадження екологічно безпечних технологій і дотримання екологічних стандартів;
    - запобігання негативному впливу на довкілля та мінімізація витрат, пов’язаних із екологічними порушеннями.
14. **інформаційна безпека:**
    - захист інформаційних ресурсів підприємства від витоку, втрати або несанкціонованого доступу;
    - використання сучасних засобів кіберзахисту, формування політики конфіденційності та резервного копіювання даних.

Окреслені складові взаємопов'язані і впливають одна на одну. Недостатня увага до будь-якого з елементів економічної безпеки може призвести до фінансових втрат, зниження конкурентоспроможності або навіть повного припинення діяльності підприємства.

Основні принципи економічної безпеки

- **Прогнозування та запобігання загрозам**. Необхідно розробляти системи раннього попередження про потенційні загрози. Сучасні технології дозволяють моніторити як внутрішні процеси, так і зовнішнє середовище для своєчасного виявлення ризиків.
- **Комплексність підходу**. Безпека підприємства має забезпечуватися на всіх рівнях: від фінансового до інформаційного, з охопленням усіх ключових аспектів діяльності.
- **Адаптивність**. Ринки та умови діяльності постійно змінюються, тому важливо мати можливість гнучко реагувати на нові виклики та швидко адаптувати бізнес-процеси до змін.
- **Ефективність ресурсного забезпечення**. Раціональне використання ресурсів, у тому числі фінансових, кадрових та матеріальних, сприяє підвищенню стійкості підприємства.

Важливість економічної безпеки для розвитку підприємства

Підприємства, які приділяють належну увагу своїй економічній безпеці, здатні не лише захиститися від потенційних загроз, але й створювати конкурентні переваги. Стратегічне управління безпекою дозволяє підвищити довіру з боку інвесторів та партнерів, покращити репутацію на ринку та забезпечити довгостроковий розвиток навіть в умовах нестабільного економічного середовища.

1.2 Ключові показники економічної безпеки

Економічна безпека промислового підприємства є багатоаспектною системою, яку неможливо виміряти лише одним показником. Для оцінки її рівня використовується система ключових показників, що дозволяє комплексно проаналізувати всі аспекти функціонування підприємства. Ці показники не тільки демонструють поточний стан підприємства, але й дають змогу прогнозувати можливі ризики та планувати стратегічні заходи для їх усунення. Основні складові економічної безпеки суб'єкта господарювання були подані на рисунку 1.2. Тому надалі зосередимо увагу на п'яти ключових аспектах, яким, як правило, приділяється ключова увага при практичній побудові системи економічної безпеки підприємства.

Класифікація ключових показників

Ключові показники економічної безпеки можна поділити на декілька основних груп, що відповідають окремим аспектам діяльності підприємства:

1. **Фінансові показники**
   - **Коефіцієнт фінансової стійкості:** співвідношення власних і залучених коштів, що демонструє здатність підприємства функціонувати незалежно від зовнішніх кредиторів.
   - **Рівень ліквідності активів:** показує здатність підприємства швидко перетворювати активи на грошові кошти для виконання фінансових зобов'язань.
   - **Рентабельність виробництва:** відображає ефективність використання ресурсів підприємства.

2. **Виробничі показники**
   - **Коефіцієнт безперервності виробництва:** вимірює стабільність роботи виробничих потужностей.
   - **Якість продукції:** визначається часткою продукції, яка відповідає встановленим стандартам.
   - **Витрати на виробництво:** включають оцінку оптимальності використання матеріальних, енергетичних та інших ресурсів.
3. **Кадрові показники**
   - **Рівень лояльності персоналу:** аналізується через анкетування та оцінку стабільності кадрів.
   - **Кваліфікація працівників:** визначається за результатами професійного розвитку та підвищення кваліфікації.
   - **Текучість кадрів:** важливий індикатор стабільності команди та збереження ключових спеціалістів.
4. **Інформаційні показники**
   - **Рівень захищеності даних:** оцінюється кількість інцидентів витоку інформації або зламів систем.
   - **Використання сучасних інформаційних систем:** аналізується частка автоматизованих процесів у загальній системі управління підприємством.
5. **Ринкові показники**
   - **Частка ринку:** демонструє конкурентоспроможність підприємства в галузі.
   - **Імідж підприємства:** оцінюється за відгуками клієнтів, рейтингами та показниками репутаційного аудиту.
   - **Обсяг замовлень:** визначає рівень попиту на продукцію чи послуги підприємства.

Методи оцінки ключових показників

Для аналізу та оцінки ключових показників переважно використовуються такі методи:

1. **Фінансовий аналіз:** аналізує баланс, звіт про прибутки та збитки, а також звіт про рух грошових коштів.
2. **SWOT-аналіз:** виявляє сильні та слабкі сторони підприємства, а також можливості та загрози.
3. **Бенчмаркінг:** порівняння ключових показників з аналогічними підприємствами у галузі.
4. **Інформаційний аудит:** перевірка надійності систем захисту інформації.

Практичне застосування ключових показників

Використання системи ключових показників дозволяє підприємству:

- Вчасно ідентифікувати слабкі місця в системі економічної безпеки.
- Порівнювати свої результати з конкурентами на ринку.
- Розробляти стратегії з мінімізації ризиків та посилення конкурентних переваг.
- Забезпечувати ефективне використання ресурсів та підвищувати стійкість до кризових ситуацій.

Зазвичай при аналізі ключових показників зосереджуються на порівнянні основних показників підприємства з середньогалузевими значеннями у вигляді стовпчикової діаграми (рис. 1.3), чи на графік змін окремого показника за останні 5-10 років (рис. 1.4).

Приклади

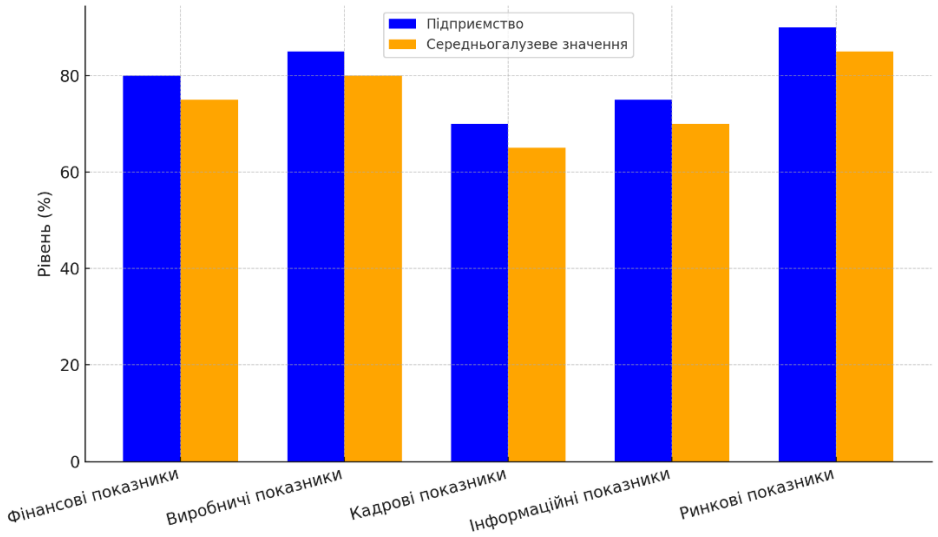

Рисунок 1.3 – Порівняння основних показників підприємства з середньогалузевими значеннями у вигляді стовпчикової діаграми (умовні дані)**.**

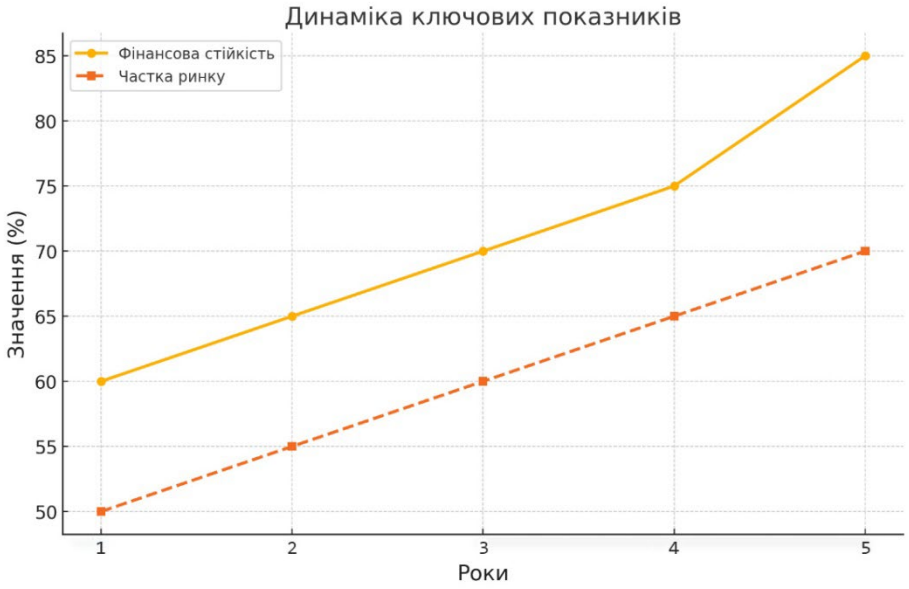

Рисунок 1.4 – Графік змін коефіцієнта фінансової стійкості та частки ринку за останні роки.

Отже ключові показники економічної безпеки є основою для стратегічного управління підприємством. Їх аналіз дозволяє вчасно виявляти ризики, розробляти ефективні заходи протидії та забезпечувати стабільний розвиток бізнесу. Успішне застосування цих показників є запорукою конкурентоспроможності та довгострокового процвітання промислового підприємства.

1.3 Основні аспекти забезпечення економічної безпеки на підприємстві

Економічна безпека підприємства є результатом системної роботи, спрямованої на захист від загроз та створення умов для стабільного розвитку. Забезпечення економічної безпеки передбачає впровадження цілого комплексу заходів, що охоплюють ключові сфери діяльності підприємства. Ці аспекти взаємопов'язані, і ефективність економічної безпеки залежить від їх гармонійного функціонування.

Для всебічної характеристики системи захищеності суб'єкта господарювання важливо зорієнтуватися у сучасних підходах щодо її функціонування:

1. Наявна система економічної захищеності суб'єкта господарювання не повинна бути стандартною. Насамперед, вона має бути досить оригінальною для кожного промислового підприємства, адже суттєвим чином зумовлюється станом розвитку та функціонуючою структурою певних виробничих можливостей, максимального їх використання, а також цілеспрямованої продуктивної виробничої діяльності. Дана система повинна спиратись на відповідну високу кваліфікацію управлінського персоналу, належний стан трудової дисципліни, розгалужену мережу зовнішніх і внутрішніх контактів суб'єкта господарювання, належного конкурентного середовища тощо.

2. Система економічної захищеності суб'єкта господарювання є певною мірою самостійною та відносно відокремленою від подібних управлінських систем інших промислових підприємств. В той же час її відокремленість є досить відносною, адже система економічної захищеності суб'єкта господарювання являє собою складову безпеки значно вищого рівня. Переважна більшість загальних аспектів роботи системи економічної захищеності суб'єкта господарювання зазвичай вимагає втручання вищої управлінської ланки, або може бути вирішена на загальнодержавному рівні.

Діяльність служби економічної захищеності конкретного суб'єкта господарювання певною мірою зумовлена потребою в активній протидії аналогічним службам безпеки підприємств-конкурентів. Така служба повинна створюватись та функціонувати, ґрунтуючись на державних нормативно-правових актах, а також на можливості придбання сучасних засобів захищеності, високому рівні підготовки й належній кваліфікації управлінського персоналу тощо.

3. Ефективна система економічної захищеності суб'єкта господарювання має бути комплексною. На неї покладається завдання забезпечення функціонування захищеності економічної, інформаційної, інноваційної, інтелектуальної, кадрової, фізичної, техногенної, екологічної, пожежної тощо. Виходячи із зазначеного, можна переконливо стверджувати, що в її структурі обов'язково повинні бути надані окреслені елементи, задіяні органи управління, використовувані продуктивні сили та необхідні засоби (рис. 1.5).

Рисунок 1.5 – Фактори до формування економічної захищеності підприємства

Сучасну систему економічної захищеності суб'єкта господарювання слід розглядати в часовій площині як тривалий проект, що спрямований на майбутнє який відповідає запитам сучасності. Підходи до розробки проекту в поточних і стратегічних перспективах є досить різними (рис. 1.6).

Рисунок 1.6 – Фактори впливу на ЕБП в короткостроковому та довгостроковому періоді

Економічна захищеність суб'єкта господарювання – це така система, в якій поєднуються різноманітні елементи або ланки, які неможливо розглядати окремо. Забезпечення необхідних умов для економічної захищеності суб'єкта господарювання можна досягти без додаткових вкладень та залучення нових інвестицій, опираючись на сучасні організаційні заходи, які дають змогу використати внутрішні резерви, впровадити заходи щодо економії ресурсів, а також часткові зміни у внутрішніх виробничих процесах суб'єкта господарювання. Проте окреслені заходи повинні реалізовуватись під жорстким контролем з боку служби економічної безпеки суб'єкта господарювання, оскільки існує вірогідність впливу значної кількості внутрішніх і зовнішніх загроз. Альтернативний спосіб передбачає ефективне втілення інноваційних технологічних розробок, і тим самим використання сучасної техніки, потребує суттєвих інвестицій, що є можливим лише при наявності порівняно високої прибутковості суб'єкта господарювання. Дуже важливе місце при створенні ефективної системи економічної захищеності суб'єкта господарювання посідають значні витрати на її утримання. Витрати на економічний захист власності залежать від її вартості або пріоритетності для власника підприємства: чим вищою є вартість власності, що вимагає захисту, тим значно більше коштів слід витратити на це. Загалом, підприємства світових лідерів промислового виробництва витрачають на цю сферу від 15 до 20% прибутку. При цьому п**рактичні інструменти забезпечення економічної безпеки мають включати:**

1. **Системи ризик-менеджменту** – ідентифікація, аналіз та управління ризиками.
2. **Інформаційний моніторинг** – відстеження змін у ринковому середовищі.
3. **Аудиторський контроль** – регулярна перевірка ефективності заходів безпеки.
4. **Планування сценаріїв** – підготовка до можливих кризових ситуацій.

1.4 Види загроз економічній безпеці

Економічна безпека підприємства тісно пов'язана із зовнішнім та внутрішнім середовищем, у якому воно функціонує. Загрози, що можуть впливати на стабільність та розвиток підприємства, є різноманітними і вимагають комплексного підходу до їх аналізу, ідентифікації та протидії. Розуміння видів загроз — перший крок до ефективного управління економічною безпекою.

Класифікація загроз економічній безпеці

1. **Зовнішні загрози**

Окреслені загрози походять із середовища, яке знаходиться поза межами контролю підприємства, і включають:

1. **Економічні загрози:**
   - коливання валютних курсів;
   - інфляція та дефляція;
   - глобальні економічні кризи;
   - висока залежність від постачальників чи клієнтів.
2. **Політичні загрози:**
   - нестабільність політичної ситуації;
   - санкції, що впливають на бізнес;
   - непередбачувані зміни у законодавстві.
3. **Соціальні загрози:**
   - демографічні зміни;
   - невдоволення місцевих громад або працівників;
   - соціальні протести, що впливають на роботу підприємства.
4. **Технологічні загрози:**
   - стрімкі темпи інновацій, що роблять існуючі технології застарілими;
   - залежність від технологій, що створюють ризики у разі збоїв.

2. **Внутрішні загрози**

Ці загрози виникають у межах самого підприємства:

1. **Фінансові загрози:**
   - неефективне використання фінансових ресурсів;
   - дефіцит оборотного капіталу;
   - ризик шахрайства серед персоналу.
2. **Кадрові загрози:**
   - висока плинність кадрів;
   - недостатня кваліфікація персоналу;
   - недобросовісні дії працівників (витік інформації, конфлікти).

3. **Інформаційні загрози:**
   - несанкціонований доступ до даних;
   - витік конфіденційної інформації;
   - кіберзагрози (хакерські атаки, шкідливе програмне забезпечення).
4. **Операційні загрози:**
   - збої у постачанні матеріалів чи комплектуючих;
   - низька якість виробленої продукції;
   - неефективне планування виробництва (табл.1.1).

Таблиця 1.1 – Класифікація загроз економічній безпеці

Тип загрози	Категорія	Приклади
Зовнішні	Економічні	Коливання валют, криза ринку
	Політичні	Санкції, зміни законодавства
	Соціальні	Демографічні зміни, протести
	Технологічні	Заходження інноваційних конкурентів
Внутрішні	Фінансові	Нестача капіталу, шахрайство
	Кадрові	Текучість кадрів, недобросовісні дії працівників
	Інформаційні	Витік даних, хакерські атаки
	Операційні	Збої у постачанні, низька якість продукції

Глибокий аналіз загроз

Для розуміння загроз і розробки ефективних заходів захисту необхідно проводити регулярний аналіз загроз за допомогою таких інструментів:

1. **PEST-аналіз** (Політика, Економіка, Соціум, Технології, Законодавство, Екологія): для ідентифікації зовнішніх загроз.
2. **SWOT-аналіз**: для оцінки слабких сторін підприємства та можливостей їх посилення.
3. **SNW** – аналіз, метод розробки сценаріїв розвитку подій
4. **Мапа ризиків:** для визначення пріоритетності загроз залежно від їхнього впливу на бізнес (рис. 1.7).

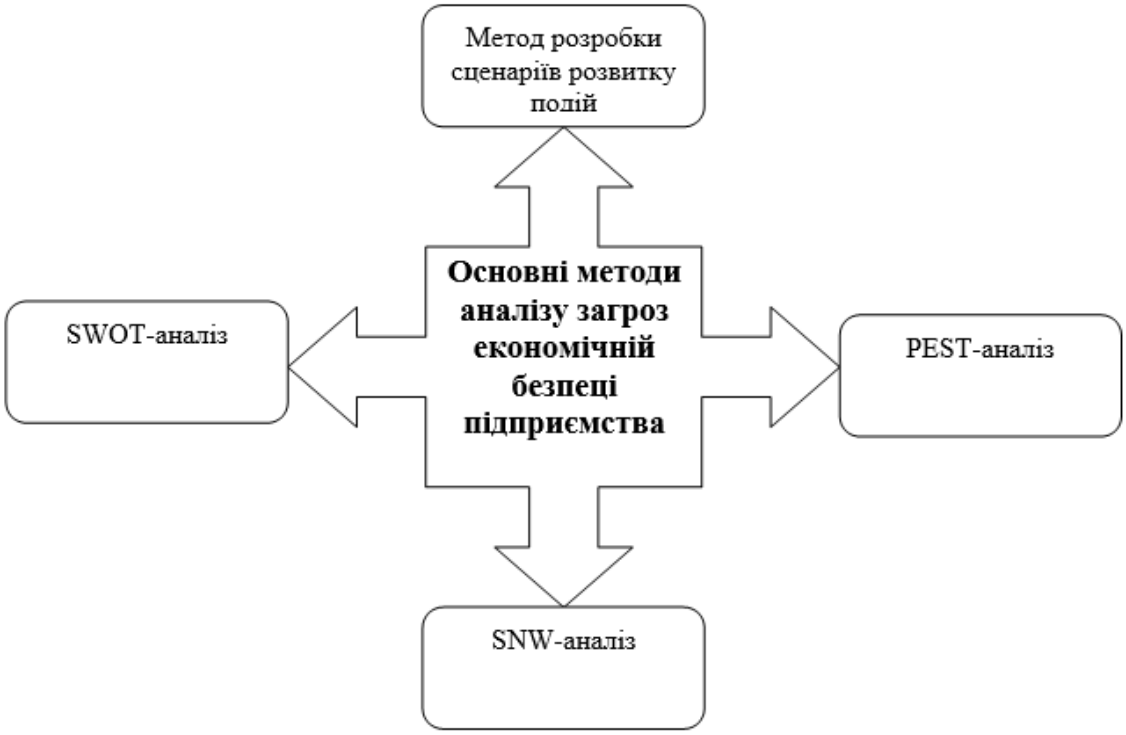

Рисунок 1.7 – Основні методи оцінювання рівня загроз економічній безпеці підприємства

Використання SWOT – аналізу як методу виявлення й якісного оцінювання рівня загроз безпеці доцільне при оцінюванні поточного стану безпеки підприємства і виявленні загроз.

Використання SWOT-аналізу при виявленні та окресленні рівня загроз економічній безпеці доцільно вважати, що найбільш суттєві загрози виявляються в процесі, коли небажаний розвиток подій зовнішнього середовища промислового підприємства стикається з уразливими сторонами власне механізму керування економічною безпекою підприємства, тобто в даному випадку виникає відємний кумулятивний ефект. Найкращі можливості досягнення бажаного рівня економічної безпеки промислового підприємства є результатом поєднання сукупної дії бажаних факторів зовнішнього середовища та переваг власне самого механізму керування фінансовою захищеністю.

Застосування SWOT-аналізу дає змогу окреслити стратегію забезпечення захисту товаровиробника. Якнайкраще для цього підходить відповідна матриця, зосередимо при цьому увагу на фінансовій складовій, як на ключовому чиннику формування ЕБП (рис. 1.8).

ЗОВНІШНЄ СЕРЕДОВИЩЕ

ВНУТРІШНЄ СЕРЕДОВИЩЕ	***МОЖЛИВОСТІ*** Позитивні зовнішні умови здійснення фінансової діяльності	***ЗАГРОЗИ*** Негативні зовнішні чинники у вигляді зовнішніх загроз фінансовій безпеці
СИЛЬНІ СТОРОНИ Позитивні внутрішні умови здійснення фінансової діяльності	Поле ВСС-ЗМ *Стратегія формування і підтримки найкращих сторін механізму керування фінансовим захистом на шляху побудови товаровиробником бажаних можливостей у зовнішньому середовищі.*	Поле ВСС-ЗЗ *Стратегія застосування сильних внутрішніх можливостей для ймовірного подолання небажаних втручань зовнішнього середовища.*
СЛАБКІ СТОРОНИ Негативні внутрішні умови у вигляді внутрішніх загроз	Поле ВСлС-ЗМ *Розробка та реалізація стратегії, яка має бути спрямована на подолоння слабких сторін механізму управління ФЗП за рахунок можливостей, які надає для нього зовнішнє середовищє.*	Поле ВСлС–ЗЗ *Кризова ситуація, коли до внутрішніх загроз фінансовій захищеності підприємства додаються ще й зовнішні.*

Рисунок 1.8 – SWOT-аналіз для виокремлення та якісної оцінки загроз фінансовій захищеності

На перехресті встановлених груп факторів утворюються поля, які дозволяють обирати бажану стратегію забезпечення фінансового захисту підприємства.

Для зазначених перехресть доцільно використовувати відповідні типи стратегій:

1) ВСС–ЗМ – на цьому перетині обєднуються внутрішні переваги механізму керування фінансовим захистом та сприятливі зовнішні фактори.

2) ВСлС–ЗМ – на даному перехресті внутрішні недоліки механізму керування фінансовою захищеністю поєднуються з сприятливими чинниками зовнішнього середовища.

3) ВСС–ЗЗ – тут загрози зовнішнього середовища перетинаються з внутрішніми перевагами механізму керування фінансовою захищеністю.

4) ВСлС–ЗЗ – це можна назвати кризовим перетином, оскільки відбувається поєднання зовнішніх загроз зі слабкими сторонами механізму керування фінансовим захистом підприємства.

З метою встановлення рівня загроз економічної безпеки товаровиробника досить вдалим є застосування методу PEST-аналізу, що дає змогу встановлювати загрози зовнішнього середовища (рис. 1.9).

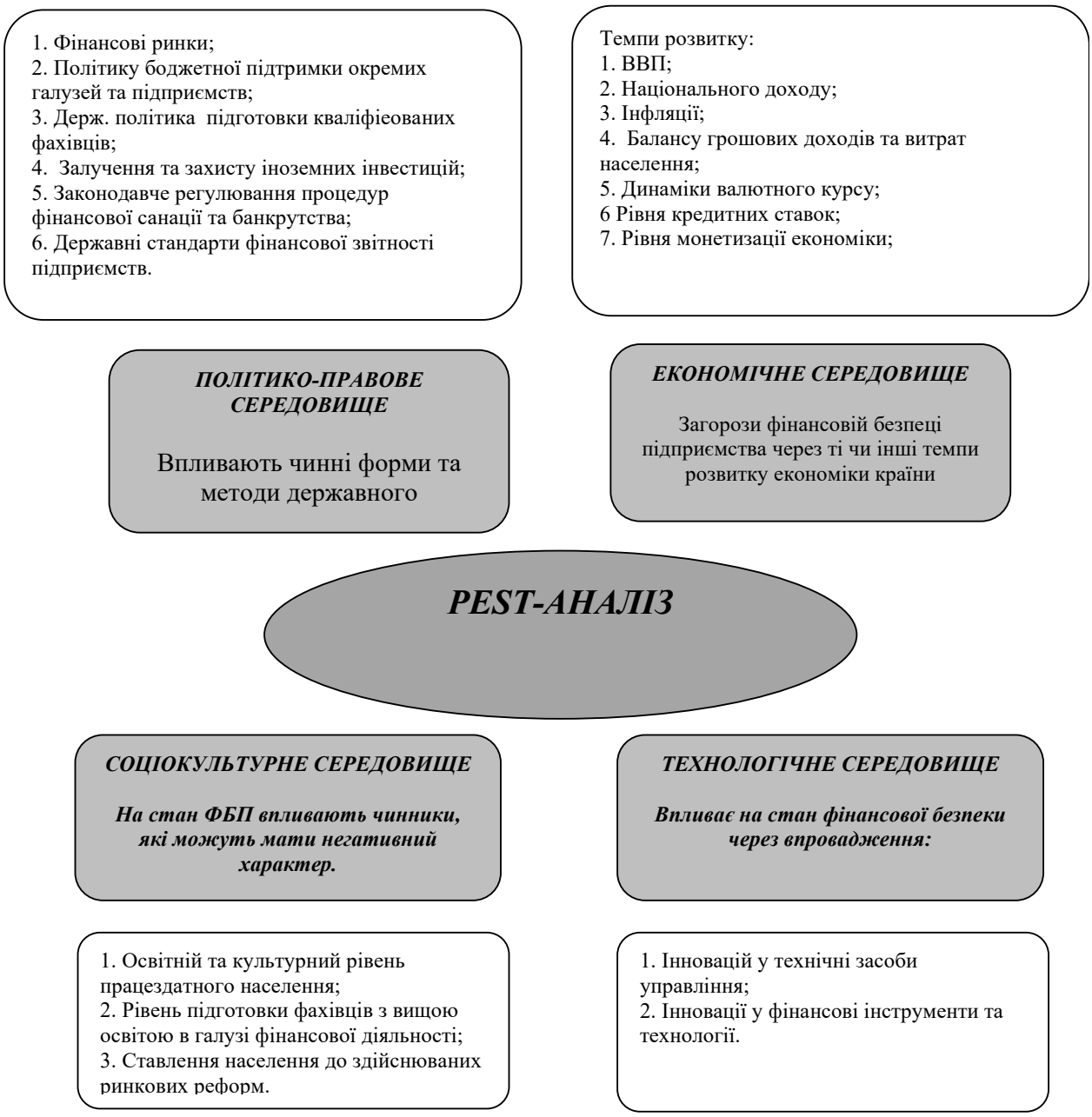

Рисунок 1.9 – PEST-аналіз загроз зовнішнього середовища

Відповідно до цього методу, зазначені загрози можна поділити різновиди, які можна позначити англійськими літерами PEST:

P (political and legal environment);

E (economic environment);

S (sociocultural environment);

T (technological environment).

Вплив бажаних чи небажаних факторів, які відбиваються на фінансовій захищеності промислового підприємства, можна дослідити спираючись на п’ятибальну систему. Тоді нейтральна позиція буде нульовою, а отже буде відповідати значенням середнім по галузі (того чи іншого фактору), а отже буде віддзеркалювати рівень фінансового захисту на аналогічних суб’єктах господарювання.

Даний підхід дозволяє приймати нейтральну позицію як певний порогів рівень фінансової захищеності промислового підприємства, тобто її критичним рівнем, після якого товаровиробник опиняється у кризовому фінансовому становищі.

Приклади

При дослідженні ЕБП, преше, що маємо зробити – це визначитись з ключовими чинниками та дослідити вплив кожної окремої складової на рівень економічної захищеності. Таким чином ми досліджуємо основні показники господарської діяльності, основні показники ефективності роботи підприємства, основні показники інноваційної діяльності, ключові дані по співробітникам. Це дає можливість визначитись з переліком ключових складових ЕБП та з-поміж 17 складових, наприклад, визначити 4 – фінансову, кадрову, інформаційну та операційну (як поєднання окремих складових інших чинників). Надалі ми маємо визначитись з рівнем впливу. Він може мати такий вигляд як на рисунку 1.10 чи на рисунку 1.11

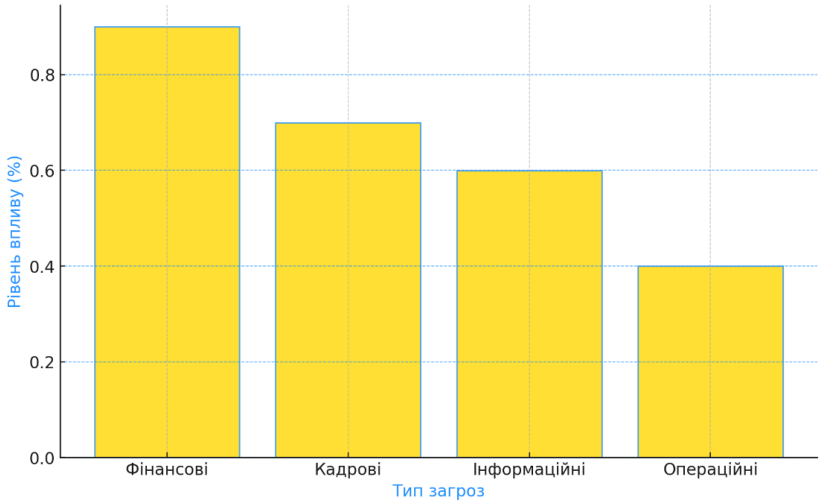

Рисунок 1.10 – Рівень впливу ключових загроз

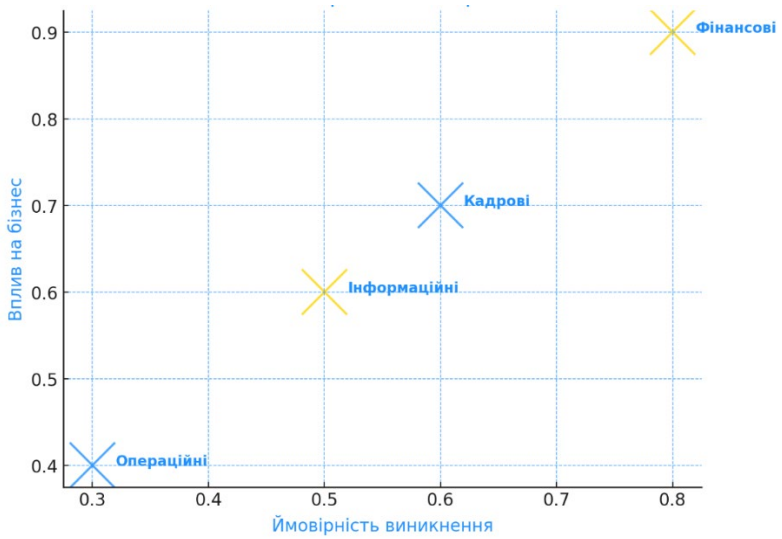

Рисунок 1.11 – Матриця, яка відображає імовірність виникнення загрози (низька, середня, висока) та її вплив на бізнес.

Формування безпечного середовища нерозривно пов'язано з побудовою відповідної бізнес-стратегії. В процесі формування бізнес-стратегії досить важливо чітко уявляти, яким чином суб'єкт господарювання створює продукт: за рахунок продуктивного бренду, досить низької вартості наявного капіталу, економії на масштабах, синергії бізнес-одиниць, приоритетних відносин з покупцями та постачальниками або доступу до специфічних ресурсів. Слід зазначити, що зазвичай не існує, уніфікованого підходу до формування бізнес-стратегії, адже кожна з них дає змогу досягнення успіхів за різнопланових умов існування. Обгрунтування підходу до формування бізнес-стратегії має відбуватись з урахуванням об'єктивної оцінки наявних ресурсів. Зазвичай при обґрунтуванні вибору підприємством альтернативи бізнес-стратегії опираються на наявні передумови – інфраструктуру та ринкове середовище, технології, компетенції й передовий досвід. Так, дослідження умов існування підприємств металургійної галузі дає можливість формувати підходи до обґрунтування бізнес-стратегій, які віддзеркалюють фундаментальні довгострокові імперативи (табл. 1.2).

Таблиця 1.2 – Структура стратегічних імперативів підприємств Запорізького металургійного комплексу

Умови функціонування	Підходи до формування захищеності	Фундаментальні стратегічні імперативи
ПАТ «Запорізький виробничий алюмінієвий комбінат» – низький рівень використання капіталу (коефіцієнт автономії у 2014р. -13,8)	Використання комплексу фінансових індикаторів	▪ Визначення загальної фінансової стратегії підприємства
ПАТ «Запорізький завод феросплавів» ПАТ «Запорізький виробничий алюмінієвий комбінат» ТОВ «Запорізький титано-магнієвий комбінат»	Позиціонування підприємства на ринку	▪ Фокусування на ідентифікації привабливих споживчих сегментів ▪ Визначення стратегічного фокусу підприємств
	Конкурентний підхід до обґрунтування інноваційного ринкового потенціалу	▪ Формування інноваційного потенціалу цінності продукту, спираючись на мінімізацію витрат та підвищення ефективності новацій, спираючись на позитивну реакцію споживача
	Взаємодія зі споживачем	▪Розробка інноваційного підходу, спираючись на знання й досвід, набуті в процесі отримання зворотнього зв'язку від споживачів.
ПАТ «Запорізький металургійний комбінат «Запоріжсталь», на інших – в стадії розробки	Ресурсно-орієнтований підхід та визначення ключових компетенцій	▪ Впровадження новаторських технологій ▪ Створення позитивного іміджу ▪ Ідентифікація, зміцнення, розвиток, підтримка й застосування власних конкурентних переваг та організаційних можливостей
ПАТ «Запорізький металургійний комбінат «Запоріжсталь» та ПАТ «Електрометалургійний комбінат «Дніпроспецсталь» ім. Кузьміна» – найвищий рівень розвитку	Підхід, орієнтований на розвиток власного персоналу підприємства та його навчання	▪ Наявність кваліфікованого, високо мотивованого персоналу ▪ Розробка «амбіційної» бізнес-стратегії

Ідентифікація видів загроз та їх класифікація є основою для забезпечення економічної безпеки промислового підприємства. Розуміння сутності загроз дозволяє підприємству ефективно протидіяти викликам, залишатися конкурентоспроможним навіть у складних умовах ринкової нестабільності, а також гарантувати сталий розвиток бізнесу.

Перелік питань:

1. Що таке економічна безпека промислового підприємства? Як її визначають у сучасному бізнес-середовищі?
2. Які основні характеристики притаманні економічній безпеці підприємства?
3. Чому економічна безпека є важливим елементом стабільного функціонування підприємства?
4. Які ключові показники використовуються для оцінки рівня економічної безпеки підприємства?
5. Як фінансові показники впливають на економічну безпеку підприємства?
6. Що включає поняття виробничої безпеки? Як вона сприяє економічній стійкості підприємства?
7. Як оцінюється рівень інформаційної безпеки на підприємстві?
8. Які ризики можуть виникати в кадровому аспекті економічної безпеки?
9. Які зовнішні загрози найчастіше впливають на економічну безпеку промислового підприємства?
10. Як політичні фактори впливають на економічну безпеку підприємства? Наведіть приклади.
11. Які внутрішні загрози можуть становити найбільшу небезпеку для підприємства?
12. Як можна мінімізувати операційні ризики на підприємстві?
13. Що таке PESTLE-аналіз, і як його використовують для ідентифікації зовнішніх загроз?
14. У чому полягає значення регулярного аудиту для забезпечення економічної безпеки?
15. Як впровадження сучасних інформаційних технологій може підвищити рівень економічної безпеки?
16. Які аспекти корпоративної культури сприяють економічній безпеці підприємства?
17. Як законодавчі зміни можуть впливати на економічну безпеку підприємства?
18. Що таке мапа ризиків, і як її можна застосовувати для управління загрозами?
19. Які стратегії слід використовувати для захисту підприємства від кіберзагроз?
20. Як маркетингова діяльність підприємства впливає на його економічну безпеку?

Тести:

1. **Економічна безпека підприємства — це:**
   а) здатність підприємства мінімізувати витрати;
   б) захищеність підприємства від зовнішніх і внутрішніх загроз;
   в) досягнення максимальної рентабельності;
   г) підвищення кваліфікації працівників.
2. **До зовнішніх загроз економічній безпеці належать:**
   а) низька кваліфікація працівників;
   б) зміни в політичному середовищі;
   в) низький рівень інформаційної безпеки;
   г) витік комерційної таємниці.

3. **Основна мета фінансової безпеки підприємства:**
   а) зменшення витрат;
   б) уникнення банкрутства;
   в) забезпечення фінансової стабільності;
   г) оптимізація податкових виплат.

4. **Виробнича безпека спрямована на:**
   а) зменшення витрат на енергоресурси;
   б) захист інтелектуальної власності;
   в) забезпечення безперебійності виробничих процесів;
   г) уникнення санкцій.

5. **Інформаційна безпека підприємства охоплює:**
   а) контроль фінансових витрат;
   б) забезпечення захисту конфіденційних даних;
   в) підвищення кваліфікації персоналу;
   г) оптимізацію використання ресурсів.

6. **Який метод використовується для аналізу зовнішніх загроз підприємства?**
   а) SWOT-аналіз;
   б) PESTLE-аналіз;
   в) фінансовий аудит;
   г) мапа ризиків.

7. **До основних функцій управління економічною безпекою належить:**
   а) створення конкурентних переваг;
   б) контроль витрат;
   в) захист ресурсів підприємства;
   г) оптимізація операційних процесів.

8. **Ключовий показник фінансової безпеки — це:**
   а) рівень ліквідності активів;
   б) рівень лояльності працівників;
   в) кількість інформаційних загроз;
   г) обсяг виробництва.

9. **Основне завдання кадрової безпеки підприємства:**
   а) створення системи кіберзахисту;
   б) підвищення кваліфікації працівників;
   в) забезпечення якісного постачання сировини;
   г) оптимізація витрат на персонал.

10. **Що таке мапа ризиків?**
   а) система оцінки активів підприємства;
   б) візуалізація імовірності та впливу загроз;

в) метод управління інформаційною безпекою;
г) оцінка якості персоналу.

11. **Який із наведених аспектів є внутрішньою загрозою для підприємства?**
а) політична нестабільність;
б) низька кваліфікація персоналу;
в) зростання конкуренції;
г) зміни у валютному курсі.

12. **Основна мета аудиту в економічній безпеці:**
а) підготовка до фінансової звітності;
б) виявлення слабких місць у системі безпеки;
в) оптимізація витрат;
г) аналіз продуктивності працівників.

13. **Що таке корпоративна культура безпеки?**
а) система правил для підвищення ефективності роботи;
б) стратегія розвитку корпоративного бренду;
в) комплекс заходів для підвищення безпеки через цінності й поведінку персоналу;
г) навчальна програма для працівників.

14. **Головною метою управління інформаційною безпекою є:**
а) контроль витрат на інформаційні технології;
б) забезпечення конфіденційності, цілісності та доступності даних;
в) запобігання фінансовим ризикам;
г) моніторинг роботи інформаційних систем.

15. **До інструментів протидії внутрішнім загрозам належить:**
а) створення стратегічного запасу матеріалів;
б) підвищення кваліфікації персоналу;
в) використання систем PESTLE-аналізу;
г) впровадження технологій блокчейн.

16. **Як фінансова стабільність впливає на економічну безпеку?**
а) забезпечує незалежність від зовнішніх джерел фінансування;
б) дозволяє зменшити витрати на операції;
в) сприяє підвищенню ефективності персоналу;
г) запобігає витоку інформації.

17. **Що є ключовим елементом правового аспекту економічної безпеки?**
а) дотримання нормативно-правових актів;
б) контроль витрат на юридичні послуги;
в) моніторинг інформаційної безпеки;
г) управління операційними ризиками.

18. **Як виробничий аспект впливає на економічну безпеку?**
    а) забезпечує стабільний обсяг продажів;
    б) підвищує конкурентоспроможність за рахунок якості продукції;
    в) зменшує кількість інформаційних загроз;
    г) сприяє формуванню корпоративної культури.

19. **Основною перевагою використання мапи ризиків є:**
    а) забезпечення прогнозування виробничих обсягів;
    б) виявлення найбільш небезпечних загроз;
    в) оцінка рівня рентабельності;
    г) управління маркетинговими кампаніями.

20. **Яка роль маркетингового аспекту в економічній безпеці?**
    а) контроль за витратами на рекламу;
    б) аналіз ризиків репутаційних втрат;
    в) управління рівнем ліквідності активів;
    г) створення стратегічного запасу сировини.

Практичні завдання:

Завдання 1. Аналіз фінансової безпеки

Використовуючи умовні дані про підприємство (фінансовий баланс, звіт про прибутки та збитки), розрахуйте такі показники фінансової безпеки:

1. Коефіцієнт ліквідності активів.
2. Рентабельність виробництва.
3. Частку власного капіталу в структурі фінансування. Поясніть, як кожен із показників впливає на фінансову безпеку підприємства.

Завдання 2. Ідентифікація загроз

1. Перерахуйте можливі зовнішні та внутрішні загрози для промислового підприємства, що працює у сфері машинобудування.
2. Використовуючи метод PESTLE-аналізу, проаналізуйте зовнішнє середовище підприємства.
3. Розробіть заходи для мінімізації найбільш імовірних загроз.

Завдання 3. Оцінка кадрової безпеки

1. Визначте ключові ризики, пов’язані з персоналом, для підприємства у сфері послуг.
2. Запропонуйте механізми підвищення лояльності працівників та захисту від витоку комерційної інформації.
3. Розробіть анкету для оцінки рівня задоволеності персоналу та його лояльності до підприємства.

Завдання 4. Побудова мапи ризиків

1. На основі наведеної таблиці загроз, визначте ймовірність виникнення кожної загрози та її потенційний вплив на підприємство.

2. Побудуйте мапу ризиків, відобразивши загрози у координатах "імовірність" – "вплив".
3. Запропонуйте заходи зниження ризиків для двох найбільш небезпечних загроз.

Завдання 5. Інформаційна безпека

1. Складіть список потенційних загроз для інформаційної безпеки підприємства.
2. Розробіть політику безпеки для запобігання витоку конфіденційних даних.
3. Опишіть, як впровадження багатофакторної аутентифікації може підвищити рівень захисту даних.

Завдання 6. Створення плану захисту

1. Розробіть короткий план захисту фінансових, інформаційних та виробничих ресурсів підприємства.
2. Укажіть, які інструменти та технології необхідно використовувати для забезпечення безпеки кожного виду ресурсів.
3. Визначте відповідальних осіб за виконання заходів безпеки.

Завдання 7. SWOT-аналіз економічної безпеки

Використовуючи умовний приклад підприємства, проведіть SWOT-аналіз.

1. Визначте сильні сторони, слабкі сторони, можливості та загрози для економічної безпеки підприємства.
2. На основі аналізу розробіть рекомендації щодо покращення системи економічної безпеки.

Завдання 8. Оцінка інформаційної загрози

1. Наведіть приклад реального або умовного випадку витоку інформації на підприємстві.
2. Проаналізуйте наслідки цієї події для економічної безпеки.
3. Запропонуйте заходи для уникнення подібних інцидентів у майбутньому.

Завдання 9. Аналіз корпоративної культури

1. Визначте, як корпоративна культура впливає на економічну безпеку підприємства.
2. Запропонуйте заходи для формування культури безпеки серед працівників.
3. Розробіть набір правил для поведінки працівників у критичних ситуаціях.

Завдання 10. Оцінка ефективності заходів економічної безпеки

1. Використовуючи дані про заходи безпеки підприємства, оцініть їх ефективність за такими критеріями:
   - зниження кількості ризиків;
   - вартість впровадження заходів;
   - рівень задоволеності персоналу та партнерів.
2. Запропонуйте можливі поліпшення системи економічної безпеки.

ТЕМА 2. НОРМАТИВНО-ПРАВОВА БАЗА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

2.1 Законодавчі акти, що регулюють економічну безпеку.
2.2 Міжнародні стандарти та практики.
2.3 Аналіз правових ризиків для підприємств.
2.4 Дотримання законодавства як основа економічної безпеки.

2.1 Законодавчі акти, що регулюють економічну безпеку

Забезпечення економічної безпеки підприємства в Україні регулюється низкою законодавчих актів, які встановлюють правові основи для захисту інтересів суб'єктів господарювання. Основними документами в цій сфері є:

1. **Конституція України**: Головний закон держави, який визначає основи економічної безпеки. Зокрема, стаття 17 зазначає, що "забезпечення економічної безпеки України є найважливішою функцією держави". Стаття 42 гарантує право на підприємницьку діяльність та обов'язок держави захищати конкуренцію і права споживачів.
2. **Цивільний кодекс України**: Встановлює загальні положення щодо майнових і немайнових відносин, які впливають на економічну безпеку підприємств, зокрема щодо зобов'язань та відповідальності.
3. **Кримінальний кодекс України**: Містить норми, що передбачають відповідальність за економічні злочини, такі як шахрайство, розкрадання, ухилення від сплати податків, які можуть загрожувати економічній безпеці підприємства.
4. **Закон України "Про основи національної безпеки України"**: Визначає основні напрями державної політики у сфері національної безпеки, включаючи економічну складову, та встановлює механізми її забезпечення.
5. **Закон України "Про охоронну діяльність"**: Регулює діяльність суб'єктів, що надають послуги з охорони майна та фізичних осіб, що є важливим аспектом економічної безпеки підприємств.
6. **Закон України "Про інформацію"**: Встановлює правові основи інформаційної діяльності, захисту інформації та доступу до неї, що є критичним для захисту комерційної таємниці та конфіденційних даних підприємства.
7. **Закон України "Про захист економічної конкуренції"**: Спрямований на запобігання монополізму та недобросовісній конкуренції, що безпосередньо впливає на економічну безпеку підприємств.
8. **Закон України "Про захист прав споживачів"**: Визначає права споживачів та обов'язки підприємств щодо якості продукції та послуг, що впливає на репутацію та економічну стабільність підприємства.
9. **Закон України "Про відновлення платоспроможності боржника або визнання його банкрутом"**: Регулює процедури банкрутства, що є важливим для підприємств у кризових ситуаціях.

Крім національних законодавчих актів, на економічну безпеку підприємств впливають міжнародні стандарти та угоди, такі як Європейська конвенція "Про деякі міжнародні

аспекти банкрутства" та рекомендації Європейського комітету зі стандартизації, які сприяють гармонізації підходів до забезпечення економічної безпеки на міжнародному рівні.

Варто зазначити, що в Україні існує потреба в удосконаленні нормативно-правової бази для більш ефективного забезпечення економічної безпеки підприємств, зокрема шляхом розробки спеціалізованих законодавчих актів та впровадження міжнародних стандартів у національне законодавство.

2.2 Міжнародні стандарти та практики

Забезпечення економічної безпеки підприємства вимагає дотримання міжнародних стандартів та впровадження передових практик, які сприяють ефективному управлінню ризиками та захисту від потенційних загроз. Основними міжнародними стандартами в цій сфері є:

1. **ISO 31000:2018 "Управління ризиками – Принципи та настанови"**: Цей стандарт надає універсальні принципи та настанови щодо управління ризиками, які можуть бути застосовані в будь-якій організації, незалежно від її розміру чи галузі діяльності. Він допомагає підприємствам ідентифікувати, оцінювати та мінімізувати ризики, що впливають на їхню економічну безпеку.
2. **ISO 22301:2019 "Безпека та стійкість – Системи управління безперервністю бізнесу – Вимоги"**: Стандарт визначає вимоги до створення, впровадження та вдосконалення систем управління безперервністю бізнесу. Він сприяє підготовці підприємства до можливих збоїв у діяльності та забезпечує швидке відновлення критичних функцій після інцидентів.
3. **ISO/IEC 27001:2022 "Інформаційні технології – Методи захисту – Системи управління інформаційною безпекою – Вимоги"**: Цей стандарт встановлює вимоги до систем управління інформаційною безпекою, допомагаючи підприємствам захищати свої інформаційні ресурси від несанкціонованого доступу, втрати чи пошкодження.
4. **ISO 28000:2007 "Системи управління безпекою для ланцюгів постачання – Вимоги"**: Стандарт спрямований на забезпечення безпеки в ланцюгах постачання, допомагаючи підприємствам ідентифікувати та контролювати загрози, що можуть вплинути на процес постачання товарів і послуг.
5. **ISO 22316:2017 "Безпека та стійкість – Організаційна стійкість – Принципи та настанови"**: Цей стандарт надає настанови щодо підвищення організаційної стійкості, що є ключовим елементом економічної безпеки підприємства.

Впровадження цих стандартів дозволяє підприємствам:

– **систематизувати процеси управління ризиками**: Стандарти надають структурований підхід до ідентифікації та оцінки ризиків, що сприяє ефективному їх контролю.

– **підвищити готовність до надзвичайних ситуацій**: Визначення процедур реагування на інциденти забезпечує швидке відновлення діяльності після збоїв.

– **забезпечити захист інформаційних ресурсів**: Впровадження заходів інформаційної безпеки мінімізує ризики витоку чи втрати даних.

– **підвищити довіру партнерів та клієнтів**: Дотримання міжнародних стандартів свідчить про відповідальність підприємства та його здатність забезпечувати безпеку своїх процесів.

Крім стандартів ISO, існують інші міжнародні практики, які сприяють економічній безпеці підприємств:

- **Модель COSO (Комітет спонсорських організацій Тредвей)**: Рамкова модель для управління ризиками та внутрішнього контролю, яка допомагає підприємствам ефективно ідентифікувати та управляти ризиками.
- **Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**: Підхід до оцінки ризиків інформаційної безпеки, що дозволяє підприємствам визначати критичні загрози та вразливості.

Варто зазначити, що впровадження міжнародних стандартів та практик потребує адаптації до специфіки діяльності конкретного підприємства та врахування національних особливостей регулювання. Проте, дотримання цих стандартів сприяє підвищенню загальної економічної безпеки та конкурентоспроможності підприємства на міжнародному ринку.

2.3 Аналіз правових ризиків для підприємств

Аналіз правових ризиків є ключовим елементом забезпечення економічної безпеки підприємства. Правові ризики виникають через можливі зміни в законодавстві, недотримання нормативних вимог або укладення невигідних контрактів. Ідентифікація та управління цими ризиками дозволяють мінімізувати потенційні збитки та забезпечити стабільну діяльність підприємства.

Основні види правових ризиків для підприємств:

1. **Регуляторні ризики**: пов'язані зі змінами в законодавстві, які можуть вплинути на діяльність підприємства. Наприклад, введення нових податків або змін у трудовому законодавстві.
2. **Контрактні ризики**: виникають при укладенні договорів з контрагентами. Недостатньо чіткі умови або відсутність важливих положень можуть призвести до спорів або фінансових втрат.
3. **Судові ризики**: пов'язані з можливими судовими позовами проти підприємства, що можуть призвести до фінансових санкцій або репутаційних втрат.
4. **Ризики інтелектуальної власності**: виникають при порушенні прав на торговельні марки, патенти або авторські права, що може спричинити юридичні спори та фінансові втрати.

Етапи аналізу правових ризиків:

1. **Ідентифікація ризиків**: визначення потенційних правових загроз, які можуть вплинути на діяльність підприємства.
2. **Оцінка ризиків**: визначення ймовірності настання кожного ризику та можливих наслідків для підприємства.
3. **Розробка заходів управління**: визначення стратегій для мінімізації або усунення виявлених ризиків.

4. **Моніторинг та контроль**: постійне відстеження правового середовища та ефективності впроваджених заходів.

Методи управління правовими ризиками:

– **створення внутрішніх політик та процедур**: розробка чітких інструкцій для працівників щодо дотримання законодавства та внутрішніх нормативів;

– **юридичний аудит**: регулярна перевірка діяльності підприємства на відповідність чинному законодавству;

– **страхування ризиків**: укладення договорів страхування для покриття можливих збитків від реалізації правових ризиків;

– **навчання персоналу**: підвищення кваліфікації працівників у сфері правових питань та дотримання нормативних вимог.

Процес управління правовими ризиками при цьому матиме вигляд:

1. Ідентифікація ризиків → 2. Оцінка ризиків → 3. Розробка заходів управління → 4. Впровадження заходів → 5. Моніторинг та контроль → Повернення до 1 (цикл повторюється)

Ефективне управління правовими ризиками сприяє підвищенню економічної безпеки підприємства, знижує ймовірність фінансових втрат та покращує репутацію на ринку. Впровадження системного підходу до аналізу та управління правовими ризиками є невід'ємною складовою стратегії сталого розвитку підприємства.

Приклади

Таблиця 2.1 – Приклади правових ризиків та заходів управління

Вид ризику	Приклад	Заходи управління
Регуляторний	Зміна податкового законодавства	Постійний моніторинг законодавчих змін
Контрактний	Недотримання умов постачання контрагентом	Ретельний юридичний аналіз договорів
Судовий	Позов від споживача через неякісну продукцію	Впровадження системи контролю якості
Інтелектуальної власності	Використання незареєстрованої торговельної марки	Реєстрація торговельних марок та патентів

2.4 Дотримання законодавства як основа економічної безпеки

Дотримання законодавства є фундаментом економічної безпеки підприємства, оскільки забезпечує його стабільне функціонування та захист від потенційних загроз. Недотримання нормативно-правових актів може призвести до фінансових санкцій, репутаційних втрат та інших негативних наслідків.

Ключові аспекти дотримання законодавства для забезпечення економічної безпеки:

1. **Відповідність нормативним вимогам**: Підприємства повинні постійно стежити за змінами в законодавстві та адаптувати свою діяльність відповідно до нових вимог. Це стосується податкового, трудового, екологічного та інших аспектів законодавства.
2. **Розробка внутрішніх політик та процедур**: Створення чітких внутрішніх регламентів, які відповідають законодавчим вимогам, допомагає працівникам дотримуватися встановлених норм та мінімізує ризик порушень.
3. **Навчання та підвищення кваліфікації персоналу**: Регулярне проведення тренінгів та семінарів щодо актуальних змін у законодавстві сприяє підвищенню обізнаності працівників та запобігає можливим порушенням.
4. **Внутрішній контроль та аудит**: Постійний моніторинг діяльності підприємства на предмет відповідності законодавчим вимогам дозволяє вчасно виявляти та усувати недоліки.

Наслідки недотримання законодавства:

- **Фінансові санкції**: Штрафи та пені за порушення податкового, трудового чи екологічного законодавства можуть суттєво вплинути на фінансовий стан підприємства.
- **Репутаційні втрати**: Інформація про порушення може негативно вплинути на імідж підприємства, що призведе до втрати клієнтів та партнерів.
- **Юридичні наслідки**: Порушення законодавства можуть стати підставою для судових позовів, що спричинить додаткові витрати та відволікання ресурсів.

Схема процес забезпечення відповідності законодавству матиме такий вигляд:

1. Моніторинг законодавчих змін → 2. Оновлення внутрішніх політик → 3. Навчання персоналу → 4. Впровадження контролюючих механізмів → 5. Оцінка та коригування процесів

Приклад

Таблиця 2.2 – Приклади наслідків недотримання законодавства

Сфера порушення	Можливі наслідки
Податкове право	Штрафи, нарахування пені, блокування рахунків
Трудове право	Судові позови від працівників, компенсації
Екологічне право	Штрафи, призупинення діяльності, репутаційні втрати

Дотримання законодавства не лише запобігає негативним наслідкам, але й сприяє підвищенню довіри з боку клієнтів, партнерів та інвесторів, що в цілому зміцнює економічну безпеку підприємства.

Перелік питань:

1. Що таке нормативно-правова база економічної безпеки підприємства, і чому вона є важливою?
2. Які законодавчі акти України визначають основи економічної безпеки підприємств?
3. Як Конституція України впливає на регулювання економічної безпеки?
4. Які основні положення Господарського кодексу України стосуються економічної безпеки підприємств?
5. Як податкове законодавство може впливати на економічну безпеку підприємства?
6. Яка роль Закону України "Про захист економічної конкуренції" у забезпеченні економічної безпеки?
7. Які ризики виникають для підприємств через зміни у законодавстві?
8. Як судові позови можуть впливати на економічну безпеку підприємства?
9. Які міжнародні стандарти регулюють питання економічної безпеки підприємств?
10. Що таке ISO 31000, і як він допомагає у забезпеченні економічної безпеки?
11. Як стандарт ISO/IEC 27001 сприяє захисту інформаційної безпеки підприємств?
12. У чому полягає значення стандарту ISO 22301 для забезпечення безперервності бізнесу?
13. Які міжнародні практики, крім стандартів ISO, можуть бути корисними для українських підприємств?
14. Що таке регуляторні ризики, і як вони можуть впливати на діяльність підприємства?
15. Як правильно оцінити правові ризики, пов’язані з контрактною діяльністю?
16. Чому дотримання екологічного законодавства є важливим для економічної безпеки?
17. Як підприємства можуть запобігати втратам через ризики інтелектуальної власності?
18. Що таке внутрішній аудит, і яку роль він відіграє у забезпеченні відповідності законодавству?
19. Які наслідки можуть виникнути для підприємства у разі недотримання законодавства?
20. Які заходи потрібно впроваджувати для постійного моніторингу змін у нормативно-правовій базі?

Тести:

1. **Основна мета нормативно-правової бази економічної безпеки підприємства:**
   а) забезпечення прозорості бізнес-процесів;
   б) регулювання діяльності підприємства в рамках закону;
   в) визначення конкурентних переваг підприємства;
   г) створення стратегій для збільшення прибутку.
2. **До яких наслідків може призвести недотримання трудового законодавства?**
   а) підвищення рівня доходів;
   б) фінансові штрафи та судові позови;
   в) розширення ринкових можливостей;
   г) покращення умов праці для співробітників.

3. **Який з наведених стандартів стосується управління ризиками?**
   а) ISO 27001;
   б) ISO 22301;
   в) ISO 31000;
   г) ISO 28000.

4. **Основним завданням Закону України "Про захист економічної конкуренції" є:**
   а) регулювання ціноутворення;
   б) захист прав споживачів;
   в) запобігання монополізму та недобросовісній конкуренції;
   г) стимулювання інновацій.

5. **Що є основною функцією внутрішнього аудиту?**
   а) моніторинг змін у ринковому середовищі;
   б) перевірка відповідності діяльності підприємства законодавству;
   в) аналіз репутації підприємства;
   г) підготовка річної звітності.

6. **До міжнародних стандартів, які впливають на економічну безпеку підприємств, належить:**
   а) ISO 22301;
   б) ISO 14001;
   в) ISO 45001;
   г) ISO 9001.

7. **Які заходи сприяють запобіганню правових ризиків?**
   а) створення системи мотивації співробітників;
   б) проведення юридичного аудиту та моніторинг законодавства;
   в) впровадження програм підвищення кваліфікації співробітників;
   г) аналіз фінансової звітності.

8. **Що є ключовим елементом забезпечення відповідності законодавству?**
   а) оптимізація витрат;
   б) створення внутрішніх регламентів;
   в) аналіз ринкової стратегії;
   г) розширення клієнтської бази.

9. **Основним завданням ISO 27001 є:**
   а) забезпечення кібербезпеки підприємства;
   б) управління ризиками;
   в) забезпечення безперервності бізнесу;
   г) управління ланцюгами постачання.

10. **Що таке регуляторні ризики?**
    а) ризики, пов’язані з втратами через конкуренцію;
    б) ризики, що виникають через зміни в законодавстві;
    в) ризики втрати інформаційних ресурсів;
    г) ризики, пов’язані з низькою якістю продукції.

11. **Яке з наведених правопорушень може призвести до репутаційних втрат для підприємства?**
    а) недотримання екологічного законодавства;
    б) затримка постачання продукції;
    в) порушення умов контракту;
    г) збільшення витрат на виробництво.

12. **Що є ключовим завданням міжнародного стандарту ISO 22301?**
    а) управління інформаційними ресурсами;
    б) забезпечення безперервності бізнесу;
    в) захист інтелектуальної власності;
    г) управління фінансовими потоками.

13. **До яких основних сфер належать правові ризики підприємств?**
    а) фінансова, кадрова, виробнича;
    б) податкова, контрактна, інтелектуальна власність;
    в) інформаційна, екологічна, репутаційна;
    г) маркетингова, логістична, стратегічна.

14. **Що таке внутрішній регламент підприємства?**
    а) стратегія розвитку бізнесу;
    б) система внутрішніх правил, що відповідають законодавчим вимогам;
    в) метод управління кадрами;
    г) фінансовий звіт.

15. **Що є основним наслідком недотримання екологічного законодавства?**
    а) втрати продукції;
    б) штрафи та репутаційні втрати;
    в) скорочення персоналу;
    г) збільшення операційних витрат.

16. **Що таке юридичний аудит?**
    а) перевірка фінансової звітності;
    б) оцінка відповідності діяльності підприємства законодавству;
    в) аналіз маркетингових кампаній;
    г) моніторинг репутації підприємства.

17. **Основна мета Закону України "Про охоронну діяльність":**
    а) забезпечення безпеки особистих даних;

б) регулювання діяльності охоронних структур;
в) управління конфіденційною інформацією;
г) підтримка правової системи.

18. **Як підприємства можуть відслідковувати зміни у законодавстві?**
а) через впровадження автоматизованих систем моніторингу;
б) шляхом регулярних тренінгів для персоналу;
в) за допомогою фінансового аудиту;
г) через проведення ринкових досліджень.

Практичні завдання:

Завдання 1. Аналіз законодавчих ризиків
Використовуючи відкриті джерела, виконайте такі дії:
1. Ознайомтеся зі змінами в податковому законодавстві України за останній рік.
2. Визначте можливі ризики для підприємства, пов'язані зі змінами.
3. Розробіть заходи, які дозволять зменшити вплив цих ризиків на підприємство.

Завдання 2. Розробка внутрішніх політик відповідності
1. Оберіть сферу діяльності підприємства (наприклад, торгівля, виробництво або IT).
2. Розробіть приклад внутрішньої політики, яка відповідає вимогам законодавства (наприклад, політика захисту персональних даних або дотримання трудового законодавства).
3. Визначте механізми контролю за виконанням цієї політики.

Завдання 3. Побудова мапи правових ризиків
1. Складіть перелік правових ризиків для підприємства у вибраній галузі.
2. Оцініть кожен ризик за ймовірністю його виникнення (низька, середня, висока) та можливими наслідками (незначні, середні, критичні).
3. Побудуйте мапу ризиків у форматі матриці та запропонуйте заходи для управління найбільш серйозними ризиками.

Завдання 4. Дотримання вимог ISO 27001
1. Ознайомтеся з вимогами стандарту ISO 27001 щодо інформаційної безпеки.
2. Визначте три основні кроки для впровадження системи управління інформаційною безпекою на підприємстві.
3. Запропонуйте методи оцінки ефективності впроваджених заходів.

Завдання 5. Впровадження системи моніторингу законодавства
1. Розробіть план впровадження автоматизованої системи моніторингу змін у законодавстві для підприємства.
2. Визначте джерела, які потрібно моніторити (державні реєстри, інформаційні портали тощо).
3. Опишіть переваги автоматизації моніторингу порівняно з ручним процесом.

Завдання 6. Контрактний аналіз

1. Ознайомтеся з типовим контрактом на постачання товарів або послуг.
2. Визначте потенційні ризики, пов’язані з умовами контракту (наприклад, штрафи за порушення строків постачання).
3. Запропонуйте зміни до умов договору, які можуть зменшити ці ризики.

Завдання 7. Визначення впливу недотримання законодавства

1. Знайдіть приклад реального підприємства, яке зазнало наслідків через порушення законодавства.
2. Проаналізуйте причини порушення та наслідки для компанії (фінансові, репутаційні тощо).
3. Розробіть рекомендації, які могли б допомогти уникнути подібних ситуацій у майбутньому.

Завдання 8. Оцінка відповідності підприємства екологічному законодавству

1. Визначте основні вимоги екологічного законодавства до підприємства у вибраній галузі.
2. Проведіть оцінку відповідності діяльності підприємства цим вимогам.
3. Запропонуйте заходи для усунення можливих недоліків.

Завдання 9. Розробка тренінгу для працівників

1. Розробіть програму тренінгу для працівників щодо дотримання норм трудового законодавства.
2. Включіть у програму ключові теми (наприклад, права та обов'язки працівників і роботодавців).
3. Складіть перелік очікуваних результатів від проведення тренінгу.

Завдання 10. Розробка політики корпоративної відповідальності

1. Визначте основні принципи корпоративної відповідальності підприємства у сфері дотримання законодавства.
2. Розробіть політику корпоративної відповідальності, яка включає механізми управління ризиками.
3. Опишіть, як ця політика вплине на репутацію підприємства та його економічну безпеку.

ТЕМА 3. ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА В УМОВАХ ВОЄННОГО СТАНУ

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

3.1 Сутність економічної безпеки у воєнний час.
3.2 Основні загрози для підприємств під час воєнного стану.
3.3 Механізми адаптації підприємств до умов воєнного стану.
3.4 Державне регулювання та підтримка підприємств у період воєнного стану.
3.5 Приклади успішних адаптацій бізнесу до умов війни.

3.1 Сутність економічної безпеки у воєнний час

Економічна безпека підприємства у воєнний час є основою його виживання, адаптації та розвитку в умовах військових конфліктів. Цей стан характеризується необхідністю оперативного реагування на нові загрози та виклики, забезпечення стабільності функціонування бізнесу та збереження ключових ресурсів.

Особливості економічної безпеки у воєнний час

1. **Високий рівень непередбачуваності:**
   - постійні зміни в економічній та політичній ситуації;
   - загроза фізичного знищення матеріальних активів підприємства.
2. **Динаміка зовнішніх та внутрішніх ризиків:**
   - зовнішні загрози: військові дії, блокада транспортних маршрутів, економічні санкції;
   - внутрішні загрози: відтік кваліфікованих кадрів, фінансові труднощі через втрату ринків збуту.
3. **Потреба в адаптації бізнес-процесів:**
   - перехід до кризового менеджменту;
   - диверсифікація постачань та збуту продукції.

Ключові компоненти економічної безпеки у воєнний час

1. **Фінансова безпека:**
   - забезпечення ліквідності та зниження залежності від зовнішніх кредиторів;
   - контроль за витратами та пошук нових джерел фінансування.
2. **Кадрова безпека:**
   - збереження ключового персоналу через мотиваційні програми;
   - забезпечення безпеки працівників у зонах бойових дій.
3. **Інформаційна безпека:**
   - захист конфіденційних даних від кібератак;
   - встановлення резервних каналів комунікації.
4. **Логістична безпека:**
   - відновлення та перебудова ланцюгів постачання;
   - пошук альтернативних транспортних маршрутів.

Основні загрози економічній безпеці у воєнний час

1. **Фізичне знищення активів:**
   - руйнування виробничих потужностей через бойові дії;
   - втрата складів та логістичних центрів.
2. **Збої у фінансовій системі:**
   - заборона на операції з певними контрагентами;
   - нестабільність національної валюти.
3. **Соціальні та кадрові виклики:**
   - вимушена міграція працівників;
   - зниження продуктивності через психологічний стрес.

Зміна рівня загроз (до та під час воєнного стану) відображено на графіку (рис. 3.1)

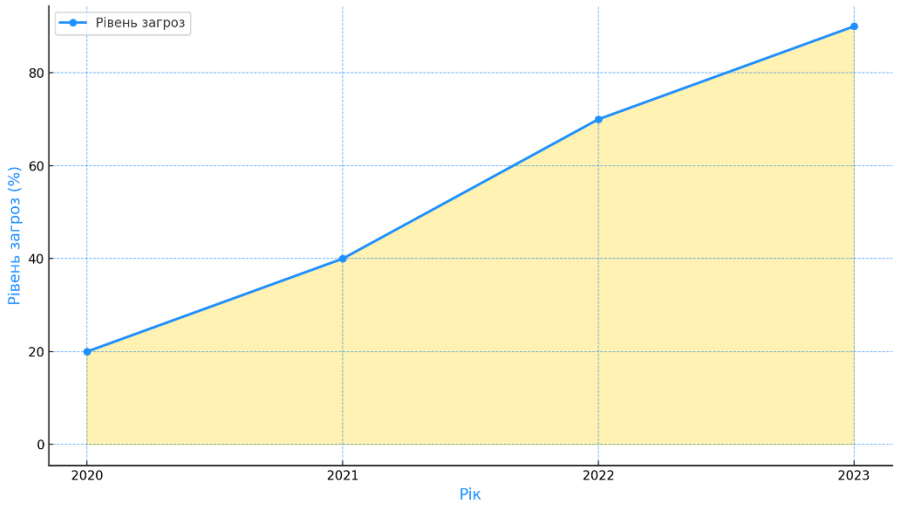

Рисунок 3.1 – Динаміка впливу загроз на підприємство (до та під час воєнного стану)

3.2 Основні загрози для підприємств під час воєнного стану

У період воєнного стану підприємства стикаються з багатогранними загрозами, які суттєво впливають на їхню діяльність. Розуміння природи цих загроз є критично важливим для забезпечення економічної безпеки, адаптації бізнесу до нових умов та розробки ефективних механізмів захисту.

Класифікація загроз

1. **Фізичні загрози:**
   - руйнування інфраструктури (виробничі потужності, склади, транспортні вузли);
   - блокування або знищення логістичних маршрутів;
   - захоплення майна підприємства.
2. **Фінансові загрози:**
   - нестабільність національної валюти та інфляція;
   - обмеження доступу до банківських послуг у регіонах бойових дій;
   - втрата платоспроможності через зменшення доходів або втрату ринків.

3. **Соціальні та кадрові загрози:**
   - втрата ключових співробітників через мобілізацію, міграцію або втрату зв’язку;
   - психологічний стрес персоналу, що знижує продуктивність;
   - дефіцит кваліфікованих кадрів у певних регіонах.
4. **Інформаційні загрози:**
   - зростання кількості кібератак на підприємства;
   - викрадення конфіденційної інформації;
   - поширення дезінформації, що шкодить репутації.
5. **Ринкові загрози:**
   - втрата доступу до традиційних ринків збуту;
   - зростання конкуренції за рахунок адаптації міжнародних компаній до нових умов;
   - падіння купівельної спроможності споживачів.

Вплив загроз на діяльність підприємств

1. **Зниження виробничих потужностей:**
   - прямий вплив бойових дій на підприємства, розташовані у зонах конфлікту;
   - перебої у постачанні сировини.
2. **Фінансова нестабільність:**
   - зростання боргового навантаження через необхідність залучення кредитів;
   - затримка платежів від клієнтів.
3. **Порушення логістичних ланцюгів:**
   - неможливість доставити продукцію до кінцевого споживача;
   - підвищення транспортних витрат через використання обхідних маршрутів.

Заходи протидії загрозам

1. **Фізичний захист активів:**
   - Перенесення критичних виробничих потужностей у безпечні регіони.
   - Використання послуг охоронних компаній для захисту майна.
2. **Фінансова адаптація:**
   - Залучення міжнародної допомоги та грантів.
   - Оптимізація витрат та скорочення необов'язкових витрат.
3. **Управління кадровими ресурсами:**
   - Впровадження програм дистанційної роботи.
   - Підтримка персоналу через психологічну допомогу та фінансові бонуси.
4. **Інформаційна безпека:**
   - Встановлення сучасних систем кіберзахисту.
   - Підвищення обізнаності працівників щодо кіберзагроз.

Вплив воєнних ризиків на підприємства

Воєнні ризики мають комплексний характер і впливають на всі аспекти діяльності підприємства: фінансовий стан, виробничі потужності, кадровий склад, ринкову позицію та інформаційну безпеку. Їхній вплив може бути як прямим (руйнування інфраструктури), так і опосередкованим (падіння попиту через зниження купівельної спроможності).

Ключові аспекти впливу воєнних ризиків

1. **Фізичний вплив**
   - руйнування виробничих потужностей, складів, офісів та іншої інфраструктури внаслідок бойових дій;
   - втрата або захоплення майна;
   - обмеження доступу до об’єктів через небезпеку в зоні бойових дій.
2. **Фінансовий вплив**
   - зниження доходів. Втрата ринків збуту через зупинку діяльності партнерів або споживачів;
   - зростання витрат. Підвищення транспортних витрат, витрат на охорону або релокацію бізнесу;
   - нестабільність валюти. Інфляція та девальвація, що впливають на вартість матеріалів і послуг.
3. **Кадровий вплив**
   - мобілізація співробітників, що призводить до втрати кваліфікованих кадрів;
   - вимушена міграція працівників та їхніх родин у безпечні регіони чи за кордон;
   - психологічний стрес, який знижує продуктивність та мотивацію персоналу.
4. **Ринковий вплив**
   - падіння купівельної спроможності споживачів через економічну кризу;
   - втрата конкурентних позицій: Здатність інших гравців швидше адаптуватися до умов або використовувати нові ринки;
   - перебої в постачанні: Неможливість доставити продукцію кінцевому споживачу через порушення логістичних ланцюгів.
5. **Інформаційний вплив**
   - збільшення кількості кібератак, спрямованих на викрадення або знищення критично важливих даних;
   - дезінформація, яка може шкодити репутації підприємства або сприяти паніці серед працівників та клієнтів.

Наслідки воєнних ризиків для підприємств

1. **Зниження фінансової стійкості,** оскільки підприємства можуть втратити частину капіталу через фінансові збитки та непередбачувані витрати.
2. **Падіння продуктивності** (виробництво знижується через нестачу сировини, енергоносіїв, працівників та зруйновану інфраструктуру).
3. **Ризик банкрутства** (якщо підприємство не зможе адаптуватися до умов, воно ризикує втратити здатність виконувати фінансові зобов'язання).
4. **Втрата конкурентних позицій** (компанії, які не встигають адаптуватися до нових реалій, поступаються конкурентам, які можуть швидше реагувати на зміни).
5. **Загроза довгостроковому розвитку** (навіть після завершення війни підприємства стикаються з проблемами відновлення та повернення на ринки).

Можливі дії для зменшення впливу

1. **Стратегічне планування** (оцінка ризиків і створення кризових планів для різних сценаріїв).

2. **Диверсифікація** (зміна постачальників, перенесення виробництва до безпечних регіонів).
3. **Фінансова адаптація** (пошук нових джерел фінансування, наприклад, грантів чи міжнародної допомоги).
4. **Підвищення інформаційної безпеки** (встановлення сучасних систем кіберзахисту та навчання працівників основам захисту даних).
5. **Підтримка персоналу** (впровадження програм підтримки, таких як фінансові бонуси, психологічна допомога чи гнучкий графік роботи).

3.3 Механізми адаптації підприємств до умов воєнного стану.

Успішні адаптації бізнесу під час воєн

Бізнеси, які діють у період воєн, стикаються з винятковими викликами, включаючи фізичні руйнування, перебої в ланцюгах постачання, фінансову нестабільність і втрату кадрів. Проте історія та сучасний досвід свідчать про те, що компанії можуть адаптуватися до умов війни і навіть процвітати завдяки стійкості, інноваціям та стратегічному плануванню. Ось приклади успішних адаптацій бізнесу:

1. **Релокація виробництва**
   - **Приклад**: під час Другої світової війни багато заводів у Європі та Азії перенесли свої операції у безпечніші регіони. Наприклад, деякі американські компанії перемістили виробництво до сільських регіонів.
   - **Адаптація**: перенесення операцій у безпечні зони дозволило уникнути руйнувань і забезпечити безперервність виробництва.
2. **Диверсифікація продуктів та послуг**
   - **Приклад**: Coca-Cola під час Другої світової війни організувала мобільні виробничі лінії, щоб постачати свою продукцію солдатам за символічною ціною.
   - **Адаптація**: це не лише підтримало бойовий дух, але й зміцнило лояльність до бренду, розширивши його впізнаваність у світі.
3. **Орієнтація на воєнні потреби**
   - **Приклад**: автовиробники, такі як Ford і General Motors, перепрофілювали свої заводи для виробництва військової техніки, включаючи танки та літаки.
   - **Адаптація**: укладання контрактів із державними установами забезпечило фінансову стабільність і нові можливості для співпраці.
4. **Альтернативні ланцюги постачання**
   - **Приклад**: логістичні компанії під час війни в Україні розробляли нові маршрути доставки, уникаючи небезпечних регіонів.
   - **Адаптація**: диверсифікація шляхів постачання гарантувала безперервний потік товарів навіть у складних умовах.
5. **Цифрова трансформація**
   - **Приклад**: українські IT-компанії під час війни швидко перейшли на віддалений формат роботи, використовуючи хмарні технології для забезпечення безпеки даних.

- **Адаптація**: використання сучасних технологій допомогло зберегти ефективність роботи та виконувати проєкти для міжнародних клієнтів.

6. **Фінансова стійкість**
   - **Приклад**: підприємства на Близькому Сході під час конфліктів розширювали свою діяльність у стабільні країни, щоб диверсифікувати джерела доходів.
   - **Адаптація**: залучення міжнародної фінансової допомоги та відкриття нових ринків дозволило мінімізувати ризики.
7. **Залучення робочої сили**
   - **Приклад**: під час Першої світової війни жінки масово замінили чоловіків на виробництвах, що дозволило зберегти продуктивність економіки.
   - **Адаптація**: розширення доступу до робочої сили за рахунок залучення нових груп населення підтримало стабільність бізнесу.
8. **Підтримка громад**
   - **Приклад**: компанії, як-от Unilever, під час криз забезпечували населення необхідними товарами, такими як мило чи засоби гігієни.
   - **Адаптація**: такі дії покращували репутацію компаній і створювали довгострокові зв'язки із клієнтами.
9. **Інновації у кризовий час**
   - **Приклад**: підприємці в Сирії під час війни створювали сонячні системи для іригації, вирішуючи проблему нестачі електроенергії.
   - **Адаптація**: інновації дозволяли вирішувати локальні проблеми та відкривати нові ринкові можливості.
10. **Співпраця з урядами та міжнародними організаціями**
    - **Приклад**: українські компанії співпрацюють із державними структурами та міжнародними організаціями для відновлення інфраструктури та підтримки бізнесу.
    - **Адаптація**: таке партнерство забезпечувало стабільність і сприяло ефективності спільних зусиль.

Спільні риси успішних адаптацій:

1. **Гнучкість і адаптивність** – швидке реагування на змінювані обставини.
2. **Довгострокове планування** – розробка стратегій для виживання та розвитку.
3. **Оптимізація ресурсів** – ефективне використання обмежених ресурсів.
4. **Інвестиції у безпеку** – захист активів, даних та персоналу.
5. **Соціальна відповідальність** – підтримка громад та партнерів.

Воєнні виклики є серйозним випробуванням для бізнесу, але історія доводить, що завдяки адаптації, інноваціям та стратегічному підходу підприємства можуть зберегти стійкість і навіть зміцнити свої позиції. Успішне управління ризиками стає ключовим фактором для виживання та довгострокового процвітання.

3.4 Державне регулювання та підтримка підприємств у період воєнного стану.

Державне регулювання та підтримка є критично важливими факторами, які сприяють забезпеченню економічної безпеки підприємств під час воєнного стану. Уряди створюють нормативно-правову базу, впроваджують фінансові, організаційні та інформаційні механізми підтримки, що дозволяють бізнесу адаптуватися до складних умов.

Оскільки захищеність суб'єкта господарювання є компонентом системи національної безпеки нашої держави, то відповідно держава найістотнішим чином впливає на створення системи економічної захищеності промислового підприємства. Застосовуючи пряме чи опосередковане втручання, саме держава формує та координує необхідне економічне поле функціонування суб'єкта господарюванн. Координування державою виробничої діяльності суб'єкта господарювання, як правило, забезпечується в кількох напрямах (рис. 3.1).

Рисунок 3.1 – Основні напрями державного регулювання

Варто брати до уваги те, що іноді запити суб'єкта господарювання не тотожні інтересам держави, у зв'язку з цим економічну захищеність можна розглядати як їх спільне мірило. Тому обов'язково потрібно дотримуватися правила: формуючи фундамент для

розвитку державної економіки, не можна шкодити чи завдавати збитків запитам промислового підприємства.

Водночас варто наголосити на тому, що важливе значення для суб'єкта господарювання має державна політика в сфері оподаткування та загалом вся податкова система країни. У зв'язку з цим важливою запорукою захищеності суб'єкта господарювання виступає усталеність державної політики в галузі оподаткування. Наступною передумовою захищеності промислового підприємства варто вважати виваженість державного втручання в економіку країни. У випадку, коли державне втручання в економіку країни є мінімальним, маємо справу з традиційною капіталістичною моделлю, натомість, у разі високого рівня державного регулювання доцільно говорити про загальноприйняту державну модель соціалізму, що мала місце СРСР впродовж тривалого часу.

Загальновідомо, що державне регулювання економіки певною мірою простежується свіже у всіх державах з економікою ринкового типу. Вплив держави має на меті забезпечити врівноваженість економічних запитів у самій державі. Нагальна потреба ролі держави у координуванні діяльності суб'єктів господарювання пов'язана, насамперед, з недостатнім рівнем співпраці між промисловими підприємствами.

Процес координування державою виробничої діяльності промислових підприємств може мати вигляд безпосереднього та опосередкованого втручання. Опосередковане втручання покликане створити ефективну систему мотивування, забезпечити сприятливі ринкові умови для суб'єктів підприємницької діяльності (ціноутворення, кредитно-грошові відносини та планування держзамовлення), а безпосереднє державне втручання включає в себе формування на державному рівні нормативно-правового поля, комплексу заходів, покликаних прямо регулювати виробничу діяльність підприємств у ринкових умовах (закони, укази, положення та ін. нормативно-законодавчі акти). Координування підприємницької діяльності на державному рівні не залежить від форми власності суб'єкта господарювання на засоби виробництва і забезпечується через реалізацію комплексу правових і соціально-економічних заходів.

Через певну неузгодженість інтересів держави та запитів конкретного суб'єкта господарювання або групи промислових підприємств виникає ситуація, коли вплив держави на підприємницьку діяльність може бути сприятливим або несприятливим для економічної захищеності суб'єктів господарювання. Найбільш помітним та несприятливим є державний вплив на економічну захищеність суб'єктів господарювання приватного сектора, адже держава сама по собі не бере на себе відповідальності за показники їх виробничої діяльності (табл. 3.1).

Таблиця 3.1 – Сприятливий вплив регулювання державою підприємницької діяльності в контексті економічної захищеності суб'єкта господарювання

Форми державного впливу	Наслідки державного впливу	Результат державного регулювання з точки зору впливу на економічну захищеність суб'єкта господарювання
1	2	3
Запровадження різних форм власності	Виникнення приватного сектора в економіці	Можливості для прояву приватної ініціативи, посилення зацікавленості в результатах роботи суб'єкта господарювання

Продовження таблиці 3.1

1	2	3
Формування ринку фінансової сфери	Виникнення мережі фінансових посередників	Розширення потенційних джерел інвестування
Координування та обмеження рівня монополізації	Створення оптимальних умов для здорової конкуренції	Зменшення загрози з боку монополій. Попередження виникнення або ліквідація ринкових утворень чи поводження ринкових агентів, які мають небажаний характер. Можливість надання підтримки одним підгрупам ринкових агентів за допомогою інших
Звуження імпортування продукції для захисту інтересів вітчизняного виробника	Створення сприятливих умов для реалізації продукції вітчизняних товаровиробників	Наповненість ринку
Гарантування державного забезпечення для залучення зовнішніх (в т.ч. і іноземних) інвестицій	Збільшення обсягів залучених іноземних інвестицій	Збільшення числа втілених інвестиційних програм, покращення організаційно-технічного стану виробництва та підвищення конкурентних переваг товарної продукції, можливість виходу суб'єктів господарювання на зовнішні ринки

Разом з тим, зміст різних форм втручання держави не узгоджується, а іноді навіть суперечить інтересам суб'єкта господарювання, в результаті чого чинить несприятливо позначається на економічній безпеці підприємства (табл. 3.2).

Таблиця 3.2 – Несприятливий вплив координування державою підприємницької діяльності в контексті економічної захищеності суб'єкта господарювання

Сфера впливу	**Несприятливий вплив**	**Захисна реакція суб'єктів господарювання**	**Вплив державного втручання на економічну захищеність суб'єкта господарювання**
1	2	3	4
Податкова система	Завищені податкові ставки Відсутність чіткої та прозорої системи пільгового оподаткування	Втрата стимулу до збільшення прибутку. Неврахування частини прибутку	Зменшення обсягів виробництва або його заморожування. Високі витрати на забезпечення виробничої діяльності. Повна відсутність власних ресурсів для інвестування. Недостатній організаційний та техніко-технологічний стан виробництва. Низька конкурентоспроможність власної продукції на зовнішніх ринках

Продовження таблиці 3.2

1	2	3	4
Інноваційна система	Відсутність субсидій і дотацій суб'єктам господарювання державної форми власності	Нехтування технічними та управлінськими новаціями	Недостатній організаційний та техніко-технологічний стан виробництва. Високий рівень енергозатратності виробництва. Низький рівень продуктивності праці. Непродуктивна система управління
Інвестиційна система	Несуттєві державні гарантії іноземним інвесторам. Відсутність сприятливого інвестиційного середовища	Згортання співпраці з іноземними партнерами. Виведення капіталу за межі країни	Відсутність умов для продуктивної співпраці з іноземними партнерами. Гальмування розвитку
Інфраструктура суб'єкта господарювання	Жорстокі рамки діяльності	Відмова від користування послугами інфраструктури суб'єкта господарювання	Збільшення витрат за низького рівня якості робіт, які виконуються самостійно. Відсутність додаткового інвестування у зв'язку з несформованістю фондового ринку

В цілому нормативно-правове поле регулювання діяльності суб'єкта господарювання – це багаторівневе ієрархічне утворення на базі Конституції України, у ст. 17 якої наголошується, що формування економічної захищеності належить до пріоритетних завдань нашої держави та є справою всього народу, адже саме держава, згідно зі статтями 13 і 14 Конституції України виступає гарантом економічної захищеності підприємств, нагальні питання реформування якої, як запоруки суспільно-політичних і соціально-економічних зрушень, порушуються у щорічних зверненнях Президента до ВР України та низці інших законодавчих актів.

Вплив державної підтримки на ЕБП:

1. **Підвищення стійкості бізнесу** (фінансова допомога дозволяє підприємствам подолати тимчасові труднощі).
2. **Збереження робочих місць** (релокація та підтримка підприємств сприяють збереженню кадрів).
3. **Розширення ринкових можливостей** (допомога у виході на міжнародні ринки створює нові перспективи для бізнесу).
4. **Створення сприятливого бізнес-середовища** (спрощення регуляторних процедур та зменшення бюрократії стимулюють розвиток підприємництва).

3.5 Приклади успішних адаптацій бізнесу до умов війни

Під час війни українські підприємства зіткнулися з безпрецедентними викликами, які вимагали швидкої та ефективної адаптації. Незважаючи на складні умови, багато компаній змогли не лише вижити, але й продемонструвати стійкість та інноваційність.

1. **Релокація та відновлення виробництва**
   ПрАТ "Оболонь": Після пошкодження заводу в Київській області компанія перенесла частину виробництва до інших регіонів, що дозволило зберегти робочі місця та продовжити випуск продукції.
2. **Диверсифікація діяльності**
   ТОВ "Розетка": Інтернет-ритейлер розширив асортимент товарів, включивши продукти першої необхідності, а також організував доставку гуманітарної допомоги в постраждалі регіони.
   АТ "Укрзалізниця": Окрім основної діяльності, компанія почала надавати послуги з евакуації населення та транспортування гуманітарних вантажів.
3. **Соціальна відповідальність та підтримка**
   Група компаній "ДТЕК": З початку повномасштабного вторгнення компанія спрямувала понад 1,1 млрд грн на підтримку Збройних Сил України та гуманітарні цілі, включаючи постачання палива, медикаментів та обладнання.
   АТ "Миронівський хлібопродукт" (МХП): Компанія активно надавала гуманітарну допомогу, забезпечуючи продуктами харчування населення та військових у зонах бойових дій.
4. **Інновації та цифровізація**
   ТОВ "Нова Пошта": Впровадила цифрові сервіси для відстеження посилок та безконтактної доставки, що підвищило безпеку та зручність для клієнтів.
   АТ "Ощадбанк": Розширив спектр онлайн-послуг, дозволяючи клієнтам здійснювати більшість операцій дистанційно, що стало критично важливим під час воєнного стану.
5. **Підтримка співробітників та громад**
   ТОВ "SoftServe": Організувала евакуацію працівників із небезпечних регіонів, надаючи їм житло та підтримку в нових місцях проживання.
   АТ "Київстар": Забезпечив безкоштовний зв'язок для абонентів у зоні бойових дій та підтримував роботу мережі в складних умовах.

Ці приклади демонструють, як український бізнес здатен швидко адаптуватися до екстремальних умов, зберігаючи економічну стабільність та підтримуючи суспільство. Вони служать натхненням для інших підприємств, показуючи, що навіть у найскладніші часи можливо знайти шляхи для розвитку та процвітання.

Перелік питань:

1. Що таке економічна безпека підприємства, і чому вона набуває особливого значення під час воєнного стану?
2. Які основні загрози виникають для підприємств у період воєнного стану?
3. Як впливають фізичні ризики на економічну безпеку підприємства?
4. Які фінансові загрози постають перед підприємствами у воєнний час?
5. Як кадрові ризики впливають на діяльність підприємств у період військових дій?
6. У чому полягає небезпека інформаційних ризиків для підприємств під час війни?
7. Як війна впливає на логістичні ланцюги підприємств?
8. Які механізми адаптації підприємств є найбільш ефективними у воєнних умовах?
9. Що включає у себе процес релокації бізнесу? Які основні етапи цього процесу?
10. Які кроки повинно зробити підприємство для забезпечення фінансової стійкості під час воєнного стану?
11. Як державне регулювання може підтримати підприємства у період військових конфліктів?
12. У чому полягає роль податкових пільг у підтримці бізнесу у воєнний час?
13. Як державні програми релокації сприяють збереженню виробничих потужностей підприємств?
14. Які види державної фінансової допомоги існують для підтримки бізнесу під час війни?
15. Як міжнародна допомога сприяє збереженню економічної безпеки українських підприємств?
16. Чому соціальна відповідальність бізнесу є важливим аспектом під час воєнного стану?
17. Як підприємства можуть захистити свою інформацію від кіберзагроз у період війни?
18. Які приклади успішних адаптацій бізнесу до умов воєнного стану ви знаєте?
19. Як компанії можуть використовувати інновації для підвищення своєї економічної безпеки під час війни?
20. У чому полягає значення кризового управління для забезпечення безперервності бізнесу в умовах війни?

Тести:

1. **Яка основна мета економічної безпеки підприємства у воєнний час?**
   а) забезпечення максимізації прибутку;
   б) мінімізація витрат на інновації;
   в) збереження стійкості та адаптації до ризиків;
   г) оптимізація податкового навантаження.

2. **Що є ключовим фактором для успішної релокації підприємства?**
   а) зниження витрат на персонал;
   б) доступ до нових ринків збуту;
   в) вибір безпечного регіону з доступною інфраструктурою;
   г) мінімізація витрат на оренду.

3. **Які заходи сприяють захисту інформаційної безпеки підприємства?**
   а) збільшення кількості робочих місць у зоні ризику;
   б) використання хмарних сервісів для резервування даних;
   в) зменшення кількості співробітників;
   г) обмеження доступу до виробничих потужностей.

4. **Який основний ризик виникає у підприємства під час воєнного стану?**
   а) збільшення маркетингових витрат;
   б) переривання ланцюгів постачання;
   в) розширення фінансових можливостей;
   г) зниження конкуренції на ринку.
5. **Який механізм адаптації підприємства є найбільш ефективним у воєнних умовах?**
   а) оптимізація маркетингових витрат;
   б) інноваційні стратегії автоматизації виробництва;
   в) збільшення кількості зовнішніх підрядників;
   г) зменшення кількості активів.

6. **Що є ключовим аспектом державної підтримки бізнесу у воєнний час?**
   а) забезпечення стабільного доступу до фінансування;
   б) впровадження обов'язкової релокації;
   в) скорочення виробничих потужностей;
   г) заборона на нові інвестиції.

7. **Який інструмент забезпечує безперервність бізнес-процесів у воєнних умовах?**
   а) розробка нових маркетингових кампаній;
   б) впровадження кризового менеджменту;
   в) пошук додаткових співробітників;
   г) скорочення витрат на логістику.

8. **Що є основним завданням соціальної відповідальності бізнесу під час війни?**
   а) збільшення кількості продажів;
   б) забезпечення підтримки громад і працівників;
   в) оптимізація витрат на рекламу;
   г) розширення логістичних потужностей.

9. **Який із наведених механізмів є прикладом фінансової адаптації?**
   а) підвищення цін на продукцію;
   б) отримання грантів і пільгових кредитів;
   в) розширення асортименту товарів;
   г) зменшення кількості співробітників;

10. **Що є основною метою кризового управління у воєнний час?**
    а) максимізація прибутку;

б) забезпечення стійкості та безперервності бізнесу;
в) скорочення логістичних витрат;
г) уникнення нових інвестицій.

Практичні завдання:

Завдання 1. Аналіз ризиків підприємства під час воєнного стану
Мета: Оцінити ризики, які виникають для підприємства під час воєнного стану, та запропонувати заходи для їх мінімізації.

1. Виберіть реальне підприємство або змоделюйте умовне.
2. Складіть перелік основних ризиків, з якими воно може зіткнутися (фізичні, фінансові, кадрові, інформаційні).
3. Запропонуйте мінімум три заходи для кожного ризику, які можуть знизити їхній вплив.
4. Представте результати у вигляді таблиці:

Ризик	**Опис**	**Заходи мінімізації**
Фінансова нестабільність	Зменшення прибутків через втрату ринків	1. Диверсифікація ринків

Завдання 2. Розробка плану релокації підприємства
Мета: Розробити детальний план перенесення виробничих потужностей підприємства до безпечного регіону.

1. Оберіть регіон для релокації (умовний або реальний). При цьому врахуйте ключові фактори: наявність інфраструктури, логістичні можливості, доступність робочої сили.
2. Опишіть кроки реалізації плану.
3. Підготуйте графік релокації з урахуванням часових рамок.

Завдання 3. Оцінка ефективності державної підтримки
Мета: Проаналізувати вплив інструментів державної підтримки на економічну безпеку підприємства.

1. Оберіть реальну програму державної підтримки (наприклад, пільгові кредити).
2. Проаналізуйте, як ця програма впливає на фінансову стабільність підприємства, на збереження робочих місць та на можливість виходу на нові ринки.
3. Представте висновки у вигляді SWOT-аналізу.

Завдання 4. Розробка кризового плану
Мета: Створити план дій для підприємства на випадок ескалації загроз.

1. Виберіть підприємство у будь-якій галузі.
2. Опишіть потенційні загрози для його діяльності.
3. Розробіть кризовий план, що включає роль кризового комітету та алгоритм дій для кожної загрози.
4. Запропонуйте спосіб перевірки ефективності плану (наприклад, симуляція кризової ситуації).

Завдання 5. Інформаційна безпека під час війни

Мета: Розробити рекомендації для захисту інформації підприємства у воєнний час.

1. Оцініть основні інформаційні ризики (наприклад, кібератаки, витік даних).
2. Запропонуйте заходи для забезпечення безпеки даних (резервне копіювання, багаторівневий доступ тощо).
3. Опишіть, як підприємство може навчити працівників основам інформаційної безпеки.

Завдання 6. Соціальна відповідальність бізнесу у воєнний час

Мета: Розробити програму соціальної відповідальності для підприємства.

1. Оберіть підприємство (умовне чи реальне).
2. Опишіть програму підтримки громади (гуманітарна допомога, надання робочих місць тощо).
3. Визначте очікувані результати цієї програми.
4. Оформіть результати у форматі презентації для представлення керівництву.

Завдання 7. Аналіз адаптаційних механізмів

Мета: Проаналізувати, які механізми адаптації є найефективнішими у різних галузях.

1. Виберіть три різні галузі (наприклад, виробництво, IT, транспорт).
2. Визначте адаптаційні механізми, які використовуються в цих галузях.
3. Оцініть їхню ефективність за такими критеріями: фінансова стійкість, операційна безперервність, інноваційність.
4. Зробіть висновки у вигляді порівняльної таблиці.

ТЕМА 4. ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ВИКЛИКИ КРИПТОВАЛЮТНОЇ ЕПОХИ

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

4.1 Сутність криптовалют як фінансового інструменту.
4.2 Можливості та загрози використання криптовалют для підприємств.
4.3 Правове регулювання криптовалют.
4.4 Інтеграція криптовалют у бізнес-процеси.
4.5 Ризики криптовалютної діяльності.
4.6 Приклади використання криптовалют у бізнесі.

4.1 Сутність криптовалют як фінансового інструменту

Визначення криптовалют

Криптовалюта – це цифровий або віртуальний актив, який використовує криптографію для забезпечення безпеки транзакцій, створення нових одиниць і контролю над їх обігом. На відміну від традиційних валют, криптовалюти працюють на децентралізованих платформах, зазвичай на основі технології блокчейн. Оданак сучасні тенденції вже тяжіють до того, що крипторинок тяжіє до фондового. Будова криптовалюти подана на рисунку 4.1.

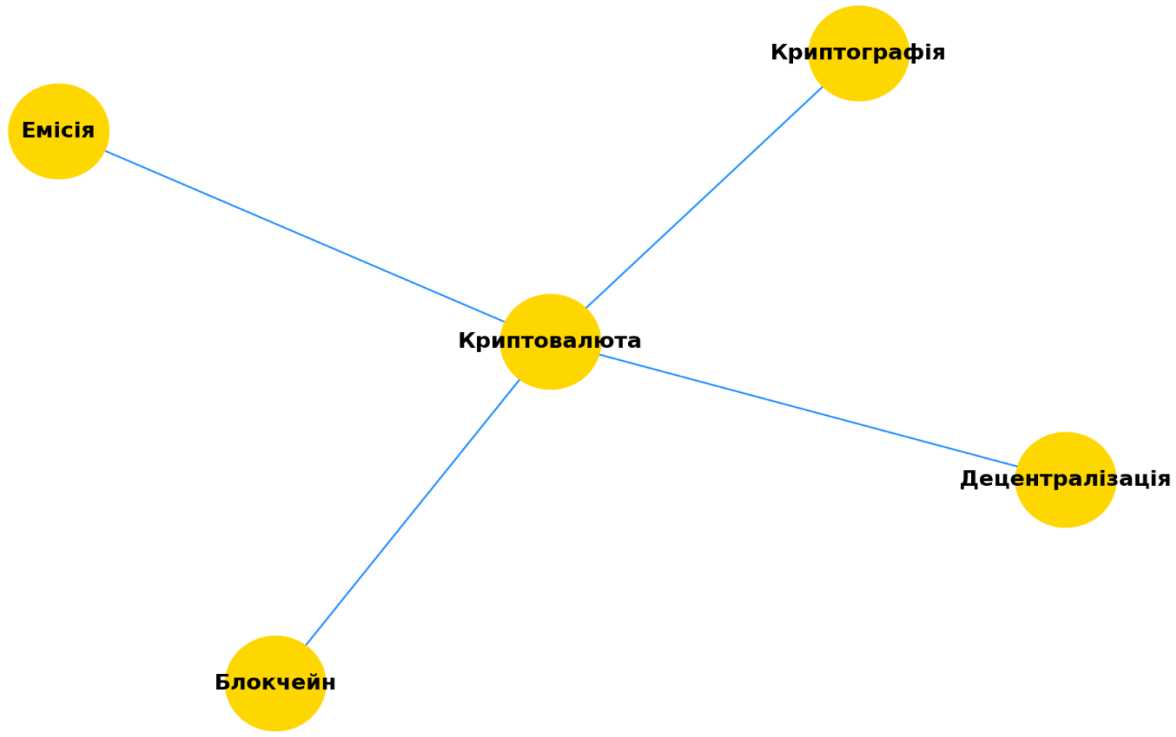

Рисунок 4.1 – Будова криптовалюти

Основні характеристики криптовалют

1. **Децентралізація:**
   - відсутність центрального органу, який контролює випуск чи обіг криптовалюти;
   - транзакції відбуваються через розподілену мережу.
2. **Криптографічний захист:**
   - використання алгоритмів шифрування забезпечує безпеку транзакцій;
   - гарантує анонімність і захищеність даних.
3. **Обмежена емісія** (у більшості криптовалют існує обмеження на кількість монет (наприклад, 21 мільйон для Bitcoin)).
4. **Глобальність:**
   - криптовалюта не залежить від кордонів чи національних валютних систем;
   - транзакції можливі в будь-якій точці світу.
5. **Анонімність** (транзакції не містять особистих даних, що ускладнює їх відстеження).
6. **Висока волатильність** (курси криптовалют змінюються значно швидше, ніж традиційні валюти).

Роль криптовалют у сучасній економіці

1. **Альтернативний платіжний засіб** (використовується для транзакцій без посередників, таких як банки та зменшує комісії за транзакції).
2. **Інструмент інвестування** (багато компаній та приватних осіб розглядають криптовалюти як перспективний актив для довгострокових інвестицій).
3. **Засіб залучення фінансування** (за допомогою ICO (Initial Coin Offering) компанії можуть залучати кошти для реалізації проєктів).
4. **Інновації у фінансових системах** (впровадження блокчейн-технологій для прозорості, безпеки та автоматизації транзакцій).

Однією з найпопулярніших криптовалют є Bitcoin (BTC), рисунок 4.2 показує його тренди та волатильність.

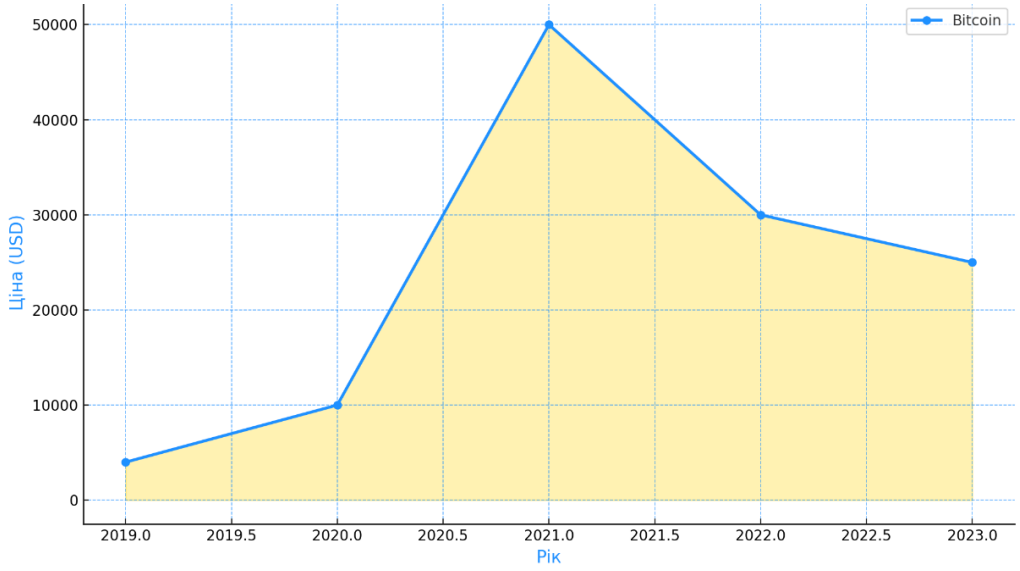

Рисунок 4.2 – Динаміка курсу Bitcoin за останні 5 років

Види криптовалют

1. **Bitcoin (BTC)**
   - перша і найвідоміша криптовалюта, створена у 2009 році.
2. **Ethereum (ETH)**
   - використовується для запуску смарт-контрактів та децентралізованих додатків.
3. **Stablecoins (USDT, USDC)**
   - прив'язані до вартості традиційних валют (наприклад, долара США) для зменшення волатильності.
4. **Altcoins (Litecoin, Ripple, Cardano)**
   - криптовалюти, створені як альтернатива Bitcoin (табл. 4.1).

Таблиця 4.1 – Порівняння Bitcoin, Ethereum та Stablecoins

Криптовалюта	Волатильність	Призначення	Масштабованість
Bitcoin	Висока	Цифрове золото, збереження вартості	Обмежена
Ethereum	Середня	Смарт-контракти, децентралізовані додатки	Вища, ніж Bitcoin
Stablecoins	Низька	Захист від волатильності, стабільність	Висока
Altcoins (Litecoin, Ripple, Cardano)	Середня	Оптимізація транзакцій, інноваційні рішення, альтернатива BTC/ETH	Варіюється (залежно від платформи)

Переваги криптовалют:

1. Зменшення витрат на транзакції.
2. Швидкість міжнародних переказів.
3. Відсутність бюрократії.
4. Можливість роботи у країнах із нестабільною економікою.

Недоліки криптовалют:

1. Висока волатильність.
2. Ризик втрати через хакерські атаки.
3. Використання у незаконних операціях.
4. Недостатнє правове регулювання в багатьох країнах.

Криптовалюти стали інноваційним фінансовим інструментом, який впливає на глобальну економіку. Вони відкривають нові можливості для бізнесу, але водночас створюють серйозні виклики, такі як регулювання, волатильність та безпека. У сучасних умовах кожне підприємство має враховувати ці фактори при інтеграції криптовалют у свою діяльність.

Механізм роботи блокчейну

Блокчейн — це децентралізована, розподілена база даних, яка використовується для запису транзакцій у безпечний і незмінний спосіб. Його механізм базується на кількох ключових елементах, які забезпечують прозорість, безпеку та децентралізацію. Блокчейн знаходить застосування не лише у фінансовій сфері, але й у логістиці, охороні здоров'я, управлінні даними та багатьох інших галузях.

Основні компоненти блокчейну

1. **Блоки:**
   - кожен блок містить набір транзакцій, хеш поточного блоку та хеш попереднього блоку;
   - включає часову мітку, яка фіксує момент створення блоку.
2. **Ланцюг блоків:**
   - блоки зв'язані між собою за допомогою хешів, утворюючи ланцюг;
   - будь-яка зміна у транзакції змінює хеш блоку, порушуючи цілісність ланцюга.
3. **Розподілена мережа:**
   - копії блокчейну зберігаються на всіх вузлах мережі (нодах);
   - всі вузли синхронізовані, що забезпечує децентралізацію.
4. **Криптографія:**
   - транзакції захищені цифровими підписами;
   - використовуються хеш-функції (наприклад, SHA-256) для створення унікальних ідентифікаторів.

Механізм роботи блокчейну

1. **Ініціювання транзакції:**
   - користувач створює транзакцію, наприклад, переказ коштів4
   - транзакція підписується приватним ключем користувача, що забезпечує її автентичність.
2. **Передача транзакції до мережі** (транзакція передається до вузлів (нодів) мережі, які перевіряють її дійсність).
3. **Перевірка транзакції:**
   - вузли перевіряють баланс відправника та цілісність цифрового підпису.
   - якщо транзакція дійсна, вона додається до пулу непідтверджених транзакцій.
4. **Формування блоку:**
   - майнери або валідатори об'єднують непідтверджені транзакції у блок;
   - у процесі майнінгу використовується алгоритм консенсусу (наприклад, Proof of Work, Proof of Stake).
5. **Додавання блоку до ланцюга:**
   - після успішного створення блоку він додається до ланцюга;
   - інформація синхронізується між усіма вузлами мережі.
6. **Підтвердження транзакції:**
   - після додавання блоку транзакція вважається підтвердженою;
   - чим більше блоків створено після цього блоку, тим безпечнішою є транзакція.

Алгоритми консенсусу

1. **Proof of Work (PoW)** (майнери розв'язують складні математичні задачі, щоб додати блок до ланцюга. Використовується, наприклад, у Bitcoin).
2. **Proof of Stake (PoS)** (валідатори обираються залежно від кількості криптовалюти, яку вони тримають. Енергоефективний, використовується в Ethereum 2.0).
3. **Delegated Proof of Stake (DPoS)** (учасники мережі голосують за валідаторів, які створюють блоки. Використовується в EOS).

Переваги блокчейну

1. **Децентралізація** – відсутність центрального органу управління.
2. **Прозорість** – будь-хто може переглядати дані в блокчейні.
3. **Безпека** – хешування та криптографія забезпечують захист даних.
4. **Незмінність** – запис у блокчейні не може бути змінений.

Недоліки блокчейну

1. **Складність масштабування** (більша кількість транзакцій може спричинити затримки).
2. **Високі енергозатрати** (особливо характерно для PoW).
3. **Обмежена інтеграція** (блокчейн ще не повністю інтегрований у традиційні системи).

Основні ризики криптовалют

Криптовалюти, як інноваційний фінансовий інструмент, мають значний потенціал, але також пов'язані з низкою ризиків. Їхній характер залежить від природи криптовалют, їхньої децентралізованості, правового статусу та інших факторів.

1. **Волатильність.** Криптовалюти характеризуються значними коливаннями вартості. Через це може відбутись швидке зростання або падіння ціни, що може призвести до фінансових втрат, а отже інвестори стикаються з труднощами в прогнозуванні. Так, таприклад, вартість Bitcoin у 2021 році сягнула $69,000, але згодом впала до $30,000 у 2022 році.

2. **Відсутність регулювання.** У багатьох країнах криптовалюти залишаються нерегульованими або мають неоднозначний правовий статус, що створює правову невизначеність для компаній та інвесторів, як наслідок високий рівень ризику шахрайства та складність у вирішенні спорів, пов'язаних із криптоактивами.

3. **Кібератаки та безпека.** Тут ризики перш за все полягають у високій ймовірності хакерських атак на біржі, гаманці та платформи, а отже у втраті доступу до гаманця через втрату приватного ключа. Так у 2022 році хакери викрали криптовалют на суму понад $3,8 млрд, згідно з даними Chainalysis.

4. **Використання у незаконних операціях.** Нажаль криптовалюти широко використовуються для фінансування тероризму, відмивання грошей, нелегального продажу товарів у даркнеті. Так на платформах, таких як Silk Road (до її закриття), криптовалюти широко використовувалися для незаконної торгівлі.

5. **Енергоспоживання.** Майнінг криптовалют, особливо Bitcoin, споживає значну кількість енергії, що призводить до екологічного навантаження та збільшення викидів CO_2. Зокрема енергоспоживання мережі Bitcoin у 2021 році перевищувало споживання електроенергії деяких країн, таких як Аргентина.

6. **Шахрайство та фінансові піраміди.** Поява фіктивних проєктів або ICO (Initial Coin Offering), які націлені на обман інвесторів. Схема OneCoin, яка позиціонувала себе як криптовалюта, виявилася шахрайством, що призвело до втрат мільйонів доларів.

7. **Втрата приватного ключа.** Гаманці криптовалют захищені приватними ключами, а отже втрата ключа означає неможливість доступу до активів, без можливості відновлення.

8. **Низька ліквідність.** Деякі криптовалюти мають низьку ліквідність, що ускладнює їхній продаж або обмін, що створює додаткові труднощі для великих інвесторів.

9. **Складність у розумінні.** Багато користувачів досі не розуміють технічних і економічних аспектів криптовалют, що збільшує ймовірність прийняття неправильних рішень.

10. **Технічні ризики.** Перш за все це збої в роботі блокчейн-мережі та вразливості в смарт-контрактах.

Способи мінімізації ризиків

1. **Регулювання**
   запровадження чітких правових норм і регуляторної бази.
2. **Освіта користувачів**
   навчання користувачів основам безпеки.
3. **Диверсифікація**
   інвестування в різні криптовалюти для зниження ризиків.
4. **Використання холодних гаманців**
   зберігання активів у гаманцях, які не підключені до інтернету.

Криптовалюти пропонують значний потенціал, але вимагають обережного та обізнаного підходу. Інвестори та компанії повинні враховувати всі ризики, щоб ефективно використовувати цей фінансовий інструмент.

4.2 Можливості та загрози використання криптовалют для підприємств

Використання криптовалют підприємствами відкриває нові горизонти для розвитку, але водночас створює певні ризики. Розуміння цих аспектів дозволяє підприємствам приймати обґрунтовані рішення щодо інтеграції криптовалют у свою діяльність.

Можливості використання криптовалют

1. **Зменшення витрат на транзакції**, оскільки криптовалюти дозволяють уникати високих банківських комісій за міжнародні платежі, а транзакції здійснюються без посередників, що прискорює процес.
2. **Глобальні платежі**, тому що використання криптовалют дозволяє підприємствам обслуговувати клієнтів з будь-якої точки світу, таким чином відсутність обмежень, пов’язаних із валютним регулюванням.

3. **Залучення нової аудиторії**: прийом криптовалют як оплати може привабити клієнтів, які віддають перевагу цифровим активам.
4. **Інноваційність і престиж**: використання криптовалют свідчить про сучасність підприємства та його готовність до технологічних змін.
5. **Захист від інфляції**: криптовалюти, такі як Bitcoin, можуть використовуватися для збереження капіталу у країнах із нестабільною економікою.
6. **Смарт-контракти**: автоматизація угод завдяки блокчейн-технологіям та підвищення ефективності бізнес-процесів і зниження ризику помилок.

Можливості використання криптовалют для бізнесу подано на рисунку 4.3, де центральним блоком є "Криптовалюти", та відповідні відгалудження – "Зменшення витрат", "Смарт-контракти", "Глобальні платежі", "Захист від інфляції".

Рисунок 4.3 – Можливості використання криптовалют для бізнесу

Також варто звернути увагу на зростання кількості підприємств, що використовують криптовалюти (рис. 4.4)

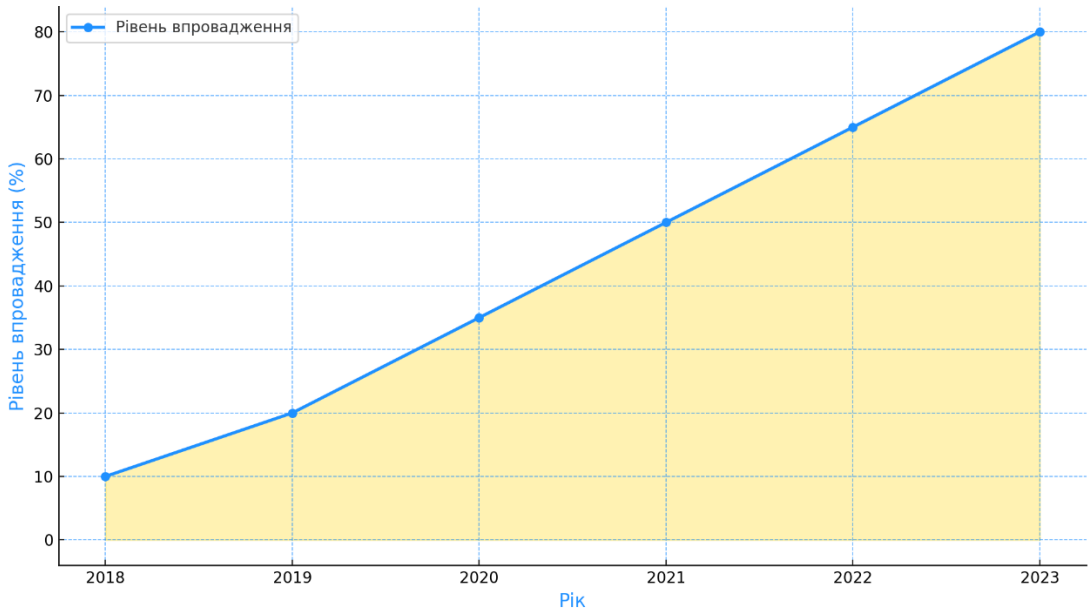

Рисунок 4.4 – Динаміка впровадження криптовалют у бізнес-практиках

Загрози використання криптовалют

1. **Волатильність**, оскільки нізкі коливання курсу можуть призвести до фінансових втрат, а тому важко прогнозувати вартість активів.
2. **Відсутність регулювання**: у багатьох країнах немає чіткої правової бази для роботи з криптовалютами, що ускладнює використання криптоактивів у бухгалтерії та звітності.
3. **Ризик шахрайства**, що виникає через небезпеку співпраці з ненадійними партнерами, які можуть використовувати криптовалюти для незаконної діяльності.
4. **Кібератаки** (хакери можуть викрасти криптовалюту через злам гаманців чи платформ).
5. **Високі енергозатрати**, що особливо актуально для компаній, які займаються майнінгом.
6. **Складність інтеграції** (впровадження криптовалют вимагає технічної інфраструктури та знань, що може бути проблемою для традиційних компаній).

Якщо порівнювати можливості і загрози, що дає використання криптовалют (табл. 4.2), то це матиме такий вигляд:

Таблиця 4.2 –– Порівняння можливостей і загроз

Аспект	Можливості	Загрози
Фінансові транзакції	Зменшення комісій	Волатильність курсів
Репутація	Інноваційний імідж	Невизначеність у регуляції
Технічна інтеграція	Смарт-контракти, автоматизація	Високі витрати на впровадження
Безпека	Захист через децентралізацію	Ризики кібератак

В одночас ми можемо не лише констатувати позитивні сторони та прораховувати ймовірні загрози, але й керувати ними (табл. 4.3)

Таблиця 4.4 – Загрози криптовалют для бізнесу

Загроза	Опис	Рекомендації
Волатильність курсу	Різкі зміни вартості активів	Використовувати стабільні криптовалюти (Stablecoins)
Кібератаки	Ризик втрати через злом гаманця або платформи	Встановлення систем безпеки та холодних гаманців
Відсутність регулювання	Правова невизначеність у багатьох країнах	Стежити за змінами у законодавстві
Складність інтеграції	Необхідність технічної підготовки та інфраструктури	Проводити навчання персоналу та тестування систем

Криптовалюти є перспективним фінансовим інструментом, здатним значно змінити традиційні бізнес-процеси. Однак їхнє використання вимагає врахування ризиків і розробки стратегій для їхньої мінімізації. Для підприємств, готових до змін, криптовалюти можуть стати джерелом конкурентних переваг у сучасному глобалізованому світі.

4.3 Правове регулювання криптовалют

Правове регулювання криптовалют є ключовим фактором для забезпечення їхнього безпечного використання у бізнесі. Через децентралізовану природу криптовалют уряди по всьому світу стикаються з викликами, пов’язаними з визначенням їхнього правового статусу, оподаткуванням, протидією шахрайству та відмиванню грошей.

Сучасний стан регулювання криптовалют у світі

1. **Сполучені Штати Америки**
   - криптовалюти розглядаються як власність для цілей оподаткування;
   - SEC (Комісія з цінних паперів і бірж) регулює криптовалюти, які вважаються цінними паперами;
   - FinCEN вимагає дотримання законів про боротьбу з відмиванням грошей (AML) та верифікацію користувачів (KYC).
2. **Європейський Союз**
   - у 2023 році ухвалено регламент MiCA (Markets in Crypto-Assets), який стандартизує правила використання криптовалют;
   - регламент спрямований на захист інвесторів та зниження ризиків шахрайства.
3. **Україна**
   - Закон "Про віртуальні активи" прийнято у 2021 році;
   - криптовалюти визнано як віртуальні активи, а діяльність з ними регулюється Національним банком України та Комісією з цінних паперів;
   - закон передбачає реєстрацію провайдерів послуг з віртуальними активами.
4. **Китай**
   - криптовалюти заборонені для використання у платежах та майнінгу;
   - уряд активно розвиває цифровий юань (CBDC).
5. **Японія**
   - одна з перших країн, яка легалізувала криптовалюти як засіб платежу.
   - регулювання здійснюється Агенцією фінансових послуг (FSA).

Кількість країн, що регулюють криптовалюти, з року в рік (рис. 4.5)

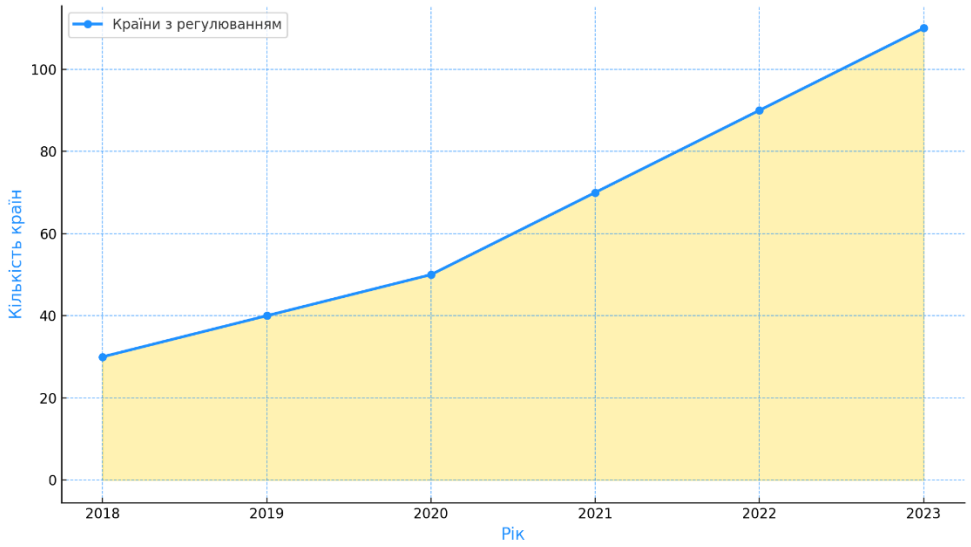

Рисунок 4.5 – Динаміка ухвалення законодавства щодо криптовалют

Основні аспекти правового регулювання (рис. 4.6)

1. **Визначення правового статусу**. Криптовалюти можуть розглядатися як власність, валюта, активи чи цінні папери, що визначає, які закони до них застосовуються.
2. **Оподаткування**. Доходи від криптовалют підлягають оподаткуванню у більшості країн. Наприклад, у США прибуток від продажу криптовалюти оподатковується як капітальний дохід.
3. **Протидія відмиванню грошей (AML)**. Законодавство вимагає проведення верифікації користувачів (KYC) для боротьби з незаконною діяльністю.
4. **Регулювання ICO (Initial Coin Offering)**. ICO часто розглядаються як емісія цінних паперів і підлягають відповідному регулюванню.
5. **Схема "Міжнародні моделі регулювання криптовалют"**. Відображає підходи різних країн (заборона, регуляція, вільне використання).

Рисунок 4.6 – Міжнародні моделі регулювання криптовалют

Виклики правового регулювання криптовалют

1. **Технологічна складність** – регулювання не завжди встигає за розвитком блокчейн-технологій.
2. **Різні підходи у країнах** – відсутність єдиних стандартів регулювання ускладнює міжнародні транзакції.
3. **Швидкість змін** – волатильність криптовалют створює труднощі для встановлення стабільних правил.

Правове регулювання криптовалют є важливим інструментом для забезпечення їх безпечного використання. Воно сприяє розвитку ринку, захисту інвесторів та протидії незаконній діяльності. Успішна інтеграція криптовалют у бізнес-практики можлива лише за умови врахування правових аспектів, тому важливим є їх регулювання на рівні держави (табл. 4.5).

Таблиця 4.5 – Порівняння підходів до регулювання в різних країнах

Країна	Правовий статус	Оподаткування	Протидія шахрайству
США	Власність	Капітальний дохід	KYC/AML
ЄС	Цифрові активи	В залежності від країни	MiCA
Україна	Віртуальні активи	Передбачено	Закон 'Про віртуальні активи'
Китай	Заборонено	Не застосовується	Повна заборона
Японія	Засіб платежу	Передбачено	FSA регуляція

4.4 Інтеграція криптовалют у бізнес-процеси

Інтеграція криптовалют у бізнес-процеси відкриває перед підприємствами нові можливості для розвитку, модернізації операцій та виходу на глобальні ринки. Однак цей процес потребує обережного підходу, врахування правових аспектів та адаптації до специфіки криптовалютних технологій.

Переваги інтеграції криптовалют

1. **Міжнародні платежі**. Криптовалюти усувають необхідність у банках та валютних обмеженнях та знижують витрати на транзакції, особливо при роботі з іноземними партнерами.
2. **Залучення нових клієнтів**. Прийняття криптовалют як оплати приваблює клієнтів, які використовують цифрові активи.
3. **Швидкість транзакцій**. Перекази здійснюються миттєво, незалежно від географічного розташування учасників.
4. **Інноваційність**. Використання криптовалют підкреслює сучасний підхід підприємства, що підвищує його репутацію.
5. **Доступ до інвестицій**. Криптовалюти можна використовувати для залучення коштів через ICO або STO.

Основні етапи інтеграції криптовалют

1. **Аналіз можливостей**
   - визначення доцільності використання криптовалют у бізнес-моделі;
   - аналіз конкурентів та потенційної клієнтської бази.
2. **Вибір платформи**
   - обрання криптогаманця та біржі для обслуговування транзакцій;
   - розгляд таких платформ, як Binance, Coinbase або Kraken.
3. **Інтеграція платіжних рішень**
   - використання API криптоплатформ для інтеграції платежів;
   - приклади рішень: BitPay, CoinGate.
4. **Навчання персоналу** – проведення тренінгів для працівників щодо особливостей криптовалютних операцій.
5. **Забезпечення безпеки**
   - використання багаторівневих систем захисту для криптогаманців;
   - резервне копіювання даних.
6. **Правове забезпечення** – реєстрація бізнесу для роботи з криптовалютами відповідно до законодавства (рис. 4.7).

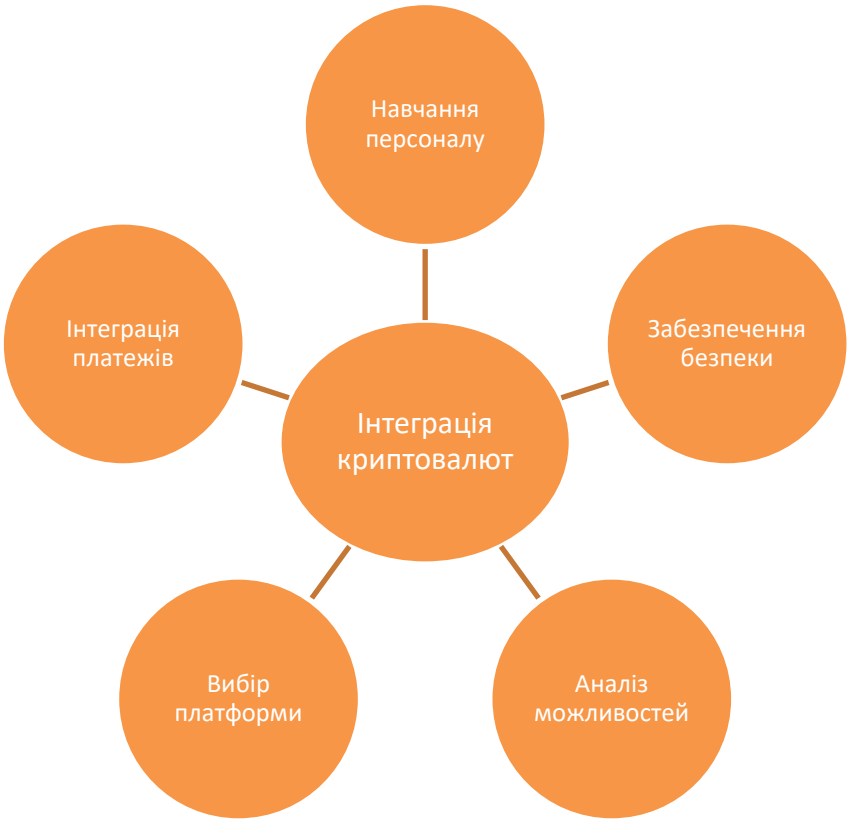

Рисунок 4.7 – Етапи інтеграції криптовалют у бізнес-процеси

Виклики інтеграції криптовалют

1. **Правові та регуляторні обмеження**. Відсутність єдиних стандартів регулювання ускладнює інтеграцію.
2. **Волатильність**. Коливання курсу криптовалют можуть впливати на доходи компанії.

3. **Кібербезпека**. Ризик хакерських атак на криптогаманці або біржі.
4. **Технічні складнощі**. Інтеграція вимагає спеціальних технічних знань та адаптації систем.

Платформи, комісії, рівень безпеки також є важливими складовими на шляху прийняття рішення щодо інвестування у криптовалюту (табл. 4.6).

Таблиця 4.6 – Порівняння криптоплатформ для бізнесу

Криптоплатформа	Комісії	Безпека	Ключові особливості
Binance	0.1%	Двофакторна аутентифікація, холодні гаманці	Широкий вибір криптовалют, високі обсяги торгів
Coinbase	1.49%	Двофакторна аутентифікація	Простота використання, підходить для новачків
Kraken	0.16%	Двофакторна аутентифікація, холодні гаманці	Підтримка фіатних валют, API для інтеграції
BitPay	1%	Шифрування транзакцій, підтримка смарт-контрактів	Зручний для бізнесу, інтеграція платежів

Реальні приклади інтеграції криптовалют

1. **Microsoft** приймає Bitcoin для покупки програмного забезпечення та ігор.
2. **Tesla** тимчасово приймала Bitcoin як оплату за автомобілі.
3. **Overstock** одна з перших платформ електронної комерції, яка почала приймати криптовалюти.
4. **PayPal** дозволяє купувати, продавати та зберігати криптовалюти у своєму додатку.

Динаміка прийняття криптовалют серед бізнесів подана на графіку (рис. 4.8)

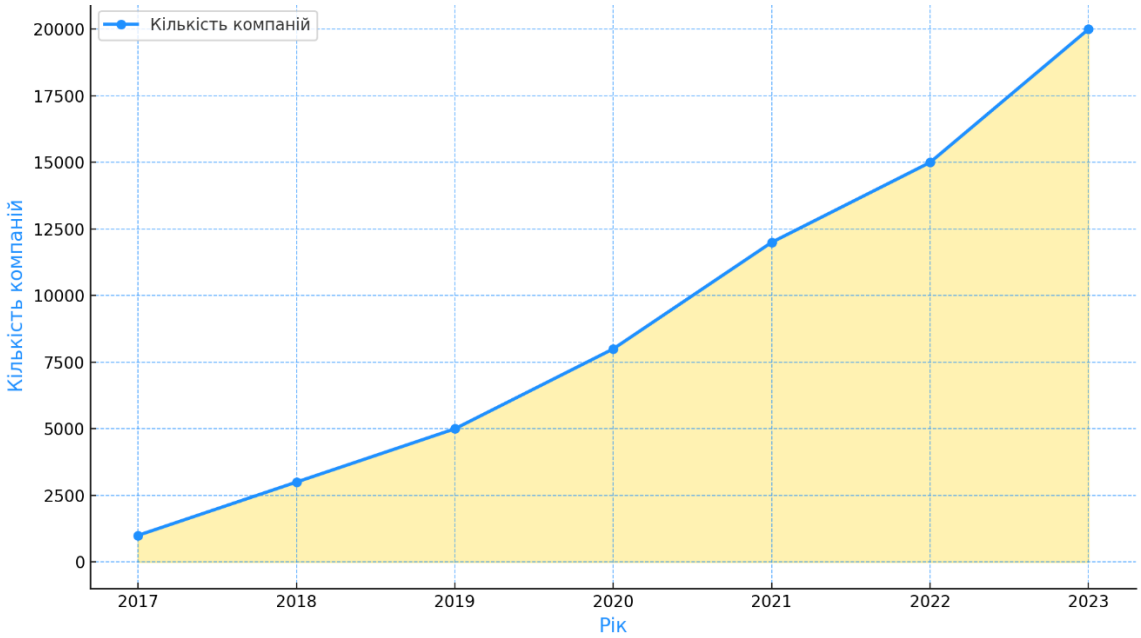

Рисунок 4.8 – Кількість компаній, які приймають криптовалюти

Інтеграція криптовалют у бізнес-процеси може стати потужним інструментом для модернізації компанії, залучення нових клієнтів та оптимізації операцій. Підприємства, які

правильно оцінюють ризики та переваги, отримують значні конкурентні переваги на сучасному ринку.

Вплив криптовалют на світову економіку

Криптовалюти докорінно змінюють структуру світової економіки, впливаючи на фінансові ринки, міжнародну торгівлю та взаємодію між державами, бізнесом і громадянами. Криптовалюти змінюють світову економіку, впроваджуючи нові моделі фінансової взаємодії, сприяючи розвитку технологій та змінюючи геополітичний ландшафт. Хоча ці зміни відкривають значні можливості, вони також потребують обережного підходу, зокрема у регулюванні та врахуванні екологічних викликів. Криптовалюти відкривають нові можливості для бізнесу, але пов'язані з низкою ризиків. Щоб мінімізувати їхній вплив, підприємства повинні розробити комплексну стратегію управління ризиками.

Стейкінг криптовалют

Стейкінг (staking) – це процес, під час якого власники криптовалют надають свої активи для підтримки операцій блокчейн-мережі, що працює на основі алгоритму консенсусу Proof of Stake (PoS) або його варіацій. Учасники отримують винагороду за зберігання криптовалют і участь у верифікації транзакцій (табл. 4.7).

Таблиця 4.7 Відмінності між стейкінгом та майнінгом

Параметр	Стейкінг	Майнінг
Алгоритм	Proof of Stake	Proof of Work
Енергоспоживання	Низьке	Високе
Вимоги	Замороження криптовалюти	Потужне обладнання
Винагороди	За участь у верифікації транзакцій	За створення блоків

Як працює стейкінг?

1. **Proof of Stake (PoS)**. У цьому механізмі власники криптовалют заморожують певну кількість монет на своєму рахунку, щоб стати валідаторами (учасниками, які перевіряють транзакції), оскільки чим більше криптовалюти заблоковано для стейкінгу, тим вищі шанси стати валідатором нового блоку.
2. **Винагорода за стейкінг**. Валідатори отримують винагороду у вигляді нових монет або частини комісії за транзакції в блокчейні.
3. **Підтримка мережі**. Стейкінг забезпечує безпеку, стійкість і функціонування мережі без потреби у великих обчислювальних потужностях (як у Proof of Work).

Процес стейкінгу

1. **Вибір криптовалюти**. Стейкінг доступний для криптовалют, які працюють на PoS, наприклад Ethereum (ETH) після переходу на Ethereum 2.0, Cardano (ADA), Solana (SOL), Polkadot (DOT).
2. **Створення гаманця**. Для стейкінгу потрібен криптогаманець, який підтримує відповідну монету та стейкінг.
3. **Заморожування активів**. Власник заморожує певну кількість монет у гаманці або передає їх до спеціального пулу.

4. **Вибір стейкінг-пулу (для делегованого PoS)**. Деякі блокчейни дозволяють передавати монети до пулів, що полегшує участь у стейкінгу для користувачів із невеликими обсягами криптовалют.
5. **Отримання винагороди**. Винагороди надходять періодично залежно від правил конкретної мережі.

Переваги стейкінгу

1. **Пасивний дохід**. Стейкінг дозволяє заробляти без необхідності продавати криптовалюту.
2. **Енергоефективність**. На відміну від майнінгу, стейкінг не потребує великих витрат електроенергії.
3. **Підтримка мережі**. Участь у стейкінгу сприяє стабільності та безпеці блокчейна.
4. **Низький поріг входу**. Деякі мережі дозволяють брати участь у стейкінгу навіть із невеликою кількістю монет.

Ризики стейкінгу

1. **Волатильність**. Ціна криптовалюти може впасти, що вплине на загальну вартість активів.
2. **Замороження активів**. Під час стейкінгу активи заморожуються, і їх не можна використовувати до завершення стейкінг-періоду.
3. **Технічні ризики**. Неправильна конфігурація гаманця або атака на пул можуть призвести до втрати винагород.
4. **Інфляція**. Емісія нових монет може знизити вартість криптовалюти.

Приклади платформ для стейкінгу

1. **Binance Staking**. Проста інтеграція для новачків та високі ставки винагороди.
2. **Kraken**. Підтримка різних криптовалют та легке управління активами.
3. **Coinbase**. Інтуїтивний інтерфейс для стейкінгу Ethereum.
4. **Ledger**. Пропонує стейкінг через апаратний гаманець для максимальної безпеки.

Стейкінг криптовалют — це перспективний спосіб заробітку, який поєднує підтримку блокчейн-мережі з отриманням пасивного доходу. Однак для успішного стейкінгу важливо враховувати ризики, дотримуватися правил безпеки та вибирати надійні платформи.

4.5 Ризики криптовалютної діяльності

Криптовалюти стають важливим інструментом у сучасній економіці, але їх використання супроводжується низкою ризиків. Знання цих ризиків і вміння їх уникати – ключ до успішного використання криптовалют у бізнесі.

1. **Волатильність ринку.** Криптовалюти відомі своїми значними коливаннями вартості, що може призвести до значних фінансових втрат. Нариклад, вартість Bitcoin у 2021 році зросла до $69,000, але потім впала до $30,000 у 2022 році. Уникнути цього ризику

можна шляхом використовувати стабільні криптовалюти (Stablecoins), або ж конвертувати отримані криптовалюти у фіатні гроші.

2. **Відсутність регулювання.** У багатьох країнах відсутня чітка правова база для криптовалют, що створює правову невизначеність. Таким чином зростає ймовірність шахрайства саме через слабке регулювання, а також виникає ускладнення інтеграції криптовалют у бухгалтерські та фінансові системи. Уникнити цього можна шляхом дотримання актуального законодавства та співпраці лише з надійними платформами.

3. **Кібератаки.** Криптовалюти приваблюють хакерів через великий обсяг активів, які можна викрасти. **Прикладами таких ризиків** є злом криптобірж (наприклад, крадіжка $500 млн з біржі Mt. Gox у 2014 році) та втрата приватного ключа до гаманця. **Тому бажано** икористовувати холодні гаманці для зберігання активів та забезпечити багаторівневу аутентифікацію.

4. **Ризик шахрайства.** Висока популярність криптовалют спричинила зростання кількості шахрайських схем, таких як фіктивні ICO чи "криптовалютні піраміди". Тому важливо перевіряти репутацію криптоплатформ і ICO та інвестувати лише через надійні джерела.

5. **Замороження активів.** У багатьох країнах уряди можуть блокувати або обмежувати використання криптовалют. Наприклад, заборона криптовалют у Китаї. Тобто при прийнятті рішення щодо інвестування потрібно обирати країни із законодавством для ведення криптодіяльності, яке відповідає меті підприємства для цієї діяльності.

6. **Непередбачуваність технологій.** Технології криптовалют розвиваються, що може призвести до технічних помилок або застарівання інфраструктури. А отже потрібно постійно оновлювати системи та навчати персонал та співпрацювати з професійними технічними фахівцями.

7. **Репутаційні ризики.** Використання криптовалют може викликати негативну реакцію клієнтів або партнерів. Тому важливо забезпечити прозорість бізнесу та залучати сторонніх експертів для розробки політик з використання криптовалют (табл. 4.8).

Таблиця 4.8 – Основні ризики криптовалютної діяльності

Тип ризику	Опис	Рекомендації
1	2	3
Волатильність	Різкі коливання вартості активів	Використовувати Stablecoins, конвертувати у фіат
Відсутність регулювання	Невизначеність у законодавстві, слабкий правовий захист	Дотримуватись актуальних законів, співпрацювати з надійними платформами
Кібератаки	Хакерські атаки, втрата ключів	Холодні гаманці, багаторівнева аутентифікація

Продовження таблиці 4.8

1	2	3
Шахрайство	Фіктивні ICO, криптовалютні піраміди	Перевірка репутації, інвестування через надійні джерела
Замороження активів	Обмеження з боку урядів	Обирати країни з прогресивним регулюванням
Непередбачуваність технологій	Можливі технічні помилки, швидке застарівання інфраструктури	Постійне оновлення систем, навчання персоналу, співпраця з технічними фахівцями
Репутаційні ризики	Негативне сприйняття з боку клієнтів або партнерів	Забезпечення прозорості, розробка політик, залучення експертів

Однак рівень збитків від атак від атак на криптобіржі та платформи зростає, а в 2023 році зріс майже у три рази (рис. 4.9):

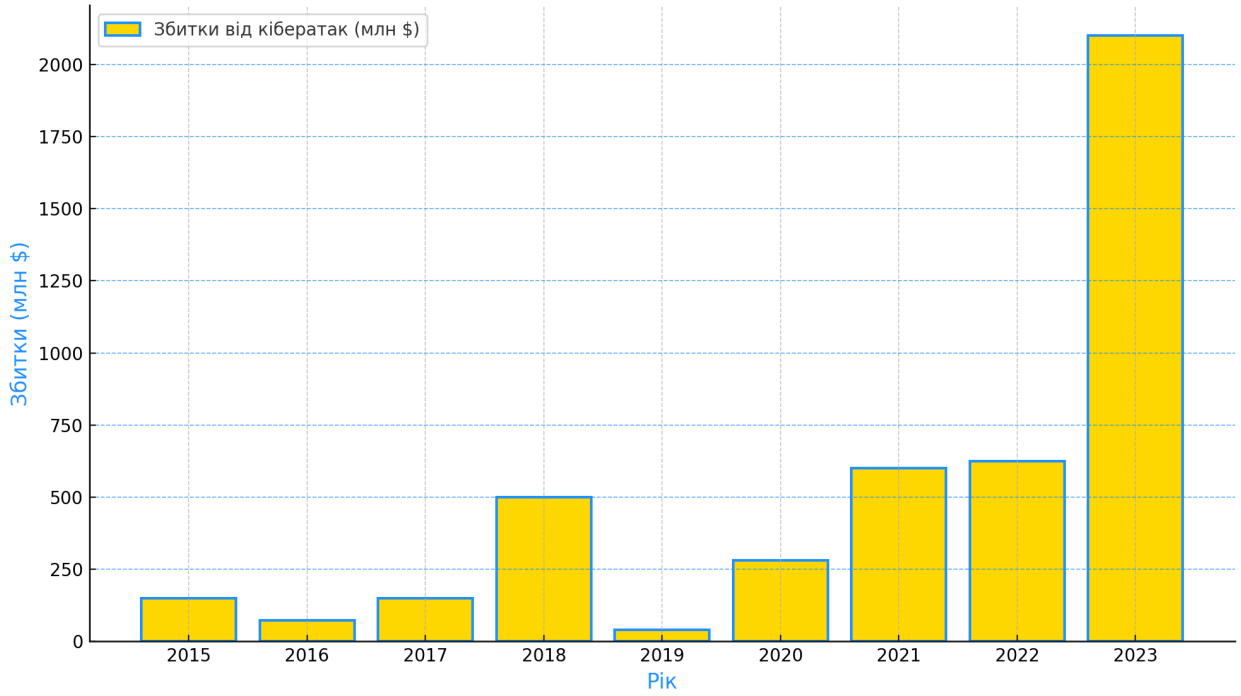

Рисунок 4.9 – Збитки від кібератак на криптовалюти (2015-2023)

Ризики криптовалютної діяльності є значними, але вони можуть бути ефективно зменшені за умови правильного управління. Бізнес повинен орієнтуватися на прозорість, безпеку та законність своїх дій у криптовалютному середовищі, щоб отримати максимальну вигоду з нових фінансових можливостей.

4.6 Приклади використання криптовалют у бізнесі

Вибір безпечної криптовалютної платформи є критично важливим для захисту ваших активів. Нижче наведено кілька провідних бірж, які відомі своїми високими стандартами безпеки:

Binance. Одна з найбільших криптовалютних бірж у світі, відома своїми високими обсягами торгівлі та широким вибором криптовалют. Binance впроваджує передові заходи безпеки, включаючи двофакторну аутентифікацію (2FA) та холодне зберігання активів.

Coinbase. Заснована у 2012 році, Coinbase є однією з найстаріших і найбільш надійних бірж, особливо популярною в США. Платформа пропонує страхування коштів користувачів та використовує надійні протоколи безпеки.

Kraken. Відома своєю надійністю та безпекою, Kraken пропонує широкий спектр криптовалют для торгівлі та впроваджує передові заходи безпеки для захисту коштів користувачів.

Gemini. Заснована братами Вінклвосс у 2014 році, Gemini відома своїм суворим дотриманням регуляторних вимог та високими стандартами безпеки.

OKX. Пропонує широкий вибір криптовалют та відома своїми передовими заходами безпеки, включаючи багаторівневу аутентифікацію та холодне зберігання активів.

Рекомендації щодо безпеки при використанні криптовалютних платформ

- двофакторна аутентифікація (2FA);
- холодне зберігання;
- сильні паролі;
- оновлення програмного забезпечення.

Пам'ятайте, що безпека ваших криптовалют залежить не лише від платформи, але й від ваших особистих заходів безпеки.

Криптовалюти, як цифрові активи, вимагають особливої уваги до безпеки, адже їхні транзакції незворотні, а втрата доступу може призвести до повної втрати активів. Нижче наведено ключові рекомендації для забезпечення безпеки криптовалют.

1. **Використовуйте надійні гаманці**
   - **Холодні гаманці** – гаманці, які не підключені до інтернету, забезпечують максимальний рівень безпеки. Наприклад, Ledger, Trezor.
   - **Гарячі гаманці** є зручними для частого використання, але менш безпечні через підключення до інтернету, тому їх доцільно використовувати для невеликих сум.
   - **Бекап і зберігання ключів**. Резервуйте приватні ключі та мнемонічні фрази в безпечному місці, наприклад, на фізичному носії.

2. **Увімкніть двофакторну аутентифікацію (2FA)** оскільки додаткова форма авторизації, наприклад, через Google Authenticator або SMS-код, значно знижує ризик злому.

3. **Оберіть надійну криптовалютну платформу** такі як Binance, Coinbase, Kraken, які мають високий рівень безпеки та перевіряйте відгуки та репутацію платформи перед використанням.

4. **Використовуйте надійні паролі.** Використовуйте довгі паролі (не менше 12 символів), які включають великі та малі літери, цифри й спеціальні символи та не використовуйте однакові паролі для різних платформ.

5. **Уникайте фішингових атак** – перевіряйте URL-адресу вебсайту криптобіржі або гаманця перед введенням особистих даних та не відкривайте підозрілі посилання в електронних листах або повідомленнях.

6. **Застосовуйте багаторівневий захист**

7. **Постійно оновлюйте програмне забезпечення,** щоб мати доступ до останніх виправлень уразливостей.

8. **Моніторинг і аудит.** Регулярно перевіряйте свої транзакції та баланс, а також використовуйте сервіси моніторингу для відстеження змін у вашому обліковому записі.

9. **Використовуйте холодне зберігання для великих сум.** Переміщуйте значні обсяги криптовалют у холодні гаманці для довготривалого зберігання, уникайте зберігання великих сум на криптобіржах.

10. **Резервне копіювання.** Зберігайте копії приватних ключів і seed-фраз у безпечному місці (наприклад, у сейфі або за допомогою спеціальних металевих карт для захисту від пошкоджень).

11. **Уникайте використання публічних мереж.** Не входьте в криптовалютні акаунти через публічні Wi-Fi мережі та використовуйте VPN для додаткового захисту в інтернеті.

12. **Страхування криптоактивів.** Розгляньте можливість страхування криптоактивів, яке пропонують деякі криптовалютні платформи та сторонні сервіси.

Рекомендації на випадок компрометації

1. **Негайно перемістіть активи**, якщо підозрюєте, що доступ до вашого гаманця компрометований.
2. **Змінюйте паролі**, пов’язані з компрометованим акаунтом.
3. **Сповістіть платформу** криптобіржі або гаманця, щоб заблокувати доступ.

Безпека криптовалют — це відповідальність кожного користувача. Використання багаторівневого захисту, надійних платформ і регулярного моніторингу допоможе захистити ваші цифрові активи від потенційних загроз.

Вплив криптовалют на інфляцію

Криптовалюти мають специфічні властивості, які можуть впливати на інфляцію як у традиційних економіках, так і у своєму власному середовищі. Їхній вплив залежить від ряду факторів, таких як кількість випущених монет, використання у фінансових операціях, а також впровадження в економічну політику.

Як криптовалюти впливають на інфляцію в традиційній економіці

1. **Обмежена взаємодія з традиційними валютами**. Більшість криптовалют працюють поза рамками традиційної банківської системи, тому їхній вплив на інфляцію національних валют поки що мінімальний. У країнах із слабкою економікою криптовалюти можуть використовуватися як захист від гіперінфляції (наприклад, у Венесуелі чи Зімбабве).
2. **Заміна традиційних валют**. Зростання використання криптовалют може зменшити попит на національні валюти, що може призвести до нестабільності на валютному ринку.
3. **Вплив на монетарну політику**. Криптовалюти обмежують можливість урядів і центральних банків регулювати економіку через емісію грошей.

Інфляція всередині криптовалютного ринку

1. **Обмежена емісія**. Багато криптовалют мають фіксований максимум випуску монет (наприклад, Bitcoin — 21 мільйон), що робить їх захищеними від інфляції. Цей механізм схожий на дефляцію, оскільки з часом видобуток монет стає дедалі складнішим.
2. **Stablecoins**. Криптовалюти, прив’язані до фіатних валют (наприклад, USDT, USDC), допомагають уникнути інфляції за рахунок стабільності вартості. Stablecoins можуть служити альтернативою у країнах із високою інфляцією.
3. **Майнінг і нагороди**. У криптовалютах, що працюють на алгоритмі Proof of Work або Proof of Stake, нові монети вводяться в обіг через майнінг чи стейкінг. Цей процес може призводити до інфляції, якщо швидкість емісії перевищує попит.

Приклади впливу криптовалют на економіку

1. **Венесуела**. Гіперінфляція болівара змусила громадян звернутися до Bitcoin як засобу збереження вартості та обміну.
2. **Ель-Сальвадор**. Впровадження Bitcoin як офіційного платіжного засобу створило нову економічну модель, яка частково знижує залежність від долара США.
3. **Розвинені країни**. У розвинених економіках криптовалюти використовуються більше як інвестиційний актив, ніж як засіб платежу, тому їхній вплив на інфляцію мінімальний.

Переваги криптовалют у боротьбі з інфляцією

1. **Захист капіталу**. Криптовалюти з обмеженою емісією (наприклад, Bitcoin) слугують захистом від інфляції фіатних валют.
2. **Децентралізація**. Відсутність централізованого контролю знижує ризик маніпуляцій з грошовою масою.

3. **Технологічні рішення**. Криптовалюти та блокчейн можуть використовуватися для створення прозорих і контрольованих фінансових систем.

Ризики криптовалют щодо інфляції

1. **Висока волатильність**. Значні коливання курсу криптовалют можуть створювати ризик втрати вартості активів.
2. **Швидка емісія**. У деяких криптовалютах (наприклад, Dogecoin) немає обмеження на кількість монет, що може призводити до інфляції.
3. **Обмежена масштабованість**. Якщо криптовалюта не може підтримувати високий обсяг транзакцій, її використання як альтернативної валюти обмежене.

Криптовалюти здатні впливати на інфляцію у двох напрямках. У традиційній економіці вони можуть стати альтернативою фіатним валютам, захищаючи капітал у країнах із нестабільною економікою. Водночас, у своєму середовищі криптовалюти з обмеженою емісією захищені від інфляції, тоді як монети з необмеженим випуском можуть знецінюватися. Їхній загальний вплив на світову економіку залежить від рівня інтеграції криптовалют у фінансові системи та монетарну політику.

Перелік питань:

1. Що таке криптовалюта, і які її основні характеристики?
2. У чому полягає сутність криптовалют як фінансового інструменту?
3. Як працює блокчейн і які його основні компоненти?
4. Які види криптовалют існують, і чим вони відрізняються один від одного?
5. У чому полягає відмінність між Bitcoin, Ethereum та Stablecoins?
6. Які основні можливості надають криптовалюти для бізнесу?
7. Які основні ризики використання криптовалют у бізнес-процесах?
8. Як криптовалюти змінюють структуру світової економіки?
9. У яких країнах криптовалюти мають найбільш чітке правове регулювання?
10. Як відбувається інтеграція криптовалют у бізнес-процеси?
11. Які платформи є найбільш популярними та безпечними для роботи з криптовалютами?
12. Що таке стейкінг криптовалют, і як він працює?
13. Як криптовалюти можуть бути використані для протидії інфляції?
14. У чому полягає основна ідея правового регулювання криптовалют?
15. Які виклики виникають під час інтеграції криптовалют у бізнес?
16. Як можна мінімізувати ризики, пов’язані з використанням криптовалют?
17. Які можливості криптовалюти надають підприємствам у період економічної нестабільності?
18. Як впливають криптовалюти на міжнародну торгівлю?
19. Чим відрізняються холодні та гарячі гаманці для криптовалют?
20. Які приклади успішної інтеграції криптовалют у бізнес-практики існують?

Тести:

1. **Що таке блокчейн?**
   а) алгоритм шифрування для забезпечення конфіденційності даних;
   б) розподілена база даних, що записує транзакції у вигляді блоків;
   в) централізована платформа для обміну крипто валютами;
   г) програмне забезпечення для майнінгу криптовалют.

2. **Яка з наведених криптовалют є прикладом Stablecoin?**
   а) Bitcoin;
   б) Ethereum;
   в) Tether (USDT);
   г) Dogecoin.
3. **Основна перевага використання смарт-контрактів:**
   а) зниження витрат на юридичні послуги;
   б) підвищення курсу крипто валюти;
   в) обмеження доступу до транзакцій;
   г) створення централізованої мережі.

4. **Який принцип роботи Proof of Stake?**
   а) використання обчислювальної потужності для підтвердження транзакцій;
   б) розподіл транзакцій за допомогою майнінгу;
   в) верифікація транзакцій на основі кількості заблокованих монет;
   г) централізований контроль операцій.

5. **Яка країна першою визнала Bitcoin офіційною валютою?**
   а) Японія;
   б) США;
   в) Ель-Сальвадор;
   г) Швейцарія.

6. **Який алгоритм забезпечує захист криптовалютних транзакцій?**
   а) SHA-256;
   б) HTTPS:
   в) RSA:
   г) AES.

7. **Що таке токенізація активів?**
   а) створення цифрових копій активів для продажу на блокчейні;
   б) перетворення криптовалют у фіатні гроші;
   в) верифікація транзакцій у децентралізованій мережі;
   г) випуск нової криптовалюти.

8. **Як забезпечити безпеку криптогаманця?**
   а) використовувати публічні Wi-Fi мережі;

б) використовувати холодний гаманець;
в) зберігати приватний ключ у електронній пошті;
г) змінювати пароль раз на рік.

9. **Який механізм захисту даних використовує блокчейн?**
   а) централізоване шифрування;
   б) розподілене зберігання та хешування;
   в) зберігання інформації у централізованих дата-центрах;
   г) компресія даних.

10. **Яке головне призначення Stablecoins?**
    а) збільшення волатильності ринку;
    б) збереження стабільності курсу;
    в) майбутнє використання в ICO;
    г) зменшення вартості транзакцій.

11. **Який метод найбільш ефективний для уникнення волатильності криптовалют?**
    а) інвестування у майнінг;
    б) використання Stablecoins;
    в) хеджування біткоїнів;
    г) використання централізованих бірж.

12. **Що таке стейкінг?**
    а) процес майнінгу криптовалют;
    б) заморожування активів для підтримки мережі Proof of Stake;
    в) торгівля криптовалютами на біржі;
    г) зберігання криптовалют у гарячих гаманцях.

13. **Яка проблема часто виникає через відсутність регулювання криптовалют?**
    а) підвищення довіри до криптовалют;
    б) непрозорість операцій;
    в) надмірне зростання стабільності ринку;
    г) підвищення вартості транзакцій.

14. **Як криптовалюти допомагають у міжнародній торгівлі?**
    а) зменшують витрати на перекази;
    б) обмежують доступ до глобальних ринків;
    в) ускладнюють фінансові операції;
    г) збільшують залежність від фіатних валют.

15. **Яка роль блокчейну в забезпеченні прозорості?**
    а) приховування даних про транзакції;
    б) фіксація всіх операцій у незмінній базі даних;

в) автоматичне видалення даних через певний час;
г) створення приватних записів у централізованих серверах.

16. **Які криптовалюти зазвичай мають обмежену емісію?**
    а) Bitcoin;
    б) Ethereum;
    в) Tether;
    г) Dogecoin.

17. **Який з нижченаведених факторів найкраще описує волатильність криптовалют?**
    а) стабільність курсу;
    б) значні коливання ціни на коротких часових інтервалах;
    в) постійний приріст вартості;
    г) відсутність змін ціни.

18. **Як криптовалюти впливають на економіку країн із високою інфляцією?**
    а) підвищують рівень інфляції;
    б) знижують залежність від національної валюти;
    в) зменшують обсяг зовнішньої торгівлі;
    г) ускладнюють фінансові операції.

19. **Що є головною перевагою токенізації активів?**
    а) створення централізованих баз даних;
    б) прискорення доступу до інвестицій;
    в) збільшення волатильності;
    г) скорочення часу транзакцій.

20. **Як уникнути шахрайства під час використання криптовалют?**
    а) використовувати публічні Wi-Fi мережі;
    б) Співпрацювати лише з перевіреними платформами;
    в) Ігнорувати верифікацію KYC;
    г) Зберігати ключі у публічному доступі.

Практичні завдання

Завдання 1. Дослідження сутності криптовалют

Мета: Зрозуміти основні властивості криптовалют та їх використання як фінансового інструменту.

1. Визначте основні характеристики криптовалют (децентралізація, прозорість, обмежена емісія).
2. Порівняйте три криптовалюти: Bitcoin, Ethereum та Tether. Результати подайте у вигляді таблиці з характеристиками (механізм консенсусу, волатильність, використання в реальному житті).

3. Обговоріть, як кожна з цих криптовалют може бути використана підприємством для досягнення фінансових цілей.

Завдання 2. Аналіз ризиків криптовалютної діяльності

Мета: Навчитися ідентифікувати та оцінювати ризики, пов'язані з використанням криптовалют.

1. Ознайомтеся із прикладом:
   Підприємство вирішило приймати платежі в Bitcoin.
   - визначте три основні ризики, пов'язані з цією практикою (волатильність, кібербезпека, правова невизначеність);
   - запропонуйте способи мінімізації кожного з ризиків.
2. Оцініть ймовірність та вплив кожного ризику за шкалою (низький, середній, високий). Заповніть таблицю.

Ризик	Ймовірність	Вплив
Волатильність		
Кібербезпека		
Правова невизначеність		

Завдання 3. Оцінка інтеграції криптовалют у бізнес

Мета: Розробити стратегію інтеграції криптовалют у бізнес-процеси підприємства.

1. Сформуйте список кроків для інтеграції криптовалют у процес прийому платежів, зокрема:
   - вибір платформи для обробки платежів;
   - впровадження системи обліку криптовалютних операцій;
   - забезпечення безпеки транзакцій.
2. Опишіть, які технічні та організаційні заходи потрібно реалізувати для успішної інтеграції.

Завдання 4. Побудова мапи ризиків

Мета: Навчитися візуалізувати ризики, пов'язані з криптовалютами.

1. Використовуючи визначені раніше ризики (волатильність, кібербезпека, правова невизначеність), побудуйте мапу ризиків.
   - X-вісь: Ймовірність виникнення ризику;
   - Y-вісь: Вплив ризику на бізнес.
2. На основі мапи визначте, які ризики потребують негайної уваги, а які є прийнятними для підприємства.

Завдання 5. Аналіз законодавства щодо криптовалют

Мета: Ознайомитися з правовим регулюванням криптовалют у різних країнах.

1. Зробіть короткий огляд законодавства щодо криптовалют у трьох країнах (наприклад, США, Україна, Китай).
2. Визначте, які вимоги до бізнесу існують у кожній країні для роботи з криптовалютами.
3. Запропонуйте рекомендації для підприємства, яке планує інтегрувати криптовалюти, з урахуванням різних правових моделей.

Завдання 6. Дослідження волатильності криптовалют

Мета: Навчитися аналізувати волатильність криптовалют та її вплив на фінансові операції.

1. Використовуючи дані про курс Bitcoin за останні 6 місяців, побудуйте графік змін ціни.
2. Проаналізуйте, як коливання курсу вплинуло б на підприємство, якби воно отримувало платежі в Bitcoin.
3. Запропонуйте механізми захисту від волатильності (наприклад, використання Stablecoins, конвертація в фіат).

Завдання 7. Розробка політики використання криптовалют

Мета: Розробити внутрішню політику підприємства щодо використання криптовалют.

1. Складіть документ, у якому визначте:
   - основні принципи роботи з криптовалютами;
   - відповідальних осіб за моніторинг криптовалютних операцій;
   - заходи безпеки для захисту криптоактивів підприємства.
2. Обговоріть, як політика підприємства може вплинути на довіру клієнтів.

Завдання 8. Практичний кейс: Впровадження криптовалютних платежів

Мета: Використати теоретичні знання для розв'язання практичної задачі.

1. Ситуація:
   Магазин електроніки вирішив приймати платежі в Ethereum.
   - розробіть детальний план впровадження криптоплатежів, включаючи технічні, організаційні та маркетингові аспекти;
   - визначте потенційні переваги та ризики цього рішення.
2. Запропонуйте заходи для підвищення безпеки криптовалютних операцій у цьому магазині.

РОЗДІЛ 2. АНАЛІЗ РИЗИКІВ ТА ЗАХИСТ ОСНОВНИХ АКТИВІВ ПІДПРИЄМСТВА

ТЕМА 5. ОЦІНКА ТА АНАЛІЗ РИЗИКІВ У СФЕРІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

5.1 Класифікація ризиків.
5.2 Методи ідентифікації ризиків.
5.3 Оцінка ймовірності та впливу ризиків.
5.4 Стратегії управління ризиками.

5.1 Класифікація ризиків

Сутність ризиків у сфері економічної безпеки

Ризики в економічній безпеці – це потенційні загрози, які можуть порушити стабільність, ефективність і конкурентоспроможність підприємства. Їхня класифікація дозволяє систематизувати загрози, визначити пріоритети та розробити ефективні механізми управління.

Категорія «ризик» виникла доволі давно, проте найбільш активно різні його аспекти стали предметом вивчення лише і кінці XIX – початку XX ст.

Для української економічної науки питання, пов’язані з ризиком та його оцінюванням, не належать до інноваційних, адже ще в 20-х роках XX ст. було розроблено низку нормативно-законодавчих документів, які брали до уваги наявність у Радянському Союзі певного господарського ризику. В той же час дещо пізніше, вже після впровадження адміністративно-командної системи формування продуктивності виробничо-господарської сфери в межах планової економіки всі наявні економічні обґрунтування запроваджуваних програм здійснювались без дослідження ймовірних ризиків.

Перебудова економічної системи нашої держави спонукала до посилення уваги до проблем ризику в виробничо-господарській площині, а наявна теорія ризику в розрізі становлення ринкових відносин не лише набула подальшого ефективного розвитку та стала популярною в практичній діяльності.

Ризик – це ймовірні загрози втрат, які лежать у площині тих або інших явищ у сфері діяльності менеджерів різних ланок управління, об’єктами якого є економічна система, орієнтована на конкретну мету з визначенням векторів її досягнення, має риси вірогідносної економічної та об’єктивно-суб’єктивної природи, широкого діапазону варіативності, оперативності, перманентності, врахування межі ризику та виступає в якості джерела прогресу.

На рисунку 5.1 окреслено основні характеристики ризику як економічної категорії.

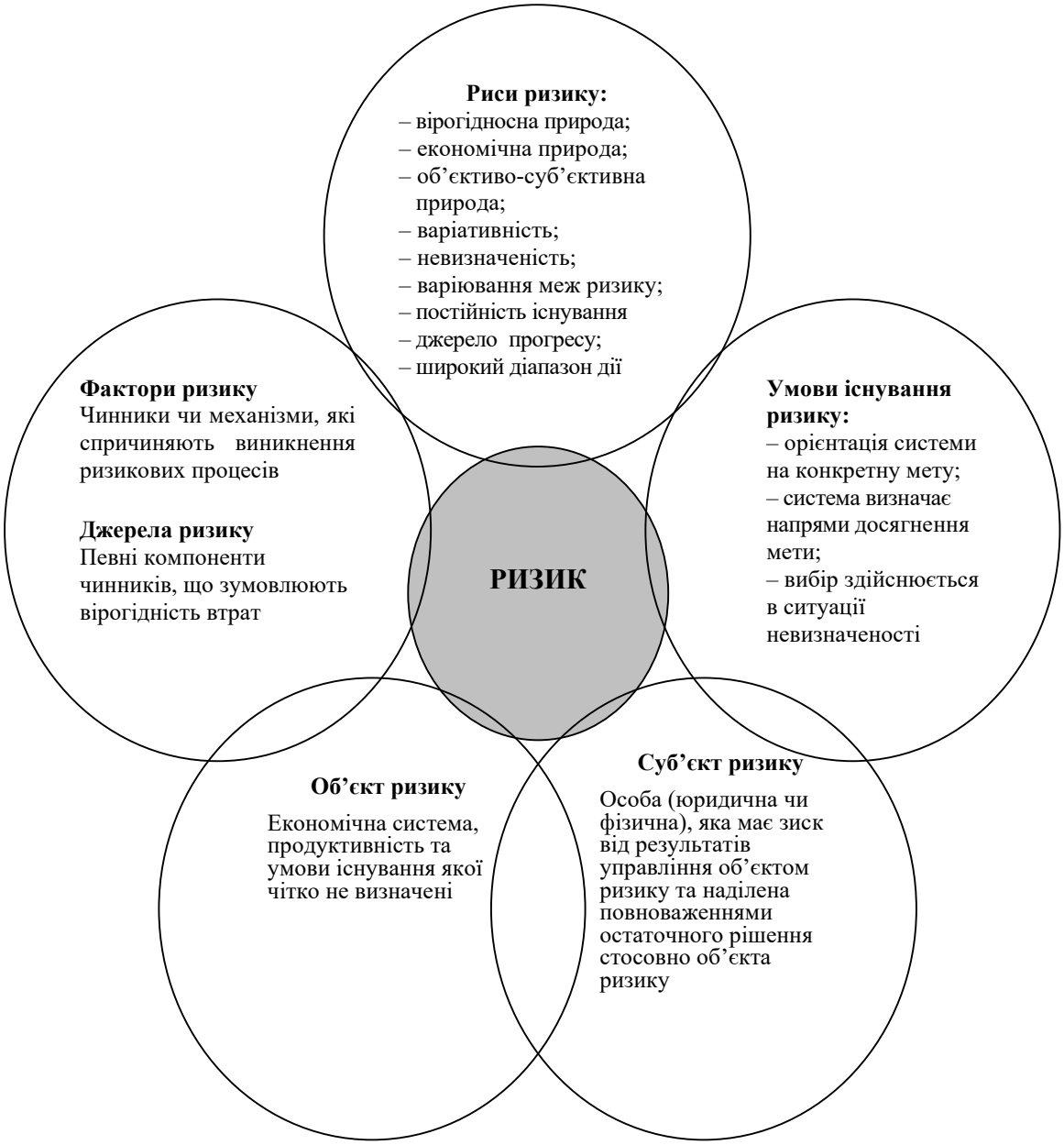

Рисунок 5.1 – Характеристика ризику як економічної категорії

Виникнення ризиків, пов'язаних з підприємницькою діяльністю, спричинене наявністю низки чинників. Представлені чинники, які окреслюють межу ризику, диференціюються за двома групами – об'єктивні чи зовнішні, а також суб'єктивні чи внутрішні. До групи об'єктивних чинників входять ті, що напряму не залежать від певного товаровиробника. Тому суб'єкт господарювання має координувати власну діяльність так, щоб мати можливість нейтралізувати їх негативний прояв та опиратись на ймовірні сприятливі можливості. Водночас, об'єктивні чи зовнішні чинники ризику включають ті, що мають прямий вплив і такі, що мають непрямий вплив.

До чинників прямого впливу можна віднести:

- законодавчі та нормативно-правові документи, що координують виробничо-господарську та підприємницьку сфери;
- бюджетна, податкова та фінансово-кредитна сфери;
- дії владних інституцій;

- дії економічних партнерів (споживачів, постачальників, посередників та ін.);
- конкурентне середовище;
- вплив кримінального середовища та ін.
- До чинників непрямого впливу можна віднести:
- соціально-політична, економічна, екологічна, демографічна ситуації та певні їх зміни;
- природні катаклізми;
- економічні зв'язки в сфері міжнародної торгівлі;
- науково-технічний прогрес та ін.

До групи суб'єктивних чинників можна віднести ті, що характеризують суб’єкт господарювання:

- стратегічне планування розвитку;
- маркетингова діяльність;
- виробничий потенціал;
- сучасні технології;
- персонал та його мотивація;
- якість товарної продукції;
- система менеджменту;
- зручність місця розташування та ін.

Зазначені чинники ризику є зазвичай керованими, а тому їх вплив можна суттєво послабити, тобто мінімізувати. Окресленим групам чинників ризику властиві спільні ознаки, які тісно взаємопов’язані. З огляду на це обидві групи чинників доцільно розглядати разом, у їх логічній послідовності.

Варто зауважити, що переважна більшість представлених ризиків у разі їх виникнення можуть призвести до деструктивних наслідків для товаровиробників, серед яких, передусім, різні - матеріальні, фінансові, трудові збитки та втрати. Всі наявні види втрат доцільно скомпонувати таким чином (табл. 5.1).

Таблиця 5.1 – Види втрат від виникнення ризиків

Вид втрат	Характеристика
1	2
Матеріальні	Понадпланове використання сировини, матеріалів, палива тощо, які виникли в результаті трансформації зовнішнього чи внутрішнього середовища функціонування товаровиробника
Фінансові	Найчисельніша група втрат у підприємницькій сфері. Являють собою безпосередні збитки фінансового характеру, спричинені з непрогнозованими платежами, сплатою штрафних санкцій; втратою грошових коштів, додаткових податків, цінних паперів; зниження надходжень через падіння цін на продукцію внаслідок інфляції; зміна валютного курсу та ін.
Виробничо-трудові	Спричинені випадково чи непрогнозованими обставинами у виробництві, що призводить до нераціонального використання робочого часу

Продовження таблиці 5.1

1	2
Соціально-економічні	Виникають як наслідок технологічних особливостей у виробничій сфері, прояву екологічних ризиків. Зумовлені з втратою роботи та спричиняють погіршення якості життя людей. Суттєвим соціально-економічним ризиком є наслідки безробіття
Просторово-часові	Виникають у випадках, коли функціонування виробничої сфери уповільнюється порівняно з планом (збільшення часу, необхідного для монтажу устаткування, впровадження нової технології, організація досліджень та наукових розробок). Випадкові часові втрати значною мірою впливають на обсяги доходу
Іміджеві	Збитки внаслідок помилок управлінців промислового підприємства, що створює атмосферу недовіри або неадекватного сприйняття його наявними та потенційними споживачами та партнерами
Специфічні	Збитки від неочікуваних політичних процесів збитки внаслідок стихійного лиха, надзвичайних ситуацій, крадіжок чи рейдерства; Збитки через низьку кваліфікацію управлінців, що відповідають за бізнес-планування та ін.

У науковій літературі налічують значну кількість різних ознак ризиків та їх видів, що свідчить про відсутність у науковців одностайності у підходах до цієї проблеми.

Варто зосередити увагу на тих класифікаційних характеристиках, які є найбільш науковоємними:

1. За специфікою прояву розрізняють – економічний, соціальний, політичний, технологічний, екологічний ризики та ін.

2. За різновидами діяльності – виробничий, фінансовий, інвестиційний, ресурсний, інноваційний, маркетинговий (комерційний), транспортний ризики та ін.

3. За масштабністю – на рівні держави, на рівні регіону, на рівні галузі, на рівні окремого товаровиробника.

4. За джерелами появи:
   - ринковий або систематичний (притаманний усім суб'єктам ринкових відносин), спричинений ринковими процесами;
   - несистематичний (ризик певних товаровиробників, зумовлений специфікою їхньої діяльності).

5. За відношенням до самого ризику:
   - ризик внаслідок активної діяльності;
   - ризик від пасивного очікування.

6. За рівнем обґрунтованості управлінських рішень чи дій можна поділити на виправданий, а також невиправданий ризики.

7. З огляду на вид виробництва виділяють ризики в площині основного виробництва та ризики в площині допоміжних виробництв.

8. За рівнем контролю:
   - жорстко контрольовані ризики, яким можливо запобігти чи послабити їх дію;
   - фрагментарно контрольовані;
   - зовсім неконтрольовані, яких дуже складно уникнути або знизити їх від'ємні наслідки.

9. З огляду відношення джерела ризику до товаровиробника виділяють внутрішній і зовнішній ризики.

Як правило, зовнішні ризики підприємницької діяльності напряму не пов'язані зі сферою діяльності товаровиробників чи їх ділових партнерів, а спричинені суттєвими змінами у зовнішньому оточенні. Перш за все, це стосується діяльності на міжнародному рівні, наявної конкуренції на ринку, суттєвим загостренням проявів економічної кризи в державі, кон'юнктури наявного фінансово-кредитного ринку, законодавства в податковій сфері, наслідками природних катаклізмів, війн, загального стану промислових підприємств тощо.

Натомість, внутрішні ризики підприємницької діяльності представлені ризиками, які є наслідком функціонування самого товаровиробника, його управлінців і контрагентів.

Водночас існують класифікації і зовнішніх, і внутрішніх ризиків. Зокрема, відомим науковцем Й.М. Петрович запропоновано ґрунтовну класифікацію ризиків.

1. Прийняття рішень в контексті часу:
   - випереджальні (дають можливість завчасно оцінити та обґрунтувати заходи по керуванню ризиками);
   - своєчасні (характеризуються динамічністю чинників ризику, потребують систематичного оцінювання та керування);
   - запізнілі (мають місце у випадку відсутності завчасної інформованості, оцінюються вже після появи ризику).
2. За наявним рівнем (ступенем) прояву ризики можна диференціювати як досить низькі, помірні, повномасштабні (мінімально допустимі, оптимальні, прийнятні, усереднені, максимально допустимі, критичні, катастрофічні).

Кваліфікація ризику відповідно до зазначених категорій зумовлюється вірогідністю настання та обсягом втрат, які ймовірно можуть виникнути в конкретній ситуації. Збитки від катастрофічних ризиків зазвичай є наймасштабнішими, а від мінімальних, як правило, найменшими. Однак такий тип ризиків, як катастрофічні трапляються досить рідко порівняно з середніми або мінімальними. Доцільно сукупність можливих ризиків надати у формі певної ієрархії, в основі якої лежать мінімальні ризики, а найвищим проявом є катастрофічні (таблиця 5.2).

Таблиця 5.2 – Ієрархічні рівні ризику

Диферен-ціація	**Рівень ризику**	**Вірогідність появи, %**	**Обсяг втрат відносно прогнозованого рівня, %**	**Негативний прояв ризику у сфері фінансів**
1	2	3	4	5
Низькі	мінімальні	0–5	0–10	Тимчасові фінансові труднощі
	оптимальні	5–15	10–15	

Продовження таблиці 5.2

1	2	3	4	5
Помірні	допустимі	15–25	15–25	Тимчасове послаблення конкурентоспроможності
	середні	25–50	25–50	Фінансова стагнація
Повні	максимальні	50–70	50–70	
	критичні	70–90	70–90	Фінансова нестабільність
	катастрофічні	90–100	90–100	Банкрутство

1. За видом (за мірою обґрунтованості появи ризику) – раціональні (виправдані: наслідки для товаровиробника мінімальні), нераціональні (певною мірою обґрунтовані: вірогідність негативного впливу значний, але ймовірні збитки не перевищують очікуваних надходжень, мають нульовий ефект), азартні (значна вірогідність того, що мета не буде досягнута, сподівання на випадковість).

2. За кількістю осіб, залучених до прийняття рішення – індивідуальні, групові або масові.

3. За тривалістю впливу – короткочасні та постійні.

4. За приналежністю до страхового випадку – ризики, які підпадають під страхування, та ризики, що лежать за межею страхової ситуації.

5. За особливістю наслідків – чисті або спекулятивні.

До чистих ризиків, тобто до простих чи статичних, належать ті, що, зазвичай, спричиняють появу втрат у підприємницькій сфері, виникають внаслідок стихійних лих, злочинів, війни, нещасних випадків, некомпетентність провідних управлінців тощо.

Спекулятивні ризики, так звані динамічні чи комерційні, відзначаються тим, що здатні призвести як до певних втрат, так і до отримання надпланового прибутку товаровиробником. Джерелами спекулятивних ризиків зазвичай є суттєві зімни кон'юнктури ринку, податкового законодавства, валютних курсів та ін.

1. За характером загрози:
   - техногенні ризики, що є результатом виробничо-господарської діяльності юридичної чи фізичної особи;
   - природні ризики, на які не впливає людська діяльність;
   - змішані ризики, тобто певні події природного плану або результати господарської діяльності.

Безумовно, пріоритетною сферою діяльності переважної більшості товаровиробників є виготовлення товарної продукції чи послуг. Однак вона нерозривно пов'язана з фінансовою діяльність, яка виконує роль забезпечення нормальної життєдіяльність промислового підприємства та покращення показників його роботи. Всі ризики, що виникають у результаті такої діяльності, виокремлюють у групу, так званих, фінансових ризиків, які мають найсуттєвіші наслідки в загальній низці ризиків суб'єкта господарювання. З огляду на це особливої уваги заслуговує питанню їх диференціації.

Фінансові ризики в широкому сенсі – це такі ризики діяльності в підприємницькій сфері, які відзначаються вірогідністю втрат наявних фінансових ресурсів, а у дещо звуженому розумінні – це вірогідність фінансових втрат внаслідок операційної діяльності у фінансово-кредитній та біржовій площині [248, с. 64].

В той же час, фінансові ризики товаровиробника відрізняються значною різноманітністю, для того, щоб продуктивно керувати ними, доцільно їх класифікують за характерними особливостями (табл. 5.3).

Таблиця 5.3 – Класифікаційні особливості захищеності підприємства від ризиків фінансової сфери

Класифікаційна ознака	Можливі загрози фінансовій сфері
За можливим місцем появи	Ризик зменшення фінансової стабільності Ризик дисбалансу ліквідності Інвестиційно-інноваційний ризик Ризик знецінення Відсотковий ризик Емісійний ризик Ризик акціонерів Позичковий ризик Інші види ризиків
За фінансовими операціями	Ризик вкладень у бізнес Ризик тривалих інвестиційних проектів Ризик керування оборотним капіталом Ризик керування основним капіталом
За наявним об’єктом	Ризик одиничної фінансової операції Ризик різних видів фінансової сфери Загальний ризик фінансової сфери суб’єкта господарювання
За комплексом важелів	Індивідуальний фінансовий ризик Портфельний фінансовий ризик
За повнотою дослідження	Одиничний фінансовий ризик Комплексний фінансовий ризик
За фінансовими результатами	Ризик фінансових втрат Ризик втрати вигоди Ризик збитків та паралельної появи додаткових втрат
За ступенем фінансових втрат	Прийнятний рівень фінансового ризику Граничний рівень фінансового ризику Фінансовий ризик на межі краху
За можливістю прогнозування	Передбачуваний фінансовий ризик Непередбачуваний фінансовий ризик Ризик невиправданих прогнозів
За характером взаємозв’язку ризиків	Взаємопов’язані ризики Непов’язані ризики Ризики з міцним внутрішнім зв’язком Ризики з слабким внутрішнім зв’язком

У процесі аналізу особливостей ризиків доцільно розглядати їх різновиди, що не перетинаються, з метою унеможливлення подвійного обліку. Проте в такому випадку мають місце певні проблеми, що потребують своєчасного вирішення:

- одні й ті ж чинники здатні впливати на позитивну та негативну динаміку різних ризиків;
- ризики, які мають певну спорідненість та особливості ризиків інших різновидів, водночас можуть бути складовими для інших груп, тобто такі ризики, які різняться за рівнем впливу, можна віднести до певних економічних ризиків, чи ризики, виокремленні за формами прояву, можна віднести до ризику державного рівня;

– один і той же різновид ризику, з огляду на різні умови, можна віднести як до зовнішніх, так і безпосередньо до внутрішніх, зокрема, ризик вкладень з власних джерел (амортизаційних відрахувань, прибутку тощо), оскільки облікова державна політика базується на єдиних підходах, проте нормативно-законодавчою базою надається право товаровиробникам на певну автономію.

5.2 Методи ідентифікації ризиків

Вивчення ризиків у їх сукупності та кожного окремо дає змогу встановити їх ієрархію, сформувати сценарії вірогідного розвитку подій у чітко окресленій ситуації, скласти прогнозну карту ризику, встановити межі стійкості системи менеджменту, опираючись на імітаційне, а також інші типи моделювання. Тобто, можна стверджувати, що класифікація ризиків є інструментом організації керування ризиками.

Ідентифікація ризиків – це перший і надзвичайно важливий етап у процесі управління ризиками. Вона дозволяє визначити потенційні загрози, які можуть вплинути на діяльність підприємства, та підготувати стратегії їхнього запобігання. Ідентифікація ризиків включає аналіз усіх аспектів діяльності підприємства для виявлення загроз, що можуть виникати як з внутрішніх, так і з зовнішніх джерел. Метою є створення повного переліку ризиків, які можуть зашкодити економічній безпеці.

В конкретних умовах об’єктивного прояву ризику та похідних від нього фінансово-економічних, морально-етичних та інших різновидів втрат виникає нагальна потреба щодо формування такого механізму, який дозволив би якомога краще (зважаючи на визначену суб’єктом господарювання або його керівництвом мету) оцінювати ризик під час ухвалення та виконання управлінських рішень. До такого механізму відносять керування ризиком, тобто ризик-менеджмент.

В цілому керування ризиком можливо надати у вигляді комплексу методів, прийомів та необхідних кроків, що дозволять значною мірою передбачити ймовірність виникнення ризикових подій та вчасно вжити ефективних заходів з метою запобігання чи мінімізації їх від’ємних результатів.

Існує альтернативне тлумачення цієї дефініції, за якою керування ризиком є певним процесом його ідентифікації, дослідження та зменшення, опираючись на засоби дієвого контролю або втілюючи заходи, що дають змогу знижувати негативний вплив внаслідок ризиків у виробничій сфері.

На переконання Майкла А. Бретта, керування ризиками – це своєрідний процес, який містить кілька послідовних стадій, зокрема: дослідження ризику, спостереження за проявами ризику, фінансове забезпечення ризику.

Відповідно до міжнародного стандарту FERMA ризик-менеджмент являє собою певний процес, дотримуючись якого суб’єкт господарювання комплексно досліджує ризики окремо взятого різновиду виробничої діяльності для забезпечення максимально можливого ефекту ймовірних кроків і, як наслідок, всієї виробничо-господарської сфери товаровиробника загалом».

Зважаючи на викладене вище, можна запропонувати власне бачення дефініції «керування ризиками», зокрема як комплексу зважених послідовних кроків суб'єкта господарювання, які певною мірою дають змогу уникнути ризиків або суттєво знизити періодичність та ймовірні обсяги їх негативних проявів.

Також варто звернути належну увагу на характерні специфічні риси ризик-менеджменту. По-перше, метою ризик-менеджменту є своєчасна ідентифікація ймовірних ризиків та їх запобігання, замість того, щоб усувати їх негативні прояви. По-друге, ризик-менеджмент являє собою комплекс інноваційних методичних підходів і процесів, застосування яких є вкрай важливим для реалізації стратегічних завдань промислового підприємства.

По-третє, ризик-менеджмент має бути систематичним процесом, який досліджує розвиток суб’єкта господарювання в динаміці, тобто попередній рівень, сучасний та подальший взаємозв’язок. Таким чином, він має інтегруватися в загальну площину корпоративної культури, підтриманий керівництвом, а згодом доведений до відома кожного працівника суб’єкта господарювання у вигляді загальної ефективної програми подальшого розвитку з окресленням конкретних завдань для виконавців. Ризик-менеджмент як цілісна система керування ризиками має включати дієву програму сучасного контролю за реалізацією визначених завдань, комплексне оцінювання продуктивності запланованих заходів, а також дієву систему мотивації на всіх рівнях підприємства [359, с. 3].

Ключові етапи процесу керування ризиками показані на рисунку 5.2.

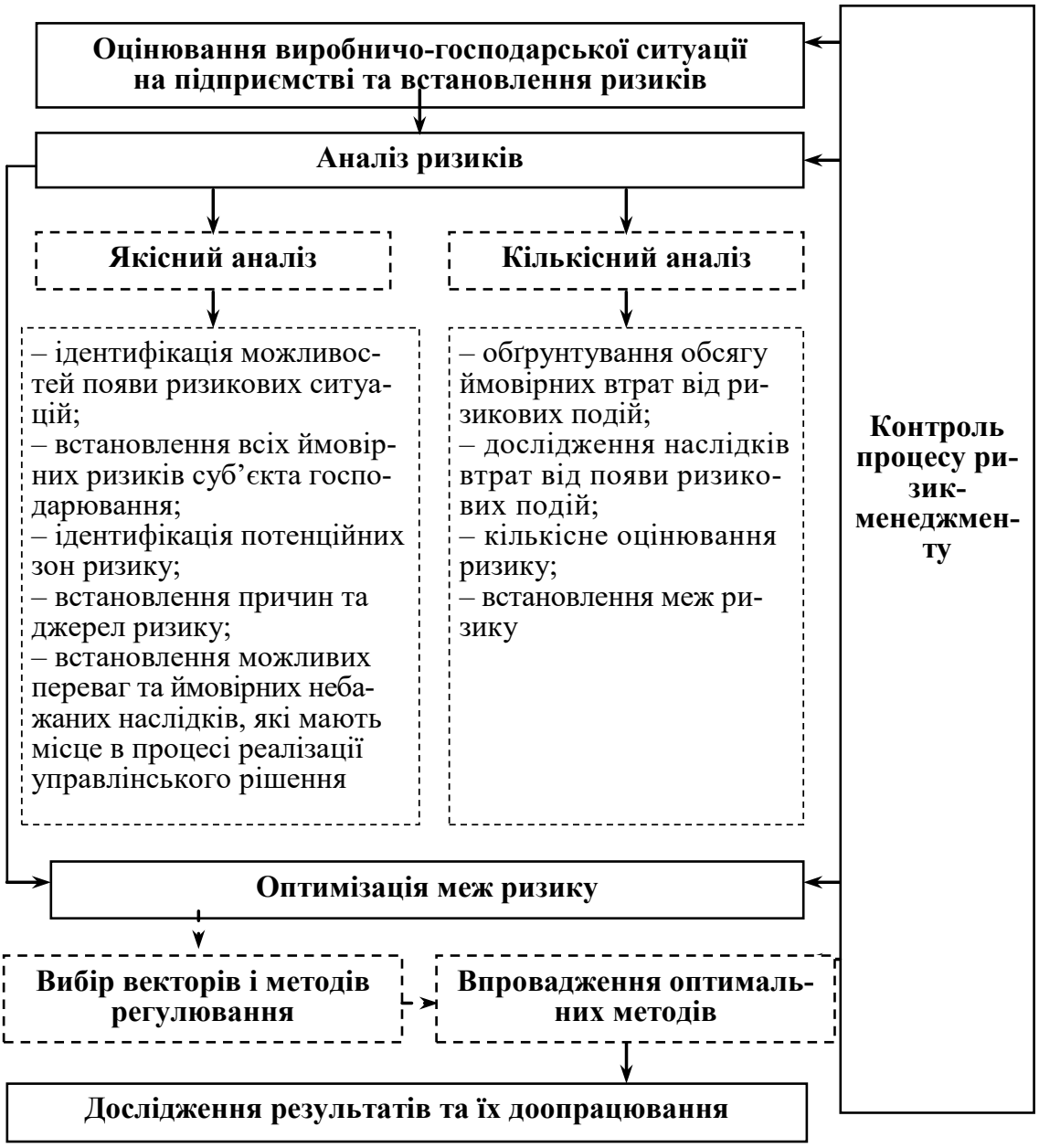

Рисунок 5.2 – Процес управління ризиками на підприємстві

Основна мета дослідження ризику полягає у формуванні та надання ймовірним партнерам потрібного масиву інформації для ухвалення рішення щодо доцільності залучення до роботи над проектом і розробки комплексу заходів щодо захищеності від ймовірних фінансових збитків.

Проведення об'єктивного та якісного аналізу належить до найбільш складних завдань економічної ризикології. Ця робота вимагає використання фундаментальних знань не тільки в площині теорії економіки, фінансів, бізнесу, але й багатьох базових навичок, якими повинен володіти конкурентоспроможний на вітчизняному ринку праці спеціаліст. Важливим також є набір потрібним вмінь та навичок, певний практичний досвід у площині економічної діяльності.

До основних завдань при здійсненні якісного дослідження ризику належить ідентифікація ймовірних різновидів ризику, оцінювання ступеня їх загрози та виокремлення чинників факторів, які формують рівень ризику.

Суттєвим доповненням до об'єктивного аналізу може бути кількісне вираження ризику підприємницької діяльності. Аналіз ризику за допомогою кількісного вираження являє собою числову величину певних різновидів ризиків, а також наявного сукупного ризику цілого напряму виробничо-господарської діяльності. Кількісне відображення ступеня ризику зазвичай не охарактеризувати однозначно. Зважаючи на те, який метод оцінювання ймовірного ризику застосовано, його величина може варіюватись.

З метою кількісного вираження ступеня ризику використовують різні способи: починаючи від досить складного імовірнісного аналізу і завершуючи суб'єктивними суто інтуїтивними. Сьогодні українські управлінці, як правило, доволі часто користуються інтуїтивними методами, опираючись на заслужений авторитет чи накопичений досвід успішних попередників. Тільки частина управлінців вищої ланки здатні дати належне оцінювання ризику на основі застосування економіко-математичних моделей.

Застосовувані методи щодо кількісного оцінювання ризику належать до універсальних, однак вони не завжди дають змогу дати об'єктивне оцінювання. Причинами цього може бути нестача часу, необхідної інформації, відповідної кваліфікації. До того ж, варто брати до уваги те, що існують такі різновиди ризиків, які потребують кардинально іншого підходу щодо їх оцінювання. Традиційно всі наявні методи оцінювання ризику узагальнюють таким чином:

– експертні, які дозволяють встановити ступінь ризику у випадку, коли немає потрібної інформації для проведення доцільних розрахунків або адекватного порівняння, базуються на результатах опитування висококваліфікованих фахівців з подальшим статистично-математичним узагальненням результатів;

– економіко-статистична група включає методи, що використовуються тільки у разі наявності значного масиву статистичних даних для обчислення достовірної кількісної величини ступеня ризику. При цьому визначають середньоквадратичне відхилення, β-коефіцієнт, коефіцієнт варіації та інші;

– розрахунково-аналітичні, спрямовані на обчислення порівняно точного кількісного показника ступеня ризику, ґрунтуючись на внутрішній інформаційній базі безпосередньо суб'єкта господарювання (як правило, використовуються для оцінювання ризику, пов'язаного з неплатоспроможністю та відсутністю фінансової стабільності);

– ідентичні – дозволяють дати оцінювання ступеня ризику за конкретними операціями на базі зіставлення з тотожними, тобто неодноразово виконуваними операціями. Зазвичай для зіставлення беруть як свій, так і запозичений досвід виконання подібних операцій.

5.3 Оцінка ймовірності та впливу ризиків

Оцінка ризиків – це процес визначення ймовірності настання ризику та його впливу на ключові аспекти діяльності підприємства. Метою є встановлення пріоритетів для управління ризиками і розробки відповідних заходів.

До найбільш поширених і певною мірою універсальних способів належить: дослідження доцільності витрат, аналітичний, статистичний, експертне оцінювання тощо.

Змістове наповнення методу дослідження доцільності витрат полягає в тому, що витрати за певним напрямом виробничо-господарської сфери, окремими її складовими характеризуються наявністю різного рівня ризику. Зокрема, рівень ризику за мірою витрат,

пов'язаних перш за все з придбанням сировини, є більш високим, ніж за витратами на оплату праці.

Встановлення рівня ризику за допомогою вивчення доцільності витрат спрямоване на визначення ймовірних сегментів ризику (табл. 5.4). З цією метою стан по кожному елементу витрат зазвичай поділяється на сфери ризику, які формують сектор загальних збитків, у рамках яких чітко визначені збитки менші за граничний рівень допустимого ступеня ризику.

Таблиця 5.4 – Межі ризику в залежності від кризового стану

Сфера діяльності підприємства	Абсолютної стабільності	Нормальної стабільності	Нестабільний стан	Критичний стан	Кризовий стан
Сектори ризику	Безризиковий сектор	Сектор мінімального ризику	Сектор підвищеного ризику	Сектор критичного ризику	Сектор неприйнятного ризику
Максимально можливі збитки	Повна відсутність збитків	Чистий прибуток	Розрахунковий прибуток	Валовий прибуток	Виручка від продажу та майно підприємства
Рівень ризику	0	0–25	25–50	50–75	75–100

До суттєвих переваг зазначеного способу можна віднести те, що, маючи інформацію щодо статті витрат з максимально допустимим ризиком, можливо визначити напрями його зменшення. Зокрема, маючи інформацію про те, що ризик має відношення до оренди транспортного засобу, виникає можливість переглянути питання щодо умов перевезення матеріальних цінностей.

Головною вадою способу є те, що суб’єкт господарювання не дає належного оцінювання потенційних джерел ризику, натомість розцінює ризик як сталу величину, не беручи до уваги його елементів.

Разом з тим, спосіб експертних оцінювань має дещо суб'єктивний характер у порівнянні з альтернативними способами. Такий суб'єктивізм виникає внаслідок того, що команда експертів, яка займається питаннями оцінювання ризику, висловлює власне суб'єктивне бачення щодо попереднього стану та перспектив розвитку.

Як правило, зазначений метод використовується у разі недостатнього обсягу інформації або у випадку встановлення міри ризику даного напряму виробничо-господарської діяльності, який не має аналогів, що не дозволяє здійснити аналіз попередніх даних.

В узагальненому вигляді роль даного способу визначається тим, що суб’єкт господарювання виокремлює певну низку ризиків і досліджує, як саме вони здатні впливати на його виробничо-господарську діяльність. Такий підхід зводиться до визначення бальних критеріїв за вірогідність появи ризику того чи іншого типу, а також до рівня його впливу на діяльність промислового підприємства.

В умовах стійкості внутрішнього та зовнішнього середовища суб’єкта господарювання, потрібного масиву даних про стан певних операцій (виручка та збитки), процесів, векторів економічного пожвавлення застосовують механізми статистичного підходу до оцінювання ризику. Даний підхід базується на теорії ймовірності певного розподілу випадкових величин.

Володіючи достатнім обсягом інформації щодо наявності окремих видів ризику в попередні періоди, товаровиробник спроможний дати оцінку вірогідності появи їх в подальшому.

Для цього обчислюють низку показників. Для встановлення найбільш вірогідного результату, який підприємство очікує отримати, слід обчислити показник математичного очікування M(x):

$$M(x) = \sum_{i=1}^{n} x_i \cdot p_i , \qquad (5.1)$$

де x_i – значення, яких може набувати досліджуваний параметр;

p_i – вірогідність набуття цих значень.

Проте для ухвалення рішення доцільно одночасно встановити діапазон показників, тобто обчислити рівень відхилення показника очікуваного значення від показника середньої величини. З цією метою у практичній діяльності зазвичай використовують два показники, які взаємопов'язані між собою:

– дисперсію D(x):

$$D(x) = \sum_{i=1}^{n} p_i \left(x_i - M(x)\right)^2 ; \qquad (5.2)$$

– середньоквадратичне відхилення σ:

$$\sigma = \sqrt{D(x)}. \qquad (5.3)$$

Якщо показник середньоквадратичного відхилення більший, то більший рівень ризику має управлінське рішення.

У розрахунках застосовують також і коефіцієнт варіації V:

$$V = \frac{\sigma}{M(x)}. \qquad (5.4)$$

Враховуючи коефіцієнт варіації, є можливість зіставити навіть діапазон ознак, які мають різне вираження. Коефіцієнт варіації може коливатись у діапазоні від 0 до 1. У цьому випадку, чим меншим є його значення, тим більшою є стійкість передбачуваної ситуації, і менший рівень ризику певного заходу чи вектора діяльності.

До суттєвих переваг даного способу можна віднести простоту математичних розрахунків, а до значимих недоліків – потреба у значній кількості початкових даних, так як, чим більший обсяг початкових даних, тим більш точними є обчислення. Статистичний спосіб дозволяє здобути найбільш повний обсяг даних щодо ступеня ризику, але не передбачає дослідження джерел виникнення ризику, тобто не враховуються певні елементи ризику.

Аналітичний спосіб дослідження ризику являє собою комплекс статистичних показників на базі попереднього відбору експертами основних характеристик з подальшим

дослідженням впливу чинників ризику на них. Він є поєднанням статистичного обчислення та принципів стосовно експертного аналізу.

Сильними сторонами аналітичного способу є поєднання факторного аналізу показників, які суттєво впливають на ризик, і встановлення доцільних методів зменшення ступеня його прояву.

Дослідження ризику, базуючись на даних про фінансовий стан суб'єкта господарювання, є найбільш популярним способом відносного оцінювання ризику для управлінця вищої ланки та для його ділових партнерів, тому що головними джерелами необхідної інформації є фінансова звітність товаровиробника, перш за все, баланс і звіт про фінансові результати. Фінансовий стан суб'єкта господарювання можна визначити як комплексну категорію, яка визначається системою збалансованих абсолютних і відносних величин, які показують не тільки наявність, але й оптимальне розміщення та ефективне використання фінансових ресурсів промислового підприємства. Вивчення цих показників дає змогу оцінити поточну фінансову стабільність суб'єкта господарювання.

Метод ідентичності застосовується у тому випадку, коли інші відомі способи оцінювання ризику є неприйнятними. Специфіка даного способу визначається тим, що у процесі дослідження рівня ризику певного вектора підприємницької сфери слід застосовувати інформацію щодо розвитку подібних напрямів минулого.

Об'єктивна складність при застосуванні зазначеного способу оцінювання рівня ризику зумовлена тим, що показники попередніх періодів необхідно застосовувати на даний момент не враховуючи те, що будь-який вектор підприємницької діяльності перебуває в постійному розвитку.

5.4 Стратегії управління ризиками

Управління ризиками економічної безпеки – це процес ідентифікації, аналізу, оцінки та реагування на ризики, які загрожують стабільності, ефективності та конкурентоспроможності підприємства. Стратегії управління дозволяють підприємствам мінімізувати вплив ризиків, уникати збитків і забезпечувати стійкість у мінливих умовах (рис. 5.3).

1. Ідентифікація ризику
↓
2. Оцінка ймовірності та впливу
↓
3. Вибір стратегії (уникнення, передача, зниження, прийняття, диверсифікація)
↓
4. Реалізація стратегії
↓
5. Контроль і моніторинг

Рисунок 5.3 – Вибір стратегії управління ризиками

Після дослідження та оцінювання ідентифікованих ризиків цілком логічно виникає необхідність вибору шляхів зменшення ризику, тобто зведення до мінімуму ймовірних втрат під час проведення тих чи інших операцій.

Міжнародний досвід містить велику кількість різноманітних та оригінальних методів зменшення проявів ризику, найбільш популярним з яких є: страхування; передача ризику; диверсифікація; отримання додаткового масиву актуальної інформації; бізнес-планування; лімітування; дотримання стандартів якості виготовленої продукції; ретельна перевірка ділових партнерів; забезпечення захищеності комерційної діяльності промислового підприємства; кваліфікований підбір кадрів для суб'єкта господарювання.

Головні підходи щодо зменшення ризиків та їх змістове наповнення представлені в таблиці 5.5.

Таблиця 5.5 – Механізми мінімізації ризиків

№ п/п	Механізм мінімізації	Сутність способу
1	2	3
1.	Запобігання ризикам – найбільш ефективний метод	а) відмова від здійснення певних господарських операцій, ступінь ризику за якими досить значний і не повною мірою узгоджується з фінансової політикою суб'єкта господарювання; б) зменшення частки запозичених коштів у виробничо-господарському обігу дає змогу запобігти втрату фінансової стабільності; в) підвищення ліквідності наявних активів шляхом зростання обігових засобів у загальному масиві дає змогу запобігти ризику неплатоспроможності
2.	Мінімізація ризиків – застосовується у випадку, коли їх уникнути неможливо	а) одержання від споживача гарантій щодо своєчасної сплати боргу; б) звуження переліку необґрунтованих форс-мажорних ситуацій у договорах із контрагентами, що дасть змогу посилити фінансову відповідальність за недобросовісне виконання договірних обов'язків, тобто зменшити комерційний ризик
3.	Диверсифікація ризиків – дає змогу зменшити рівень зосередженості ризиків	а) диверсифікація сфер діяльності дозволяє використати додаткові можливості отримання виручки та прибутку від різнопланових фінансово-господарських операцій; б) диверсифікація постачальників продукції передбачає налагодження зв'язків з багатьма партнерами з метою постачання головної номенклатури товарів; в) диверсифікація наявних товарів для реалізації – внесення до асортименту промислового підприємства продукції з протилежним попитом у межах певних товарних груп, що дає змогу знизити ризик у разі погіршення кон'юнктури визначеного товарного ринку; г) диверсифікація депозитних заощаджень полягає в розміщенні наявних тимчасово вивільнених грошових активів для депозитного зберігання в кількох банках

Продовження таблиці 5.5

1	2	3
4.	Обмеження ризиків за операціями, які мають властивість систематично виходити за допустиму межу ризику; такий ризик обмежується за допомогою впровадження відповідних фінансово-економічних стандартів	а) максимально можливий обсяг комерційної операції, спрямованої на придбання товарів у разі здійснення її з одним і тим же контрагентом; б) прийнятний обсяг використання запозичених коштів у фінансово-господарському обігу; в) максимально допустимий обсяг депозитного вкладу, розміщеного в одній комерційній банківській установі тощо

З метою мінімізації ризиків менеджерам доцільно складати програму керування ризиками, яка поєднує механізм формування чи коригування доцільних процедур ризик-менеджменту на промисловому підприємстві. З метою обґрунтування доцільності розробки програми керування ризиками необхідно визначити значимість внутрішніх загроз на сферу діяльності суб'єкта господарювання, які зазвичай становлять близько 75% від наявних ризиків, які мають відчутний вплив на функціонування промислового підприємства.

Розроблені керівництвом програми мінімізації непрогнозованих ризиків потрібно корелювати з інноваційними можливостями. Безпосередньо, відновлення та процес модернізації певного підприємства має спрямовуватись на мінімізацію ризиків нещасних випадків, завдання певної екологічної шкоди тощо.

Формування програми керування ризиками здійснюється у два етапи. Підготовчий етап складання програми керування ризиками включає вивчення довідково-інформаційної бази, яка має відношення до окресленої проблеми. Це дозволяє схвалити нагальні рішення перед наступним – основним – етапом і перейти безпосередньо до розробки й узгодження програми керування ризиками.

Головний етап розробки програми керування ризиками містить узагальнення актуальної інформації щодо можливих ризиків, від яких суб'єкт господарювання відмовився на стадії попереднього відбору, формування плану впровадження запобіжних заходів та урахування усіх ймовірних ризиків та існуючих механізмів керування ними. Програма керування ризиками має спиратись на дані про ключові особливості ризиків і максимально вірогідні, найбільш ймовірні та прогнозовані збитки.

Отже доцільно запропонувати програму керування захищеністю від ризиків, яка містить конкретні заходи, характеризує наявні ризики та важелі нейтралізації їх проявів (табл. 5.6):

Таблиця 5.6 – Зміст орієнтовної програми керування захищеністю від ризиків

Розділи	**Обсяг, сторінок**
1	2
Резюме для менеджерів вищої ланки	1
Виокремлення ризиків галузі	4–5
Характеристика діяльності товаровиробника	4–5
Дослідження найбільш ризикових ділянок	2–3

Продовження таблиці 5.6

1	2
Контекст ймовірного ризику: головна місія, стратегічна й тактична мета підприємства, очікувані збитки тощо	3–4
Вірогідні ризики товаровиробника	3–5
Оцінювання ризику	3–5
Механізми впливу на можливі ризики	3–5
Продуктивність	1
Додатки (структура керування ризиками, фінансова звітність тощо)	5–10

З метою запобігання ризикам, потрібно чітко уявляти їх повну картину. Діагностувати наявні ризики слід в кількох площинах, що дасть змогу повною мірою охарактеризувати загальний стан загроз. Насамперед дається оцінювання середовищу, в якому виникають ризики: природні умови, виробництво, соціально-політична ситуація, економічна кон'юнктура, персонал та ін.

Аналіз ризиків повинен виконуватись з дотриманням логічної послідовності:

1. За допомогою залучення експертів визначаються чинники ризиків, які найбільш суттєво впливають на реалізацію промисловим підприємством мети в різних площинах промислової сфери: стратегічній, виробничо-збутовій, фінансовій та ін. Зазвичай це має такий вигляд: експертом аналізуються дані за всіма показниками, робляться висновки щодо ймовірного впливу на рівні підприємства та держави на реалізацію головної мети суб'єкта господарювання (виробнича сфера, фінансова сфера, логістика, персонал тощо). До чинників ризику можна віднести: запровадження нової нормативно-правової бази (політичний чинник ризику), збільшення рівня інфляції прогнозованої величини (економічний), не прогнозовані кліматичні зміни тощо.

2. Окреслюються ризики, зокрема: загроза збільшення кредитної ставки внаслідок ймовірного підвищення річного показника інфляції понад 10% річних (фінанси) чи ризик зменшення обсягів реалізації у зв'язку з ймовірним розширенням пропозиції на ринку збуту. Зважаючи на обмежену інформацію у таблиці 1.9 та значний масив ризиків (орієнтовно 80–120 ризиків, за оцінюваннями експертів, по 10–15 ризиків на конкретну сферу діяльності підприємства), в клітинках можна ставити умовні (скорочені) позначки.

Надалі ризики доцільно розділити на такі групи: за частотою появи, за масштабністю наслідків тощо. Вірогідність появи ризику та ймовірних наслідків (вагомість ризику) теж визначаються експертами. Передусім варто вирішити, за якою шкалою давати оцінку проявам ризиків та їх вірогідності. Найбільш прийнятним є застосування трирівневої дев'ятибальної шкали оцінювання. Для ймовірних наслідків: не дуже значні (1–3), помірні (4–6); суттєві (7–9 балів). Для вірогідності події: низька вірогідність (1–3); середня вірогідність (4–6); висока вірогідність (7–9). Для якості керування: низький рівень якості (7–9); середній рівень якості (4–6); високий рівень якості (7–9).

Кожен суб'єкт господарювання сам визначає для себе показники значимості наслідків і вірогідності події. Зокрема, якщо товаровиробник може зазначити збитків, які корелюються з активами, то результати можна визначити як суттєві, оцінивши їх в межах 7–9 балів. Щодо вірогідності, то роль критерію виконує частота зіткнення промислового підприємства з певним чинником ризику. В той же час, якщо за весь період роботи промислового підприємства не було випадків впливу на нього природних катаклізмів, і в майбутньому вони

не очікуються, то вірогідність цього вкрай низька, і її оцінка знаходиться в межах 1–3 бали. Отримані результати оцінювання ризиків доцільно звести в таку таблицю 5.7.

Таблиця 5.7 – Узагальнені дані частково встановлених ризиків

Визначення ризику	Обсяг ймовірного збитку	Чинник ризику	Бальна оцінка ризику:			
			вірогідності події	наслідків події	якості керування ризиком	інтегральна оцінка (гр. 4+5+6)
Ризик збільшення кредитної ставки на придбання основних засобів у зв'язку з ймовірного збільшення річного показника інфляції понад 10%	Х тис. грн	Рівень інфляції понад 10%	6	4	8	18

Запропонований підхід можна доповнити, виходячи зі специфіки діяльності суб'єкта господарювання, зокрема при плануванні заходів щодо керування ризиками доцільно розробити комплекс кроків, спрямованих на зниження обсягів або вірогідності збитків від певного ризику. Слід також сформувати цільові критерії та рівень оцінки успішності керування ризиком, визначити ієрархію наявних ризиків, термін отримання результату та його відповідність очікуваному, визначити коло відповідальних осіб (таблиця 5.8).

Таблиця 5.8 – Планування процесом керування ризиками

Характе-ристика ризику	Положення на карті ризиків	Заходи щодо керування ризиком	Вимірювання успішності керування	Відповідальні особи
	Зазначення ієрархії Обсяг ймовірних втрат Найближче оточення	Опис заходу Витрати на реалізацію заходу Послідовність заходів	Узгодженість між очікуванням і реальністю	

Запровадження на промисловому підприємстві такого механізму керування ризиками виявляється менш продуктивним, ніж у разі, коли в його структурі створено спеціальний відділ, який вирішує питання, пов'язані з загрозами, оскільки фахівці цих структурних підрозділів набагато ефективніше знижують чутливість суб'єкта господарювання до прояву наявних ризиків.

Зазвичай завдання щодо керування ризиками на промислових підприємствах покладені на спеціальні структурні підрозділи. У разі, якщо в інфраструктурі промислового підприємства такого підрозділу не передбачено, то керівництво може прийняти рішення щодо залучення штатних фахівців з ризик-менеджменту чи зовнішніх консультантів. Однак, як показує досвід, доволі часто функції керування ризиками покладаються на інші структурні підрозділи. Зазвичай ці завдання можуть виконуватись відділом внутрішнього аудиту, службою контролінгу, прогнозно-аналітичним підрозділом. У такому становищі загрози своєчасно діагностуються, а їх наслідки оперативно усуваються, що захищає

товаровиробника від ймовірних суттєвих втрат.таким чином ми підходимо до загального розуміння стратегій управління ризиками (табл. 5.9).

Таблиця 5.9 – Порівняння стратегій управління ризиками

Стратегія	**Переваги**	**Недоліки**	**Приклад використання**
Уникнення	Повне усунення ризику	Втрата потенційних вигод	Відмова від інвестицій у ризиковані проекти
Передача	Мінімізація втрат	Додаткові витрати	Страхування активів
Зниження	Зменшення впливу ризику	Висока вартість реалізації	Встановлення антивірусного ПЗ
Прийняття	Мінімальні витрати	Можливість втрат	Прийняття незначних валютних коливань
Диверсифікація	Розподіл ризику	Складність реалізації	Інвестиції у кілька проектів

Застосування ефективних стратегій управління ризиками є ключовим для забезпечення економічної безпеки підприємства. Кожна стратегія має свої переваги й недоліки, тому її вибір залежить від специфіки ризику та ресурсів підприємства. Впровадження комплексного підходу до управління ризиками сприяє збереженню стабільності, підвищенню конкурентоспроможності та довгостроковому успіху бізнесу.

Перелік питань:

1. Що таке ризики економічної безпеки підприємства, і які вони мають характеристики?
2. Як класифікуються ризики у сфері економічної безпеки підприємства?
3. У чому полягає відмінність між внутрішніми та зовнішніми ризиками?
4. Які існують основні методи ідентифікації ризиків на підприємстві?
5. Поясніть сутність методу SWOT-аналізу та його використання для оцінки ризиків.
6. Як застосування сценарного аналізу допомагає у прогнозуванні ризиків?
7. Яка роль експертних оцінок у процесі ідентифікації ризиків?
8. Чим відрізняється статистичний аналіз ризиків від інших методів?
9. Що таке мапа ризиків, і як її створення сприяє управлінню ризиками?
10. Як оцінюється ймовірність настання ризиків у сфері економічної безпеки?
11. Які ключові параметри використовуються для оцінки впливу ризиків?
12. У чому полягає значення матричного підходу до аналізу ризиків?
13. Як визначити пріоритетність ризиків для ефективного управління ними?
14. Опишіть процес ранжування ризиків і його значення для підприємства.
15. Які основні стратегії управління ризиками існують, і як їх правильно обирати?
16. Що включає стратегія уникнення ризиків, і коли вона є доцільною?
17. Як працює стратегія передачі ризиків, і які її переваги?
18. У чому сутність стратегії зниження ризиків, і як вона реалізується?
19. Що таке стратегія прийняття ризиків, і в яких ситуаціях її слід застосовувати?
20. Як диверсифікація допомагає підприємствам зменшувати ризики?

Тести:

1. **Що є основною метою оцінки ризиків у сфері економічної безпеки?**
   а) Прогнозування змін у макроекономічному середовищі;
   б) Розробка механізмів мінімізації загроз;
   в) Оптимізація бізнес-процесів;
   г) Ідентифікація сильних сторін підприємства.

2. **Який метод аналізу ризиків передбачає використання історичних даних?**
   а) SWOT-аналіз;
   б) Метод експертних оцінок;
   в) Статистичний аналіз;
   г) Матричний метод.

3. **Який з перелічених підходів використовується для визначення пріоритетності ризиків?**
   а) Фінансовий аналіз;
   б) Ранжування ризиків;
   в) Використання програмного забезпечення;
   г) Моніторинг бізнес-процесів.

4. **Що є основним результатом сценарного аналізу?**
   а) Розробка стратегії зниження ризиків;
   б) Побудова моделі потенційних ситуацій;
   в) Проведення фінансового аудиту;
   г) Оцінка ринкових можливостей.

5. **Що таке мапа ризиків?**
   а) Інструмент для створення бізнес-плану;
   б) Графічне зображення ризиків за їхнім рівнем ймовірності та впливу;
   в) Список ризиків, згрупованих за сферами діяльності;
   г) Інформаційна система для управління ризиками.

6. **Який із методів дозволяє визначити слабкі місця у внутрішніх процесах підприємства?**
   а) Діагностика бізнес-процесів;
   б) Метод мозкового штурму;
   в) Статистичний аналіз;
   г) SWOT-аналіз.

7. **Що є ключовим параметром матричного методу оцінки ризиків?**
   а) Прибутковість бізнесу;
   б) Ймовірність і вплив ризику;
   в) Швидкість реагування на загрози;
   г) Кількість залучених ресурсів.

8. **Який підхід передбачає передачу ризиків іншій стороні?**
   а) уникнення ризиків;
   б) прийняття ризиків;
   в) передача ризиків;
   г) контроль ризиків.

9. **У чому полягає стратегія зниження ризиків?**
   а) повна відмова від діяльності, пов’язаної з ризиками;
   б) вживання заходів для мінімізації ймовірності або впливу ризику;
   в) використання сторонніх сервісів для управління ризиками;
   г) розширення фінансового резерву.

10. **Що включає процес управління ризиками?**
    а) ідентифікація, оцінка, контроль та реагування;
    б) лише ідентифікацію ризиків;
    в) розробку бізнес-плану;
    г) моніторинг роботи персоналу.

11. **Який із методів найкраще підходить для оцінки впливу валютних коливань на підприємство?**
    а) SWOT-аналіз;
    б) статистичний аналіз;
    в) мозковий штурм;
    г) експертні оцінки.

12. **Яка стратегія управління ризиками передбачає прийняття ризику?**
    а) контроль ризику;
    б) уникнення ризику;
    в) прийняття ризику;
    г) диверсифікація ризиків.

13. **Що є прикладом передачі ризиків?**
    а) встановлення резервних серверів;
    б) страхування майна підприємства;
    в) відмова від інвестицій у ризиковані проекти;
    г) розробка антикризових заходів.

14. **Що означає стратегія уникнення ризиків?**
    а) використання сторонніх платформ для управління ризиками;
    б) відмова від діяльності, яка створює високий ризик;
    в) розподіл фінансових ресурсів на кілька проектів;
    г) встановлення системи раннього попередження.

15. **Що таке диверсифікація ризиків?**
    а) аналіз впливу ризику на доходи підприємства;
    б) розподіл активів для мінімізації залежності від одного джерела;
    в) зменшення ймовірності ризиків шляхом їхньої передачі;
    г) використання аналітичних систем для моніторингу загроз.

16. **Яка стратегія управління ризиками застосовується, якщо підприємство приймає ризик без додаткових дій?**
    а) уникнення ризиків;
    б) передача ризиків;
    в) прийняття ризиків;
    г) зниження ризиків.

17. **Що є результатом ефективного контролю ризиків?**
    а) зниження ймовірності виникнення ризиків;
    б) повна відмова від ризикованих проектів;
    в) підвищення витрат підприємства;
    г) зниження прибутковості.

18. **Який із методів управління ризиками дозволяє мінімізувати наслідки кіберзагроз?**
    а) використання резервного копіювання;
    б) прийняття ризиків;
    в) диверсифікація ризиків;
    г) передача ризиків.

19. **Що є ключовим етапом у виборі стратегії управління ризиками?**
    а) проведення SWOT-аналізу;
    б) оцінка витрат і вигод;
    в) моніторинг бізнес-процесів;
    г) розробка фінансових звітів.

20. **Який із підходів використовується для зменшення ймовірності ризиків?**
    а) прийняття ризиків;
    б) уникнення ризиків;
    в) зниження ризиків;
    г) передача ризиків.

Практичні завдання:

Завдання 1. Ідентифікація ризиків підприємства

Мета: Навчитися визначати ризики на основі внутрішніх та зовнішніх факторів.

1. Ознайомтеся із ситуацією:
   Підприємство спеціалізується на експорті продукції до регіонів із високим рівнем

політичної нестабільності. Ідентифікуйте внутрішні та зовнішні ризики, пов'язані з такою діяльністю. Розподіліть ризики за категоріями (економічні, політичні, технологічні, соціальні).

2. Заповніть таблицю:

Ризик	Категорія	Джерело виникнення

Завдання 2. Аналіз бізнес-процесів для виявлення ризиків

Мета: Виявити внутрішні ризики через аналіз бізнес-процесів.

1. Оцініть бізнес-процеси підприємства:
   - виробництво продукції;
   - логістика постачань;
   - управління персоналом.
2. Для кожного процесу визначте потенційні загрози та ймовірність виникнення загроз.
3. Представте результати у вигляді схеми "Вхід → Процес → Вихід" із зазначенням ризиків на кожному етапі.

Завдання 3. Побудова мапи ризиків

Мета: Візуалізувати ризики за їхньою ймовірністю та впливом.

1. Виберіть наступні ризики:
   - валютні коливання;
   - кібератаки;
   - збої у постачаннях сировини;
   - політична нестабільність.
2. Побудуйте мапу ризиків, використовуючи матрицю:
   - X-вісь: Ймовірність виникнення.
   - Y-вісь: Вплив на підприємство.
3. Зробіть висновок які ризики потребують негайної уваги, а які є прийнятними.

Завдання 4. Оцінка впливу ризиків

Мета: Навчитися оцінювати вплив ризиків на фінансові показники підприємства.

1. Припустимо, що підприємство зазнає таких ризиків:
   - зменшення продажів через валютні коливання (ймовірність — 60%, вплив — 30% доходу);
   - пошкодження обладнання через техногенну аварію (ймовірність — 10%, вплив — 50% активів).
2. Для кожного ризику обчисліть:
   - ймовірність реалізації ризику (%).
   - потенційні втрати в грошовому еквіваленті.
3. Представте результати у вигляді таблиці:

Ризик	Ймовірність	Вплив	Потенційні втрати

Завдання 5. Розробка стратегії управління ризиками

Мета: Визначити ефективну стратегію для кожного типу ризику.

1. Використайте наступні ризики:
   - Кібератаки;
   - політична нестабільність;
   - збільшення витрат на сировину.
2. Для кожного ризику запропонуйте стратегію управління (уникнення, передача, зниження, прийняття).
3. Поясніть вибір стратегії для кожного ризику.

Завдання 6. Практичний кейс: Управління ризиком валютних коливань

Мета: Використати теоретичні знання для вирішення реальної проблеми.

1. Ситуація: Підприємство закуповує матеріали за іноземну валюту, і курс валюти значно коливається.
   - визначте основні ризики, пов'язані з валютними коливаннями;
   - запропонуйте стратегію управління цим ризиком.
2. Розробіть план дій, включаючи:
   - використання фінансових інструментів (наприклад, хеджування);
   - розподіл закупівель між різними постачальниками.

Завдання 7. Оцінка ефективності управління ризиками

Мета: Навчитися аналізувати ефективність реалізованих заходів.

1. Припустимо, що підприємство впровадило такі заходи:
   - страхування активів;
   - встановлення системи моніторингу кіберзагроз;
   - проведення тренінгів для персоналу.
2. Оцініть ефективність заходів за такими критеріями:
   - скорочення частоти виникнення ризиків.
   - зменшення фінансових втрат.
   - підвищення рівня обізнаності персоналу.
3. Запропонуйте додаткові заходи для покращення управління ризиками.

ТЕМА 6. ФІНАНСОВА БЕЗПЕКА ПРОМИСЛОВОГО ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

6.1 Поняття фінансової безпеки.

6.2 Методи оцінки фінансової стабільності.

6.3 Управління фінансовими ризиками.

6.4 Захист активів підприємства та роль контролінгу у цьому процесі.

6.1 Поняття фінансової безпеки

Визначення фінансової безпеки

В основі фінансово-господарської діяльності будь-якої підприємницької структури лежать фінанси, доцільно питання фінансово-економічної захищеності підприємства виділити окремим блоком. Поняття фінансово-економічної захищеності підприємства інтегрує в собі такі категорії, як економічна захищеність суб'єкта господарювання та фінанси підприємства, що дають можливість глибше його вивчити з метою визначення можливості впливу на загальний стан розвитку підприємства.

Основна мета фінансової захищеності суб'єкта господарювання полягає в його здатності самостійно розробляти й впроваджувати ефективну фінансову стратегію відповідно до поставлених цілей в умовах ризику й значної кількості конкурентів в межах фінансової захищеності підприємства загалом.

Фінансова захищеність підприємства – це здатність суб'єктів підприємництва реалізовувати свою господарську, зокрема фінансову діяльність, результативно і ритмічно протягом усього періоду функціонування підприємства за допомогою використання певної сукупності взаємопов'язаних методів та заходів фінансового характеру, покликаних оптимізувати застосування фінансових ресурсів з метою забезпечення належного їх рівня та зменшити вплив різноманітних ризиків підприємницького середовища.

Зазначимо основні характеристики небезпек фінансовій захищеності суб'єкта господарювання. Зазвичай, такі небепеки мають неупереджену природу та найбільш властива для підприємств саме в умовах функціонування ринкової економіки. Вона супроводить переважну більшість фінансових операцій та векторів фінансової сфери будь-якого суб'єкта господаювання. Неупереджений характер загрози захищеності проявляється незважаючи на те чи, враховується вона суб'єктами формування фінансової безпеки чи ні.

Як неупереджене явище небезпека фінансовій захищеності є формою виразу протиріч між фінансовою зацікавленостю суб'єкта господаювання та його зовнішньо фінансовим осередком.

Джерелом небезпек є певні від'ємні фактори й умови діяльності фінансової системи суб'єкта господаювання: це зазвичай може бути один фактор або ж їхня сукупністьВ той же час осередком загрози є не відємний фактор, а деструктивна його дія на наявні можливості запровадження певної фінансової зацікавленості суб'єкта господаювання і забезпечення його належної фінансової захищеності. Така відємна дія фактора має вірогіднісний характер, це безумовна ознака будь-якої загрози фінансовій захищеності суб'єкта господаювання. В результаті від'ємного впливу загрози її дія наносить прямий або непрямий збиток суб'єкту господаювання. Зазначена втрата може мати форму очевидної або непрямо втрати.

Основні загрози фінансової захищеності підприємства, їх вплив, джерела та основні завдання її забезпечення надано на рисунку 6.1.

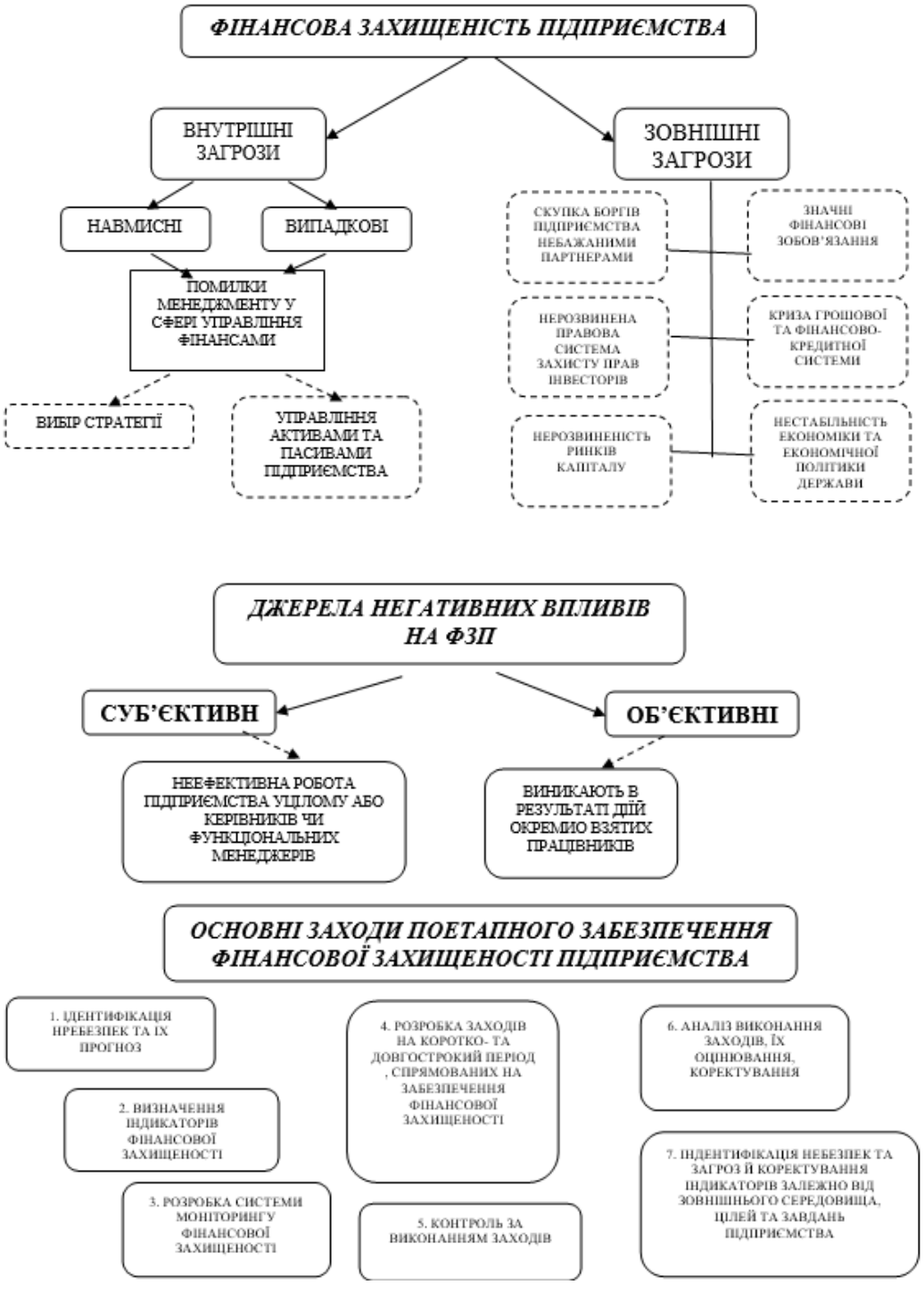

Рисунок 6.1 – Основні загрози фінансової захищеності підприємства, їх вплив, джерела та основні завдання її забезпечення

Доцільно наголосити, що дефініція фінансового ризику у площині формування фінансової захищеності охоплює дві важливих складові, а саме:

1) виявлення й оцінювання (має експертний, ймовірнісний характер);

2) управління фінансовим ризиком.

Фінансовий ризик виступає перш за все як імовірна загроза невдачі дій, що вживаються відносно забезпечення фінансової захищеності суб'єкта господарювання.

З цього випливає, що пріоритетним завданням керуваіння фінансовими ризиками повинно бути забезпечення фінансової захищеності суб'єкта господаювання в ході його діяльності і розвитку тапопередженню падіння його ринкової ціни. Саме у цьому полягає методологічний зв'язок фінансового ризику і фінансової захищеності на рівні суб'єкта господаювання (рис.6.2).

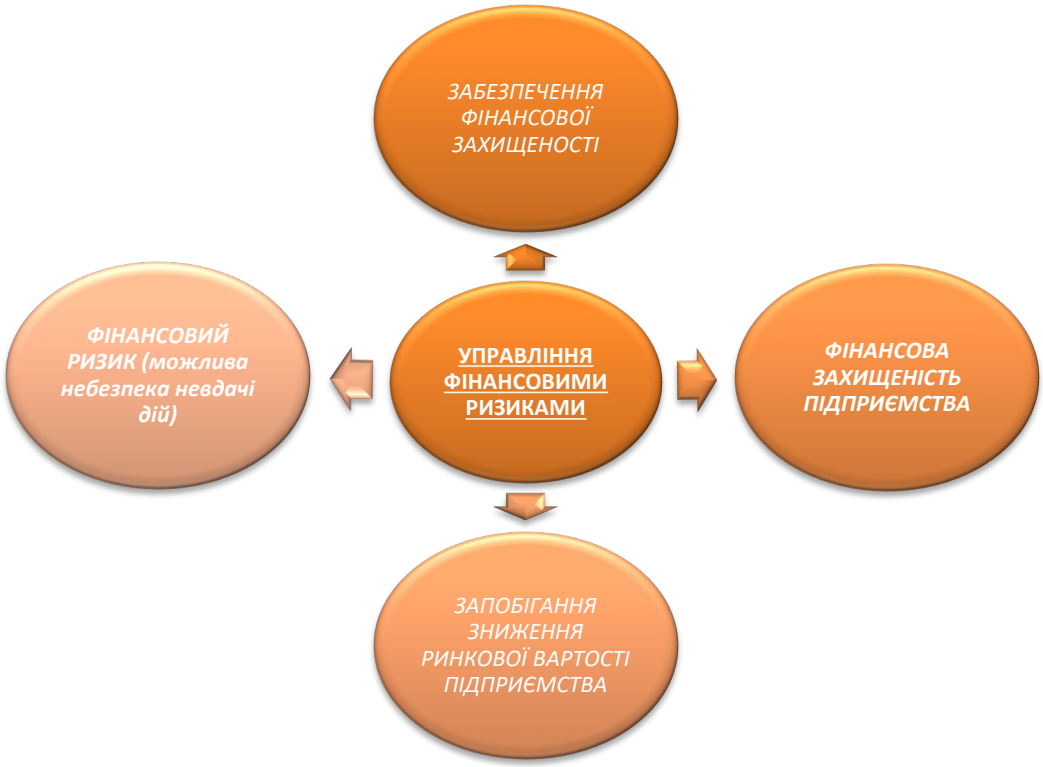

Рисунок 6.2 – Методологічний зв'язок фінансового ризику та фінансової захищеності підприємства

Загрози фінансовій захищеності дуже різноманітні і з метою їх повної і точної ідентифікації потребують класифікації (рис. 6.3).

Рисунок 6.3 – Класифікація ознак загроз фінансовій захищеності підприємства

Економічна захищеність є пріоритетним завданням суб'єкта господарювання, оскільки вона визначає стабільність функціонування підприємства, без цього суб'єкт підприємницької діяльності може збанкротувати. Тобто економічна захищеність відіграє значну роль при побудові фінансово-господарського механізму. Економічну захищеність можна розглядати, в свою чергу, як систему, що складається з таких підсистем (рис. 6.4).

Рисунок 6.4 – Структура фінансового захисту підприємства

Фінансова безпека – це ключовий елемент економічної стабільності підприємства, який дозволяє мінімізувати вплив ризиків і забезпечити сталий розвиток. Її підтримка потребує комплексного підходу, що охоплює аналіз ключових показників, врахування факторів впливу та розробку заходів щодо управління фінансами.

6.2 Методи оцінки фінансової стабільності

Нагальні питання оцінювання економічної безпеки підприємств, обґрунтування сучасних підходів до її формування, напрацювання шляхів втілення нових технологічних рішень в господарській діяльності, окреслення оптимальних напрямів її створення є актуальними та зумовлюють потребу в осмисленні зазначеного процесу на належному науково-теоретичному рівні з відповідним підґрунтям. Розв’язання цих питань вимагає спільної злагодженої роботи спеціалістів різних профілів: економістів, юристів, психологів та ін., які спеціалізуються на проблемах економічної захищеності.

Швидкоплинність ринкового середовища висуває до керівництва кожного промислового підприємства вимоги щодо систематичного внутрішнього самооцінювання, а також безпосереднього прогнозування ймовірних змін у загальному рівні його економічної захищеності, тобто здійснення дослідження стану системи економічної безпеки.

Дослідження економічної захищеності має сприяти:

– диференціації зовнішніх і внутрішніх впливів, які ймовірно матимуть негативний вплив на основні показники роботи промислового підприємства;

– окресленню та постійному відстеженню факторів, посилюючи економічну стабільність у короткостроковому та довгостроковому періоді;

– встановленню комплексу індикаторів та методів, які дають змогу встановити вплив цих показників на стан економічної захищеності;

– формуванню належної системи послідовних кроків, покликаних сприяти оптимізації існуючої системи економічної захищеності промислового підприємства

– обґрунтування критеріїв і межових значень найбільш значимих характеристик загального стану системи економічної захищеності.

Під критерієм економічної захищеності слід мати на увазі таку ознаку, на підставі якої можна обґрунтувати висновок, чи знаходиться промислове підприємство в стані належної економічної захищеності.У змістовому значенні зазначений показник є найсуттєвішою відмінною рисою, мірою відображення, а також дослідження якісних параметрів економічної захищеності.

Певний критерій, як форма оцінювання, показує очікуваний стан промислового підприємства в площині його економічної захищеності, в той час, як інші характеристики дають уявлення про здобутий рівень. Наслідком цього в наукових розробках акцентується увага на нормативній природі показників економічної захищеності, які визначають основні принципи та підходи до визначення стану системи економічної захищеності.

Таким чином, сам по собі критерій – це ширша дефініція порівняно з показниками. Зазвичай за наявністю певного критерію ймовірний цілий набір окремих показників. Водночас ці поняття доволі тісно взаємопов’язані: належним чином вмотивований вибір критерію обумовлює цілу низку певних показників, в той же час якісні параметри показників характеризуються тим, наскільки об’єктивно та повно їх окреслює зазначений критерій.

Визначення ключового критерію є основною, найвідповідальнішою фазою дослідження економічної захищеності суб'єкта господарювання. В наукових джерелах надані різноманітні підходи та методи до оцінювання рівня економічної безпеки (рис. 6.5):

Рисунок 6.5 – Основні підходи та методи оцінювання рівня економічної безпеки підприємства

– індикаторний підхід – загальний стан економічної захищеності характеризується наявною системою певних індикаторів, які виражають міру відповідності межовим (нормативним) показникам функціонування суб'єкта господарювання в різноманітних площинах. Стан економічної захищеності промислового підприємства характеризується порівнянням наявних і стандартних показників.

Індикаторний підхід в основному залежить від формування відповідних порогових значень, що знаходяться у певній залежності від стану середовища, на яке суб'єкт господарювання зазвичай не впливає, а лише пристосовується до його умов. Окрім того, досить складно встановити для товаровиробника дані порогові значення, до того ж, вони є досить різними для певного окремо взятого суб'єкта господарювання. За такого підходу рівень економічної захищеності визначають в результаті співставлення отриманих показників роботи промислового підприємства з відповідними індикаторами. Проте для даний підхід ставить питання стосовно бази для визначення обраних індикаторів, їх складу та визначення певного порогового рівня.

Комплекс індикаторів економічної захищеності, який є критеріальним підґрунтям, повинен брати до уваги такі умови:

– по-перше, ймовірність застосування основних параметрів підприємства;

– по-друге, комплекс показників має корелюватися з наявною системою як статистичного обліку, так і з підходами до прогнозування та планування;

– по-третє, здатність застосування наявних індикаторів для аналізу стану економічної захищеності та передбачення ймовірних впливів чинників, які формують економічну захищеність.

З метою формування комплексу показників економічної безпеки слід запропонувати таку класифікацію:

1. Індикатори критеріального характеру, на підставі яких можна обґрунтувати наявний стан економічної захищеності.

2. Індикатори, що безпосередньо визначають критерії економічної захищеності.

3. Індикатори, які непрямо визначають стан економічної захищеності або демонструють її роль у обґрунтуванні загального стану суб'єкта господарювання.

Запропонована класифікація дозволяє встановити стан сучасного реального сегменту економіки, визначити міру ризику інвестування у певну сферу, а також об'єктивно окреслити цільові настанови, потрібні для усунення чинників, що мають вплив на формування економічної захищеності бізнесу.

Оптимальний стан економічної захищеності досягається тоді, коли наявний комплекс індикаторів знаходиться в межах допустимості, а реальні показники одних індикаторів забезпечуються без шкоди іншим. Економічна безпека має піддаватися вимірюванню. Виходячи з цього, потрібно обґрунтувати ефективну систему індикаторів економічної захищеності, яка формує критеріальну базу;

– ресурсно-функціональний підхід – стан економічної захищеності характеризується головними функціональними ознаками, які окреслюють продуктивність застосування наявних корпоративних ресурсів у певних функціональних площинах суб'єкта господарювання з метою уникнення негативної дії ймовірних загроз.

Ресурсно-функціональний підхід до визначення рівня економічної захищеності включає такі методи:

а) вимір стану економічної захищеності на основі оцінювання рівня використання наявних ресурсів за спеціальними критеріями – власні, залучені та позичкові ресурси;

б) оцінювання рівня виконання функцій – забезпечення високої економічної ефективності діяльності підприємства, його стабільності та незалежності. Такий підхід є дуже широким, оскільки, по-перше, у цьому разі процес забезпечення економічної захищеності ототожнюється фактично з усією діяльністю промислового підприємства і, по-друге, зводиться до оцінювання використання ресурсів на підприємстві.

Ресурсно-функціональний підхід передбачає проведення оцінювання економічної захищеності за рахунок ефективності використання ресурсів підприємства. При цьому оцінювання рівня економічної захищеності підприємства ототожнюється з аналізом стану його фінансово-господарської діяльності. Переваги цього підходу – його комплексний характер, проте економічна захищеність підприємства розглядається надто детально і ототожнюється із самою діяльністю підприємства;

– програмно-цільовий підхід – передбачає дослідження економічної захищеності на основі комплексних характеристик у контексті декількох рівнів ієрархії, тобто застосування кластерного, багатоаспектного аналізу та ін. Програмно-цільовий підхід базується на інтегруванні показників, які визначають рівень економічної захищеності підприємства. Значну увагу при його використанні приділяють відбору показників та визначенню методів їх інтегрування;

– відтворювальний підхід – характеристикою стану економічної захищеності слугує обсяг прибутку, що має суб'єкт господарювання завдяки збалансованості власних потреб із потребами сторонніх суб'єктів господарювання. Стан економічної захищеності встановлюється на підставі порівняння витрат на розвиток підприємництва, тобто мається на увазі реінвестований прибуток, і витрат, потрібних для досягнення оптимального рівня наявної економічної захищеності.

– інституційний підхід передбачає такий стан економічної захищеності підприємства, за якої сукупність ресурсів та корпоративних можливостей гарантує достатній захист інтересів суб'єкта господарювання, відбувається його соціально спрямований розвиток в цілому, можливість протистояння рейдерству та іншим несприятливим впливам та загрозам;

– метод експертних оцінок передбачає здійснювати прогнозування можливих загроз підприємства на основі висновків, зроблених експертами. Основними недоліками цього методу може бути недостатня кваліфікація спеціалістів та суб'єктивізм при прийнятті рішень. Крім того, можливий вплив одного спеціаліста на решту членів групи, якщо застосовується метод колективних експертних оцінок;

– метод аналізу і обробки сценаріїв призначений для прогнозування різних варіантів розвитку ситуації;

– теорія штучних нейронних мереж базується на моделюванні нелінійних залежностей при вирішенні задачі. Цей метод є складним для використання у діяльності підприємств на сучасному етапі їх розвитку;

– основною умовою використання методу екстраполяції є відносно стабільний розвиток підприємства, адже висновки про значення прогнозних показників у майбутніх періодах здійснюються на основі вивчення їх динаміки у попередніх періодах. Даний метод є неактуальним для застосування, оскільки теперішня ситуація підприємств характеризується нестабільністю та суттєвим коливанням фінансових показників;

– теоретико-ігрові методи слугують задля обґрунтування рішень за умов невизначеності середовища. до них відносять: теорія ігор та теорія статистичних рішень. Теорія ігор використовується у випадках, коли невизначеність середовища виникла через свідомі, навмисні дії конфліктуючих сторін. Теорія статистичних рішень застосовується коли невизначеність обстановки виникла через певні (відомі чи невідомі) обставини. Таким чином теоретико–ігрові методи використовуються для визначення варіантів розвитку підприємства у непередбачуваному зовнішньому середовищі;

– методи оптимізації як правило застосовуються для розв'язання задач теорії оптимальних процесів, оптимального регулювання та ін. До методів оптимізації відносять транспортні задачі, мережне планування, задачи з організації виробництва та оптимального проектування, тощо. Тобто метод оптимізації призначено для вибору варіанту, за якого досягається бажаний результат.

– розрахунково-органолептичного підходу щодо дослідження стану економічної захищеності промислового підприємства формується за допомогою врахування здібностей менеджерів різних ланок управління шляхом відповідних аналітичних дій і розрахунків та опирається на результати здійснення органолептичних методичних прийомів, зокрема таких, як експеримент, суцільні спостереження та контрольні заміри;

– експертизо-узагальнюючого підходу, щодо визначення стану економічної захищеності шляхом застосування доцільних методичних прийомів за допомогою узагальнення та використання певних видів експертиз, опираючись на аналітичні

групування та групування недоліків зокрема, а також на систематизацію висновків та належну інтерпретацію отриманих результатів.

6.3 Управління фінансовими ризиками

Розвиток суспільного виробництва на основі інновацій відбувається швидкими темпами лише тоді, коли спостерігається пожвавлення у науковій і технічній сферах у всіх її проявах, а також з урахуванням потреб у створення ефективної системи економічної захищеності підприємства. Дифузія національної та міжнародної моделі системи економічної захищеності зумовлює потребу у адаптуванні звичних способів дієвого протистояння якісно новим загрозам, що стали наслідком економіко-технологічного дисбалансу в життєдіяльності суб'єкта господарювання.

Важливо брати до уваги те, що розвиток ринкового середовища в нашій державі відбувається у складних соціально-економічних умовах, спричинених кризовими явищами, які суттєво гальмують розвиток суспільства. Ціла низка проблемних питань, пов'язаних із суттєвими зрушеннями у ринковому просторі, поглиблюються різними соціально-економічними чинниками: постійним зростанням дефіциту вітчизняного державного бюджету, галопуючою інфляцією, суттєвим спадом виробництва, зростанням безробіття, в результаті чого відбувається гальмування економічного поступу промислових підприємтсв. Зазначені несприятливі тенденції у вітчизняній економіці постійно поглиблюються внаслідок нехтування наукових підходів до розробки ґрунтовної стратегії промислових підприємств. Варто зауважити, що заходи зі створення ефективної системи економічної захищеності промислового підприємства завжди перебувають у тісній взаємодії та визначаються особливостями економічного зростання на окремо взятому етапі та загалом у процесі розвитку суб'єкта господарювання. Окремі аспекти визначеної проблеми можуть варіюватися, виходячи з темпів розвитку та зміни внутрішнього та зовнішнього середовища існування сучасної економічної системи.

На рівень економічної захищеності підприємства впливає низка факторів та чинників, які схематично подано на рисунку 6.6.

Хоч наразі науковцями зроблено значний внесок у наукове осмислення ключових питань створення системи економічної захищеності підприємства на інноваційній основі, досі залишається невирішеним питання оптимальних інноваційні методів формування економічної захищеності вітчизняного виробника.

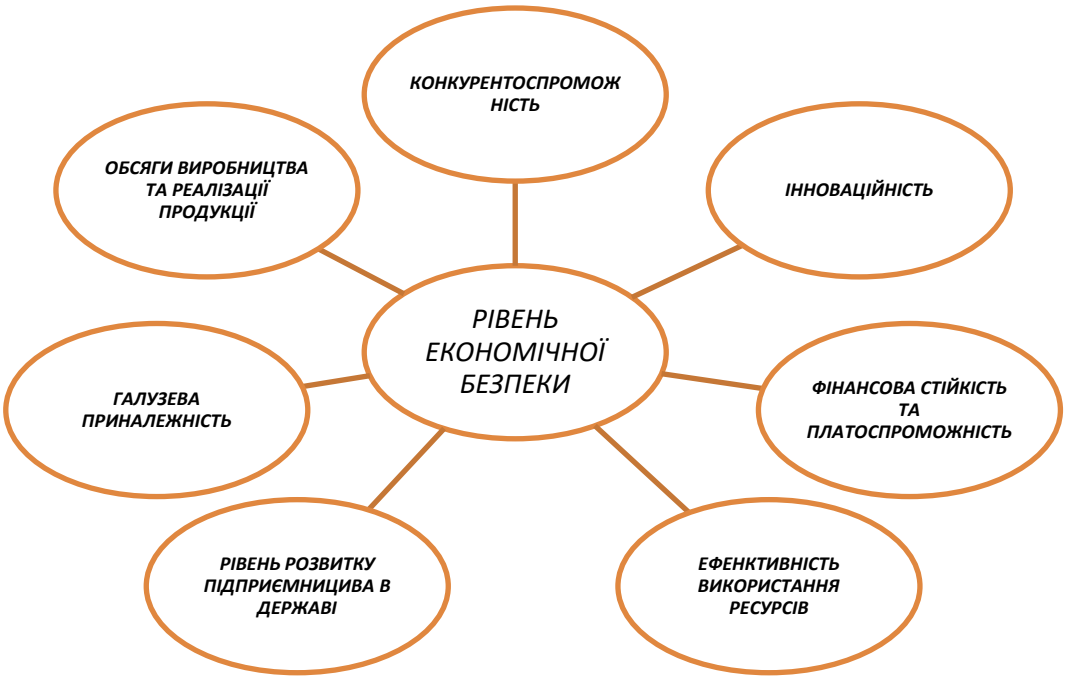

Рисунок 6.6 – Фактори та чинники впливу на економічну захищеність підприємства

Досягнення бажаного рівня економічної захищеності промислового підприємства в нестабільному середовищі сьогодні важко уявити без відповідного інноваційного менеджменту. Реалізація інноваційного потенціалу є однією з найважливіших умов сталого економічного поступу. Інноваційна діяльність підприємства починається з оцінки інноваційних пропозицій – процедури, що має допомогти на основі ключових критеріїв та наявних обмежень у ранжуванні та відборі з-поміж багатьох альтернатив певного плану інвестування новацій. При цьому найслабшою ланкою, зазвичай, є управління власне інноваційним процесом.

Ефективність інноваційної діяльності промислового підприємства можна визначити певними економічними критеріями, які мають засвідчити, що результат від реалізації обраних інвестицій у інноваційний продукт або операцію, має бажаний корисний ефект (економічну вигоду).

Визначення ефективності інноваційної діяльності досить складний та суперечливий процес, а для промислових підприємств, як правило, він поєднаний з такими особливостями (через наявність великої кількості альтернативних проектів):

1) вибір пріоритетного напрямку (інноваційну ідею, як правило, можна втілити різними шляхами і на стадії розробки необхідно з поміж можливих варіантів обрати найефективніший);

2) пріоритетність фінансування (інноваційних проектів декілька, вони не пов’язані між собою, а кошти обмежені).

Інноваційний проект можна вважати ефективним, якщо поставлені цілі та отримані економічні показники відповідають або перевершують заявлені на стадії розробки результати. Через принципові відмінності інвестиційних та інноваційних проектів економічна наука дотепер не виробила єдиного підходу до оцінки ефективності інноваційної діяльності. В інвестиційному менеджменті для такої оцінки використовують прибутковість. З інноваціями все набагато складніше, оскільки їх прибутковість як правило має

відтермнований характер, а також і через невизначеність зовнішнього середовища, процес розробки та впровадження новації піддається додатковому ризику, що врешті заважає адекватно провести аналіз та оцінку на початку та на завершальній стадії реалізації інноваційного проекту. Зокрема інновації у сфері загального менеджменту суб'єкта господарювання (злиття, поглинання, зрушення в організаційній структурі, застосування новацій в процесі управління персоналом підприємства, тощо) дають результати у довгостроковій перспективі. Результативність маркетингово-логістичних інновацій накраще оцінювати через відповідне зростання конкурентних позицій.

Оцінку інноваційного проекту господарюючого суб'єкта можна провести за такими напрямками: зміни у конкурентоспроможності промислового підприємства, зміни у діловій активності, зміни у репутації на ринку, зміни у фінансових показниках діяльності. Перші три напрямки мають більш суб'єктивний характер (їх оцінка різними експертами може дуже різнитися), то фінансові показники діяльності носять більш об'єктивний характер і у своїй сукупності дають справжню картину. Отже, можна стверджувати, що ефективність діяльності промислового підприємства виражається через сукупність економічних показників, до яких висуваються такі вимоги:

1) орієнтація на перспективу з урахуванням аналізу попередньої діяльності промислового підприємства;

2) показники мають бути прийнятними для будь-якої стадії життєвого циклу інновації;

3) спиратися на дані АВС-аналізу у ретроспективі;

4) показники мають бути пов'язані з усіма розділами інноваційного проекту та відображати всі ключові аспекти фінансової діяльності суб'єкта господарювання;

5) результуючі показники мають бути отримані шляхом відповідних розрахунків, що враховують ризик та фінансову стійкість інноваційного проекту

6) для оцінки має бути використано відповідну інформацію у достатньому для аналізу обсязі.

На сьогодні досить поширеною є система показників, які здатні характеризувати економічні показники суб'єкта господарювання, що в свою чергу передбачає вплив окремих факторів економічного середовища та виявлення на підставі цього резервів економічного зростання. Тому для оптимізації промислового виробництва при реалізації інновацій, перш за все, необхідно оцінити їх вплив на економічні показники діяльності підприємства. Через це виникає потреба у визначенні відповідних показників ефективності діяльності господарюючого суб'єкта. Завдання визначення економічної ефективності діяльності промислового підприємств на основі інноваційного поступу є неоднозначною та дискусійною. Використання таких показників, як прибуток, собівартість, фондовіддача, продуктивність праці та інші дозволяє певним чином охарактеризувати ефективність цієї діяльності. Проте для аналізу ефективності інновацій не завжди достатньо лише такого підходу. Саме тому, перш за все необхідно визначитись із чинниками, що найбільш вдало розкриють внутрішні резерви тих чи інших інновацій. Тому доцільним є використання кореляційно-регресивного аналізу, за результатами якого можна окреслити критерії, за якими слід проводити дослідження у тій чи іншій ситуації.

Загальна економічна ефективність інновацій як правило досліджується з використанням інтегрального ефекту, індексу рентабельності, норми рентабельності та періоду окупності, що дають змогу оцінити комерційну привабливість інноваційного проекту. Досить поширеними показниками при оцінці інноваційної діяльності є приріст

обсягу виробленої (товарної, реалізованої) продукції, збільшення продуктивності праці, зростання фондоозброєності та фондовіддачі, збільшення рентабельності виробництва, зміни в коефіцієнтах оновлення технології та оновлення продукції та ін.

Але не менш важливим є врахування таких чинників, як цілі учасників інноваційного проекту, умови його реалізації, рівень ризику та інші складові, що можуть бути позбавлені кількісного вираження. Тому визначення результативності інноваційних проектів має спиратись як на формалізовані, так і на експертні методи аналізу.

Для встановлення економічної захищеності застосовують різноманітні підходи, які умовно можна поділити на групи:

1) методи зіставлення головних економічних результатів з їх граничними показниками;

2) методи експертного оцінювання з метою вибудовування ієрархії суб'єктів господарювання за рівнем загроз;

3) методи загального визначення динаміки економічного розвитку за головними економічними критеріями;

4) окремі методи прикладної математики, в тому числі й багатовимірного статистичного аналізу.

Окрім наведених вище показників, подекуди слід використовувати методи, що застосовуються в інвестиційному менеджменті. З огляду на те, що часовий лаг між науковими пошуками та розповсюдженням нового продукту становить від двох до п'яти років, то постає питання щодо співмірності коштів, що були вкладені на стадії розробки і реалізації інновацій, та величиною одержаних прибутків. Такий підхід базується на тому, що норма прибутку (або ж норма позичкового відсотку) впливає на вартість грошей у часі. Для того, щоб нівелювати чинник часу звівши витрати до одного моменту часу і таким чином провести достовірний аналіз ефективності новацій необхідно скористатись таким фінансовим інструментом, як дисконтування.

6.4 Захист активів підприємства та роль контролінгу у цьому процесі

Сутність захисту активів підприємства

Активи підприємства – це ресурси, що забезпечують його діяльність, фінансову стабільність та розвиток. Захист активів спрямований на мінімізацію ризиків втрати або знецінення матеріальних, нематеріальних та фінансових ресурсів.

Захист активів є ключовим компонентом фінансової безпеки, що включає організаційні, правові, технічні та фінансові заходи для збереження майна підприємства.

Основні види активів підприємства

1. **Матеріальні активи –** будівлі, обладнання, техніка, транспортні засоби – найчастіше потерпають від крадіжок, пожеж та фізичного зношення.
2. **Нематеріальні активи –** патенти, торговельні марки, авторські права – відзначаються порушенням прав інтелектуальної власності.
3. **Фінансові активи –** грошові кошти, цінні папери, депозити – привертають увагу через валютні коливання та шахрайство.

4. **Інформаційні активи –** дані клієнтів, бази даних, комерційні секрети – переважно сконцентровані навколо таких негативних впливів, як кібератаки та витік інформації.

Захист активів є ключовим компонентом економічної безпеки підприємства. Використання організаційних, технічних, юридичних і фінансових заходів допомагає мінімізувати ризики та зберегти стійкість підприємства в умовах постійно змінного середовища.

Стратегічна мета будь-якого суб'єкта господарювання полягає в отриманні фінансового результату. Саме тому важливу роль в формуванні економічної захищеності відіграє **контролінг** як сучасна система ефективного управління прибутком промислового підприємства. В окремих випадках мета суб'єкта підприємницької діяльності може відрізнятися, зокрема, це може бути освоєння нового сегменту ринкового простору чи витіснення конкурентів, в такому випадку контролінг зосереджується саме на цих завданнях, не нівелюючи при цьому мету отримання фінансового результату.

Перебуваючи на перехресті обліку та інформаційного супроводу контролю, контролінг є ключовою ланкою менеджменту промислового підприємства, оскільки він поєднує зазначені завдання, впроваджує та узгоджує їх, до того ж не дублюючи керівні завдання, але надаючи їм якісно нового статусу. Контролінг належить до особливого механізму внутрішнього регулюванням підприємства, який формує певний оперативний зв'язок у системі менеджменту. Тобто, в контексті усвідомлення сутності контролінгу та його основних завдань відбувається покращення продуктивності управління. Ефективне втілення цього напряму передбачає, насамперед, перспективне удосконалення наукового та методичного інструментарію контролінгу та створення належної організаційно-методичної основи для всебічного інтегрування системи контролінгу в менеджмент промислового підприємства.

В Україні та за кордоном термін «контролінг» має широке тлумачення. Наразі не існує єдиного розуміння його значення. З англ. «to control» – керувати, спостерігати, перевіряти, здійснювати контроль. Натомість французьке «controle» перекладається як «зіставлення». Загальноприйнятою є думка щодо існування двох основних шкіл організаційного менеджменту – німецької та американської. В той же час у Німеччині домінує науковий підхід до формування основних принципів та ефективних методів контролінгу, натомість у Сполучених Штатах основна увага зосереджена на його практичних важелях. Система контролінгу була вперше описана та застосована в США, в результаті створення професійної організації контролерів – Controllers Institute of America) 1931), згодом перейменовану в Financial Executive Institute. Однак, термін «контролінг» в англомовних джерелах практично не використовується. Натомість у Великобританії і США функціонують служби управлінського обліку (англ. managerial accounting, management accounting), хоч працівників цих служб називають контролерами (англ. controller). Термін «контролінг» започатковано в Німеччині, звідки він і прийшов до СНД, а відтак і в Україну.

Контролінг – відносно нове явище в управлінні середовищем, тому його впровадження може викликати супротив. Щоб подолати цей супротив, а також мерщій домогтися перших успіхів та створити на промисловому підприємстві результативно функціонуючу систему, слід дослідити складнощі, які можуть з'явитись, їх причини і засоби, які дають змогу їх подолати. Феномен опору новому на перший погляд парадоксальний, але загальновідомий.

Зазвичай впровадженню контролінгу заважають дві групи чинників: недосконаліть самої моделі та соціально-психологічні фактори. Відносно останніх слід зазначити, що опір новим методам може бути індивідуальним і груповим.

Впровадження контролінгу на підприємстві зумовлено такими факторами:

- погіршення порівняно з подібними підприємствами економічних показників;
- поява нових або зміна цілей в існуючих умовах функціонування;
- відсутність узгодженості цілей;
- старі методи планування, калькуляції та аналізу, невідповідність вимогам до відстежування діяльності та прийняття управлінських рішень;
- відсутність деяких функцій, наявність конфліктних ситуацій при їх виконанні.

Аналіз сучасних наукових праць, а також практичного досвіду управління на вітчизняних і зарубіжних підприємствах дозволяє констатувати, що інтерес до проблем практичного застосування контролінгу зростає. Ефективне функціонування контролінгу в управлінні можливе лише за умови його послідовного впровадження в практичну діяльність суб'єкта господарювання з урахуванням усіх ключових аспектів цього процесу.

Досвід упровадження контролінгу на низці великих підприємств показує, що **раціонально службу контролінгу створювати в такому складі**:

- начальник служби контролінгу;
- контролер – куратор цехів;
- контролер – спеціаліст з управлінського обліку;
- контролер – спеціаліст з інформаційних систем.

Перелік організаційних аспектів впровадження контролінгу на підприємстві зазвичай включає такі складники:

- відповідальність за впровадження служби контролінгу;
- вибір спеціаліста на посаду контролера;
- вимоги, що висуваються до контролера.

Контролінг є важливим засобом успішного функціонування підприємства, оскільки: забезпечує керівництво і власника підприємства інформацією для прийняття управлінських рішень, управління ресурсами шляхом інтеграції процесів збирання, обробки, підготовки, аналізу, інтерпретації інформації; забезпечує виживання підприємства на рівнях тактичного та стратегічного управління; сприяє досягенню стану економічної захищеності.

Зазвичай одним з найбільш продуктивним методів впровадження контролінгу в умовах обмеженості ресурсів є поетапна зміна управлінських і інформаційних потоків суб'єкта господарювання. Її застосування означає послідовне здійснення низки кроків, ефективність кожного з яких можна оцінити відразу після здійснення.

Перелік основних етапів впровадження контролінгу в управління суб'єктами підприємництва:

1 етап – прийняття рішення (відбувається переважно у випадку різкого погіршення основних показників діяльності);

2 етап – діагностика існуючої системи управління (фіксація сучасного стану функціонування системи управління на підприємстві);

3 етап – розробка концепції «ідеальної» системи управління підприємством (формування технічного завдання на побудову бажаної системи управління та адекватного їй контролінгу);

4 етап – входження контролінгу в «двері» підприємства (формування інструментальної бази контролінгу та створення відповідної служби);

5 етап – запровадження контролінгу в поточну діяльність підприємства (демонстрація дієвості розробленого інструментарію та переконання менеджерів у доцільності його застосування);

6 етап – укріплення позицій (визнання та розповсюдження контролінгу в підрозділах підприємства);

7 етап – фаза зростання значущості та обсягу функцій контролінгу (постійне розширення функцій, завдань та інструментарію контролінгу).

Досліджуючи проблему ефективного впровадження контролінгу в управління суб'єктом господарювання, пропонує вісім обов'язкових етапів підготовчих робіт задля впровадження системи контролінгу на підприємстві:

- диференціація видів витрат;
- визначення другого рівня звітності;
- організація обліку доходів і витрат;
- розробка річного плану;
- розуміння цілей;
- складання планів для окремих підрозділів;
- планування в поквартальному розрізі;
- розрахунок головних показників для калькуляції.

Слід наголосити, що зазначений перелік не є капітальним, його необхідно вдосконалити залежно від галузі суб'єкта підприємництва, а також опираючись на минулу діагностику керування суб'єктом господарювання.

Досліджуючи практичний досвід запровадження контролінгу в управління суб'єктом господарювання можна визначити такі основні результати, які повинні бути досягнуті:

- удосконалення системи управління;
- удосконалення організаційної структури та взаємовідносин бізнес-одиниць та окремих їх підрозділів;
- впровадження контролінгу діяльності бізнес-одиниць та групи в цілому.

З метою отримання цих результатів автори дають рекомендацію запровадити проект «Контролінг», який містить такі етапи: впровадження інноваційної організаційної структури, створення апарату та організаційно-управлінської структури контролінгу, формування ІТ-стратегії проекту, розробка та запровадження гнучкої системи п'ятирічного бізнес-планування, формування системи економічних партперських взаємовідносин між бізнес-одиницями, удосконалення моделі проектного аналізу, побудова ефективного моніторингу, побудова ефективної системи обліку та звітності, організація контрольно-ревізійних перевірок та внутрішнього аудиту .

Цей підхід до впровадження контролінгу є досить ефективним, але в той час має деякі недоліки: дублювання етапів, а також реалізацію етапів, які безпосередньо не торкаються контролінгу.

Дослідивши різні наукові погляди щодо переліку та змісту основних етапів впровадження контролінгу задля досягнення стану економічної захищеності суб'єктами господарювання, пропонуються заходи щодо організації цього процесу на промисловому підприємстві. З огляду на особливості контролінгу в управлінні промисловим підприємством і сучасне розуміння сутності цієї управлінської технології пропонуються такі етапи впровадження контролінгу:

1. Прийняття рішення про впровадження контролінгу в управління промисловим підприємством. Цей етап передбачає узгодження думок менеджерів вищої ланки та власників підпрмємства щодо доцільності введення такої адміністративної технології, розуміння її продуктивності та задумів, які відкриваються перед промисловим підприємством при запровадженні контролінгу, а також розроблення та мотивування системи цілей та місії контролінгу при формуванні надійного підприємницького середовища.

2. Створення служби контролінгу передбачає обґрунтування місця служби контролінгу в керувані промисловим підприємством, обґрунтування її особового складу, належний розподіл повноважень поміж контролерами та формалізацію їхніх обов'язків та посадових прав.

3. Обгрунтування програми запровадження контролінгу в керування промисловим підприємством з аргументацією окреслених заходів і термінів їх дії, що має бути зазначено в плані-графіку впровадження контролінгу.

4. Розробка кошторису запровадження контролінгу в керування промисловим підприємством. Цей етап визначає планування потрібних джерел фінансування та затрат на реалізацію доцільних заходів, а також є підґрунтям для оцінювання продуктивності запровадження контролінгу в керування промисловим підприємством .

5. Започаткування здійснення освітньо-роз'яснювальної роботи серед власників, менеджерів і персоналу підприємства. Даний етап – це періодичне та систематичне проведення семінарів, тренінгів, презентацій, нарад, конференцій, тощо. Такі заходи мають забезпечити усвідомлення змін на виробництві, розуміння ролі та місця кожного з пацівників в даному процесі, а отже – суттєво знижують протидію новаціям, що впроваджуються.

6. Вхідний аналіз менеджменту промислового підприємства та одночасне дослідження результатів фінансової та господарської діяльності. Даний етап – це проведення діагностики: фінансової структури, організаційної структури, внутрішнього та зовнішнього та середовищ, вхідних та вихідних інформаційних ланцюжків та ін.

7. Формування програми щодо покращення менеджменту суб'єкта господарювання, а саме: покращення організаційної структури товаровиробника, впровадження реінжинірингу інформаційних потоків та бізнес-процесів, побудова пропозицій по реформуванню або ж створенню продуктивної виробничої структури, тощо.

8. Створення ефективної системи показників-індикаторів, які характеризують внутрішнє та зовнішнє середовище, що стануть підгрунттям для визначення службою контролінгу всіх векторів та менеджменту, встановлення критичних коливань отриманих значень від запланованих.

9. Обґрунтування інструментарію та методик контролінгу об'єктів менеджменту маркетинговими підрозділами, дослідження їх продуктивності для розв'язання певних задач,

їх адаптивність до особливостей фінансової та господарської роботи кожного окремого товаровиробника, тощо.

10. Створення системи внутрішньої звітності на підприємстві службою контролінгу. На даному етапі формують систему управлінської звітності в контексті певних споживачів даної інформації. При цьому визначаються відповідні інформаційні потреби задля прийняття продуктивних управлінських рішень, тощо.

11. Впровадження контролінгу в усіх сферах менеджменту, на всіх щаблях управлінської структури певного суб'єкта господарської діяльності.

Таким чином при запровадженні контролінгу основні заходи захисту активів передбачатимуть синергію таких складових:

1. **Організаційні заходи**
   - розробка внутрішніх політик і процедур захисту активів;
   - проведення регулярних аудитів;
   - навчання персоналу правилам безпеки.
2. **Технічний захист**
   - встановлення систем відеоспостереження, сигналізації, контролю доступу;
   - використання антивірусного ПЗ та міжмережевих екранів для захисту інформації;
   - забезпечення резервного копіювання даних.
3. **Юридичний захист**
   - реєстрація прав на інтелектуальну власність;
   - підготовка договорів, що захищають фінансові та матеріальні активи;
   - створення контрактів із застереженнями щодо конфіденційності.
4. **Фінансовий захист**
   - страхування матеріальних і фінансових активів;
   - хеджування валютних ризиків;
   - створення резервних фондів для покриття можливих збитків.

Ключові інструменти захисту активів при запровадженні контролінгу можуть бути такими:

1. **Страхування**
   - страхування майна (від пожеж, затоплень, крадіжок);
   - страхування від фінансових ризиків (банкрутство, шахрайство).
2. **Резервування коштів:** формування резервів для покриття непередбачених витрат.
3. **Використання сучасних технологій**
   - використання систем штучного інтелекту для моніторингу фінансових операцій;
   - застосування біометричних систем для захисту доступу до критичних ресурсів.
4. **Контроль доступу**
   - фізичний контроль: обмежений доступ до складів і серверних кімнат;
   - цифровий контроль: багатофакторна аутентифікація для доступу до баз даних.

Перелік питань:

1. Що таке фінансова безпека підприємства, і чому вона є важливою?
2. Які основні складові фінансової безпеки ви можете назвати?
3. Як впливають зовнішні та внутрішні фактори на фінансову безпеку підприємства?
4. Які показники використовуються для оцінки фінансової стабільності?
5. У чому сутність коефіцієнта платоспроможності, і як його розрахувати?
6. Як коефіцієнт фінансової незалежності відображає стан підприємства?
7. Які переваги має SWOT-аналіз для оцінки фінансової стабільності?
8. Що таке модель Альтмана, і як вона використовується для прогнозування банкрутства?
9. У чому полягає значення аналізу грошових потоків для оцінки фінансової стабільності?
10. Які основні ризики виникають у сфері фінансової безпеки?
11. Як підприємства можуть управляти валютними ризиками?
12. Які інструменти хеджування використовуються для мінімізації фінансових ризиків?
13. Що включає процес управління фінансовими ризиками?
14. У чому полягають особливості стратегії уникнення фінансових ризиків?
15. Як страхування допомагає захищати фінансові активи підприємства?
16. Які сучасні технології використовуються для моніторингу фінансових ризиків?
17. Що таке контроль доступу, і як він сприяє захисту активів підприємства?
18. Які заходи необхідно впровадити для захисту інформаційних активів?
19. Як юридичний захист сприяє збереженню нематеріальних активів?
20. Чому резервування коштів є важливим інструментом захисту активів підприємства?

Тести:

1. **Що таке фінансова безпека підприємства?**
   а) забезпечення фізичної безпеки працівників;
   б) стан фінансової системи, що гарантує її стабільність і ефективність;
   в) оптимізація витрат виробництва;
   г) розробка нових фінансових інструментів.
2. **Який показник відображає здатність підприємства своєчасно виконувати фінансові зобов'язання?**
   а) рентабельність активів;
   б) коефіцієнт платоспроможності;
   в) фінансова незалежність;
   г) диверсифікація активів.

3. **Що є основною метою оцінки фінансової стабільності?**
   а) прогнозування макроекономічних умов:
   б) виявлення фінансових ризиків і підтримання стійкості;
   в) збільшення частки ринку:
   г) управління персоналом.

4. **Який із методів передбачає аналіз сильних і слабких сторін фінансового стану підприємства?**
   а) аналіз балансу;
   б) SWOT-аналіз;
   в) грошовий аналіз;
   г) матричний аналіз.

5. **Який із наведених коефіцієнтів показує частку власного капіталу у загальній структурі капіталу?**
   а) рентабельність активів;
   б) коефіцієнт фінансової незалежності;
   в) коефіцієнт платоспроможності;
   г) валовий прибуток.

6. **Що таке модель Альтмана?**
   а) метод оцінки грошових потоків підприємства;
   б) модель прогнозування ймовірності банкрутства;
   в) метод оптимізації фінансових витрат;
   г) інструмент диверсифікації активів.

7. **Який із інструментів використовується для захисту активів від валютних ризиків?**
   а) хеджування;
   б) аудит;
   в) диверсифікація;
   г) аналіз балансу.

8. **Що передбачає стратегія уникнення ризиків?**
   а) застосування фінансових інструментів для мінімізації ризиків;
   б) відмова від операцій із високим рівнем ризику;
   в) передача ризиків іншій стороні;
   г) залучення додаткових інвестицій.
9. **Який показник оцінює ефективність використання активів підприємства?**
   а) рентабельність активів;
   б) коефіцієнт ліквідності;
   в) частка власного капіталу;
   г) валовий дохід.

10. **Що є ключовою метою аналізу грошових потоків?**
    а) прогнозування обсягів продажів;
    б) оцінка руху коштів у розрізі операційної, інвестиційної та фінансової діяльності;
    в) оптимізація податкових витрат;
    г) управління персоналом.

11. **Який тип активів найчастіше піддається кібератакам?**
    а) матеріальні активи;

б) нематеріальні активи;
в) фінансові активи;
г) інформаційні активи.

12. **Що є основною метою страхування активів підприємства?**
а) збільшення прибутку;
б) захист від фінансових втрат;
в) оптимізація витрат;
г) забезпечення інвестицій.

13. **Яка стратегія управління ризиками передбачає використання резервних фондів?**
а) хеджування;
б) прийняття ризиків;
в) страхування;
г) резервування.

14. **Що включає процес моніторингу фінансових ризиків?**
а) лише оцінку ринкових умов;
б) постійний аналіз фінансового середовища та коригування стратегії;
в) оптимізацію операційної діяльності;
г) створення нових продуктів.

15. **Що є основною перевагою диверсифікації активів?**
а) мінімізація витрат;
б) зниження залежності від одного джерела ризику;
в) збільшення обсягу продажів;
г) розширення ринків збуту.

16. **Що передбачає контроль доступу до активів?**
а) оптимізацію фінансових потоків;
б) обмеження фізичного та цифрового доступу до ресурсів;
в) створення резервних фондів;
г) розробку маркетингових стратегій.

17. **Як фінансові технології допомагають у моніторингу ризиків?**
а) забезпечують автоматизацію процесів;
б) збільшують кількість активів;
в) зменшують вартість операційної діяльності;
г) використовуються для залучення інвесторів.

18. **Що таке хеджування валютних ризиків?**
а) збільшення грошових резервів;
б) використання фінансових інструментів для мінімізації ризиків;
в) відмова від операцій з іноземними валютами;

г) розподіл активів між різними рахунками.

19. **Який із показників є критичним для оцінки ліквідності підприємства?**
    а) коефіцієнт фінансової незалежності;
    б) коефіцієнт платоспроможності;
    в) рентабельність активів;
    г) аналіз витрат.

20. **Що є основною метою резервування коштів?**
    а) оптимізація витрат;
    б) захист від непередбачених фінансових втрат;
    в) розширення ринків збуту;
    г) залучення інвестицій.

Практичні завдання:

Завдання 1. Оцінка фінансової стабільності підприємства

Мета: Навчитися аналізувати фінансову стабільність підприємства за допомогою фінансових коефіцієнтів.

1. Ви отримали такі дані фінансової звітності підприємства:
   Ліквідні активи: 1 500 000 грн.
   Короткострокові зобов'язання: 800 000 грн.
   Власний капітал: 2 000 000 грн.
   Загальний капітал: 3 500 000 грн.
   Чистий прибуток: 400 000 грн.
   Сума активів: 5 000 000 грн.
2. Обчисліть наступні показники:
   - коефіцієнт платоспроможності;
   - коефіцієнт фінансової незалежності;
   - рентабельність активів.
3. Зробіть висновки про фінансову стабільність підприємства на основі отриманих результатів.

Завдання 2. SWOT-аналіз фінансової безпеки

Мета: Визначити сильні та слабкі сторони, а також можливості та загрози для фінансової безпеки підприємства.

1. Врахуйте, що підприємство працює у висококонкурентному середовищі, використовуючи такі дані:
   Сильні сторони: стабільний прибуток, високий рівень ліквідності.
   Слабкі сторони: високий рівень боргового навантаження.
   Можливості: залучення іноземних інвестицій.
   Загрози: валютні коливання, посилення конкурентного тиску.
2. Побудуйте таблицю SWOT-аналізу, заповнивши її відповідно до наданих даних.

3. Запропонуйте стратегії для покращення фінансової безпеки підприємства.

Завдання 3. Аналіз ризиків у фінансовій діяльності

Мета: Оцінити вплив фінансових ризиків на діяльність підприємства.

1. Розгляньте такі ризики:
   Валютні коливання, ймовірність виникнення — 60%, вплив — 500 000 грн.
   Кредитний ризик, ймовірність виникнення — 40%, вплив — 300 000 грн.
   Ризик ліквідності, ймовірність виникнення — 20%, вплив — 200 000 грн.
2. Визначте рівень ризику для кожного типу
3. Зробіть висновки про найкритичніші ризики.

Завдання 4. Розробка стратегії управління ризиками

Мета: Навчитися обирати ефективні стратегії для управління фінансовими ризиками.

1. Оберіть стратегії для таких ситуацій:
   - валютний ризик: зміни курсу валют;
   - кредитний ризик: неспроможність контрагентів виконати зобов'язання;
   - ризик ліквідності: затримка виплат за рахунками.
2. Опишіть заходи, які потрібно впровадити, щоб знизити кожен ризик.
3. Представте результати у вигляді таблиці:

Ризик	Стратегія	Заходи
Валютний ризик	Хеджування	Використання форвардних контрактів
Кредитний ризик	Передача ризику	Страхування дебіторської заборгованості
Ризик ліквідності	Резервування коштів	Створення резервного фонду

Завдання 5. Захист активів підприємства

Мета: Розробити план заходів для захисту активів підприємства.

1. Ви отримали інформацію про активи підприємства:
   - Матеріальні активи: будівлі, обладнання.
   - Нематеріальні активи: патенти, авторські права.
   - Фінансові активи: депозити, цінні папери.
   - Інформаційні активи: бази даних, комерційна інформація.
2. Для кожного типу активів:
   - Визначте потенційні ризики.
   - Запропонуйте заходи для їхнього захисту.
3. Представте результати у вигляді таблиці:

Тип активів	Ризики	Методи захисту
Матеріальні	Пожежі, крадіжки	Страхування, сигналізація
Нематеріальні	Порушення авторських прав	Реєстрація прав, судовий захист
Фінансові	Шахрайство, валютні ризики	Аудит, хеджування
Інформаційні	Кібератаки, витік даних	Антивірусне ПЗ, багатофакторна аутентифікація

Завдання 6. Оцінка ефективності управління фінансовими ризиками

Мета: Проаналізувати, як реалізовані заходи впливають на фінансову безпеку підприємства.

1. Ви впровадили такі заходи: хеджування валютних ризиків, страхування активів, проведення регулярного аудиту.
2. Оцініть, як ці заходи вплинули на зменшення ризиків, на покращення фінансових показників та на підвищення довіри інвесторів.
3. Запропонуйте додаткові заходи для покращення фінансової безпеки.

ТЕМА 7. ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

7.1 Сутність та значення інформаційної безпеки.
7.2 Загрози інформаційній безпеці.
7.3 Методи захисту інформації.
7.4 Управління інформаційними ризиками.

7.1 Сутність та значення інформаційної безпеки

Визначення інформаційної безпеки

Інформаційна безпека підприємства — це стан захищеності його інформаційних ресурсів від зовнішніх і внутрішніх загроз. Це забезпечує конфіденційність, цілісність і доступність інформації, необхідної для стабільної роботи підприємства та прийняття ефективних управлінських рішень.

Інформаційна захищеність відіграє доволі значну роль у загальній системі економічного захисту суб'єкта підприємницької діяльності, адже стан цієї складової характеризується наявністю певної частини неточної, неповної або суперечливої інформації, яка стає підґрунтям прийняття важливих і нагальних управлінських рішень. Мінімізацією негативного впливу зазначених процесів традиційно займається інформаційно-аналітичний підрозділ разом зі службою охорони. Основними завданнями такої співпраці є: дослідження інформаційного масиву, що використовується у діяльності підприємства, збір необхідної інформації, її накопичення, обробка, структурування та зберігання, забезпечення надійного захисту отриманої інформації від можливого недозволеного доступу, систематична робота в напрямі налагодження та підтримки ділових зв'язків з партнерами, цільовою аудиторією та громадськістю.

Основні складові інформаційної безпеки

1. **Конфіденційність –** забезпечення доступу до інформації лише уповноваженим особам. Наприклад, захист баз даних клієнтів від несанкціонованого доступу.
2. **Цілісність** – гарантія, що дані не будуть змінені чи пошкоджені без дозволу. Зокрема захист фінансової звітності від несанкціонованих змін.
3. **Доступність** – забезпечення своєчасного доступу до інформації для тих, хто має на це право. Нариклад, безперебійний доступ до серверів підприємства.

Значення інформаційної безпеки

1. **Захист інтелектуальної власності:**
   - охорона комерційних секретів, патентів, ноу-хау;
   - забезпечує конкурентоспроможність підприємства.
2. **Мінімізація фінансових втрат:**
   - захист від шахрайства, кібератак та витоків даних;
   - уникнення штрафів за недотримання законодавства у сфері захисту даних.
3. **Забезпечення довіри клієнтів і партнерів:**
   - гарантія безпеки персональних даних та бізнес-інформації;
   - формування позитивної репутації.

4. Стабільність бізнес-процесів:
   - уникнення простоїв через кібератаки чи технічні збої;
   - оптимізація операційної діяльності.

Основні загрози інформаційній безпеці

1. **Кібератаки** (віруси, фішингові атаки, DDoS-атаки).
2. **Витік інформації** (несанкціоноване розголошення даних співробітниками).
3. **Технічні збої** (втрата даних через технічні несправності чи відсутність резервних копій).
4. **Недотримання політик безпеки** (використання слабких паролів, відсутність шифрування даних).

Засоби забезпечення інформаційної безпеки

1. **Технічні засоби**
   - Використання антивірусного програмного забезпечення.
   - Захист мережі за допомогою міжмережевих екранів (Firewall).
   - Резервне копіювання даних для уникнення їх втрати.
2. **Організаційні заходи**
   - Розробка внутрішніх політик безпеки.
   - Проведення тренінгів для співробітників щодо безпечної роботи з інформацією.
   - Впровадження багатофакторної аутентифікації.
3. **Юридичні інструменти**
   - Дотримання законодавства у сфері захисту персональних даних (наприклад, GDPR).
   - Оформлення договорів із застереженнями щодо конфіденційності.

Інформаційна безпека є важливим елементом загальної економічної безпеки підприємства. Сучасні технологічні рішення у поєднанні з організаційними та юридичними заходами дозволяють ефективно захищати інформаційні активи та забезпечувати стабільний розвиток бізнесу.

7.2 Загрози інформаційній безпеці

Сутність загроз інформаційній безпеці

Загрози інформаційній безпеці — це потенційні або реальні дії, що можуть призвести до втрати, несанкціонованого доступу, викривлення чи руйнування інформаційних ресурсів підприємства. Розуміння природи цих загроз є ключовим для їхнього ефективного управління та попередження.

Основні види загроз інформаційній безпеці

1. **Кібератаки** – це цілеспрямовані дії зловмисників, спрямовані на порушення роботи інформаційних систем.
   - **DDoS-атаки** (перевантаження серверів запитами, що призводить до їх недоступності);

- **фішинг** (використання підроблених повідомлень для викрадення даних);
- **шкідливе програмне забезпечення** (віруси, трояни, програми-вимагачі).

2. **Витік інформації –** втрата або крадіжка конфіденційних даних через:
   - несанкціонований доступ сторонніх осіб;
   - ненавмисні дії співробітників;
   - використання незахищених каналів передачі даних.

   Приклад: Витік персональних даних клієнтів компанії.

3. **Технічні збої** – пошкодження або втрата даних через:
   - відмову обладнання (серверів, жорстких дисків);
   - несправності програмного забезпечення;
   - аварії (пожежі, повені, електричні збої).

4. **Недотримання політик безпеки –** людський фактор є одним із найбільш поширених джерел загроз:
   - використання слабких паролів;
   - відсутність регулярного оновлення програмного забезпечення;
   - відмова від шифрування даних.

Таблиця 7.1 – Приклади загроз та їх наслідки

Загроза	Приклад	Наслідки
Кібератаки	DDoS-атака на сервер	Збої в роботі систем, втрата доходів
Витік інформації	Несанкціонований доступ до баз даних	Порушення конфіденційності, штрафи
Технічні збої	Втрата даних через поломку обладнання	Зупинка бізнес-процесів
Недотримання політик	Використання слабких паролів	Злам акаунтів, доступ до конфіденційної інформації

Фактори, що сприяють виникненню загроз

1. **Технологічні фактори:**
   - відсутність сучасних засобів захисту;
   - використання застарілого програмного забезпечення.
2. **Організаційні фактори:**
   - відсутність політик безпеки;
   - ненавченість персоналу.
3. **Зовнішні фактори:**
   - атаки з боку конкурентів;
   - глобальні кіберзагрози.

Наслідки реалізації загроз

1. **Фінансові збитки** – витрати на відновлення даних, штрафи за порушення законодавства.
2. **Втрати репутації** – зменшення довіри клієнтів і партнерів.
3. **Порушення бізнес-процесів** – зупинка діяльності через відмову систем.

Розуміння загроз інформаційній безпеці дозволяє підприємствам:

- виявляти слабкі місця в системах захисту;
- знижувати ризики через впровадження відповідних заходів;
- забезпечувати стабільність і безперервність бізнес-процесів.

Загрози інформаційній безпеці є багатогранними й динамічними. Для ефективного їх подолання підприємства мають використовувати комплексний підхід, що поєднує технологічні, організаційні та правові заходи. Це забезпечує захист інформаційних активів та сприяє розвитку бізнесу.

7.3 Методи захисту інформації

Сутність методів захисту інформації

Методи захисту інформації — це комплекс технічних, організаційних і юридичних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних. Ці методи дозволяють захистити інформаційні ресурси підприємства від несанкціонованого доступу, витоків, викривлення та втрат.

Основні методи захисту інформації:

1. **Технічні методи –** використання апаратних і програмних засобів для забезпечення безпеки.

   Основні інструменти:

   1. **Шифрування даних – з**ахист конфіденційної інформації шляхом її кодування. Наприклад, алгоритми AES, RSA для захисту фінансових транзакцій.
   2. **Міжмережеві екрани (Firewall) –** захист локальних мереж від зовнішніх атак (фільтрація трафіку, блокування несанкціонованих з'єднань).
   3. **Антивірусне програмне забезпечення** – виявлення та видалення шкідливого ПЗ.
   4. **Резервне копіювання даних –** регулярне створення копій інформації для її відновлення у разі втрати. Наприклад, хмарні сервіси Google Drive, Dropbox.
   5. **Багатофакторна аутентифікація (MFA) –** додатковий рівень захисту при вході в системи. Наприклад, використання паролю та одноразового коду на телефоні.

2. **Організаційні методи** – розробка політик, інструкцій і навчання персоналу для дотримання стандартів інформаційної безпеки.

   Основні заходи:

   1. **Розробка політики безпеки** – документування правил використання інформаційних ресурсів (регламент щодо роботи з конфіденційною інформацією).
   2. **Контроль доступу –** обмеження доступу до даних залежно від рівня привілеїв (встановлення прав доступу до баз даних).
   3. **Навчання співробітників –** проведення тренінгів із кібербезпеки.

4. **Регулярний аудит інформаційних систем –** перевірка ефективності заходів захисту. Наприклад, моніторинг логів доступу.

3. **Юридичні методи** – використання законодавчих норм для захисту інформації та відповідальності за порушення.
   Основні заходи:
   1. **Виконання законодавства про захист даних** – відповідність стандартам, як-от GDPR, ISO/IEC 27001. Зокрема для захисту персональних даних клієнтів.
   2. **Оформлення договорів** – включення умов про конфіденційність у контракти.
   3. **Судовий захист – з**ахист інтелектуальної власності через судові органи. Наприклад, врегулювання спорів щодо авторських прав.

Використання комплексного підходу до захисту інформації дозволяє підприємствам:
- захищати конфіденційну інформацію від несанкціонованого доступу;
- мінімізувати ризики фінансових втрат через кібератаки та витоки даних;
- забезпечувати довіру клієнтів та партнерів.

Методи захисту інформації мають бути комплексними, охоплюючи технічні, організаційні та юридичні аспекти. Це забезпечує стійкість інформаційних систем і дозволяє підприємствам зберігати конкурентоспроможність у сучасних умовах.

7.4 Управління інформаційними ризиками

Сутність управління інформаційними ризиками

Управління інформаційними ризиками – це процес ідентифікації, аналізу, оцінки та впровадження заходів щодо мінімізації потенційних загроз, які можуть вплинути на інформаційні ресурси підприємства. Цей процес є важливою складовою забезпечення інформаційної безпеки.

Структурні підрозділи промислового підприємства реалізують **функції, які визначають процес формування та захисту інформаційного компонента економічної безпеки суб'єкта господарювання**, зокрема:
- отримання необхідних даних, що стосуються діяльності суб'єкта господарювання;
- аналіз отриманого масиву інформації;
- передбачення ймовірних тенденцій розвитку наявного науково-технологічного потенціалу підприємства, політико-економічних процесів;
- визначення стану економічної захищеності за всіма компонентами та надання рекомендацій для його покращення в розрізі певного підприємства;
- інші види роботи в напрямі формування інформаційного компонента економічної захищеності.

Інформаційні потоки надходять на промислове підприємство з різних джерел:
- офіційні дані загального доступу;

– вірогідні нетаємні дані, отримані за допомогою неофіційного спілкування з працівниками підприємства, які володіють певною інформацією;

– конфіденційні дані, отримані незаконним способом.

Несприятливі чинники, що можуть спричинити шкоду майну суб'єкта господарювання, загрожують суттєвим зменшенням вартості активів і потраплянням у економічну залежність (поширення недостовірної або знищення важливої інформації).

Головними причинами описаних негативних процесів можуть бути:

– неспроможність самих підприємств здобути стійкі переваги легальними способами, прийнятними для ринкового середовища, тобто завдяки покращенню якості власної товарної продукції, зменшення поточних витрат на виробничу діяльність, оптимізації маркетингу тощо;

– протизаконні методи отримання злочинними суб'єктами доходів внаслідок шантажу, крадіжок чи шахрайства;

– зазіхання на життя та здоров'я менеджерів і працівників чи майно підприємства на підставі мотивів, які не мають відношення до комерційної діяльності.

Напрацюванням механізмів ефективної протидії ймовірним негативним загрозам є нагальним питанням роботи служби охорони. До основних функцій такої служби належать: фізичний захист менеджерів вищої ланки, впровадження пропускної системи, надійна охорона наявних приміщень, каналів зв'язку й обладнання, захист конфіденційної інформації від можливого недозволеного доступу, дотримання режиму секретності при роботі з важливими документами чи матеріалами. За усталеною практикою відповідальність за силову безпеку суб'єкта господарювання покладається на службу охорони, до завдань якої належить здійснення зазначених функцій.

Отже, головним завданням економічної захищеності підприємства є створення умов для стабільної роботи на сьогодні та реалізації можливостей для подальшого розвитку.

Враховуючи стан наукової розробки проблеми та досвід провідних суб'єктів господарювання, можна виокремити **шляхи покращення економічної безпеки підприємства**:

– посилення фінансової стабільності та самостійності;

– систематична робота в напрямі покращення конкурентно-здатності завдяки ефективному використанню технологічних новацій;

– модернізація системи фінансового менеджменту;

– постійне підвищення кваліфікаційного рівня співробітників та ефективне використання інтелектуальних можливостей персоналу;

– врахування екологічних характеристик, запобігання завдання шкоди довкіллю внаслідок виробничої діяльності;

– забезпечення функціонування промислового підприємства виключно у правовому полі;

– запобігання промисловому шпіонажу завдяки ефективному захисту інформаційної сфери суб'єкта господарювання, даних, що становлять комерційну таємницю, та

спрямованості до покращення інформаційного забезпечення діяльності усіх структурних підрозділів;

– створення безпечних умов для роботи персоналу, захищеності майна, комерційних інтересів і капіталу.

Наявність різного роду кризових проявів на промислових підприємствах належить до сучасних реалій, що відображають загальний стан всієї ринкової економіки України. Значна частина суб'єктів господарювання, які не здатні ефективно протидіяти загрозам і пристосовуватись до швидко змінного середовища, тобто є неконкурентоспроможними, банкрутують. У групу такого ризику, насамперед, потрапляють ті товаровиробники, які припустилися суттєвих прорахунків у площині стратегічного менеджменту: неправильно визначились з пріоритетами розвитку, галуззю діяльності, об'єктивно не оцінили кон'юнктуру ринку, окреслили помилкову стратегію та ін., тим самим прирікши себе на банкрутство, навіть не беручи до уваги різноманітні внутрішні чинники, ефективність роботи управлінської системи чи загалом економічної захищеності.

Досвід у проведенні діагностики стану економічної безпеки підприємств засвідчив, що комплекс основних показників, насамперед, повинен включати організаційно-виробничі, структурні, фінансові, наукові та інноваційні, інвестиційні індикатори формування персоналу та рівня соціального захисту співробітників, логістично-маркетингові (табл. 7.2).

Таблиця 7.2 – Індикатори економічної захищеності підприємств

Назва групи	Індикатори
1	2
Організаційно-виробничі індикатори	– динаміка продажу; – фондовіддача; – реальний стан завантаження та використання наявних виробничих потужностей; – швидкість відновлення виробничих засобів; – стабільний перебіг процесу виробництва (періодичність, завантаженість впродовж певного відрізку часу); – загальний рівень конкурентноздатності товарної продукції та суб'єкта господарювання; – вікові характеристики та технічний стан наявного парку машин і обладнання; – відсоток браку виготовленої продукції; – якісні та кількісні параметри товарної продукції
Структурні індикатори	– ієрархічність управлінської структури; – оперативність реалізації прийнятих управлінських рішень від часу виявлення певної проблеми; – структура «портфеля» попередніх замовлень (прогнозований обсяг продажу); – структура та бажаний обсяг інвестицій; – структура власних коштів; розмежування повноважень в залежно від управлінського рівня

Продовження таблиці 7.2

1	2
Фінансові індикатори	– рентабельність виробництва; – рентабельність товарної продукції; – рентабельність капіталу; – динаміка прибутків; – капіталомісткість; – заборгованість із закінченим терміном погашення (дебіторська та кредиторська); – справедлива вартість підприємства та її динаміка; – коефіцієнти маневреності, автономії, ліквідності; показники ефективності використання капіталу
Наукові та інноваційні індикатори	– стан інноваційної активності (обсяг вкладень у новації); – відсоток НДДКР у загальному обсязі реалізованої продукції; – відсоток витрат на науково-дослідну діяльність у загальних витратах підприємства; – відношення вкладень у інноваційну сферу до вартості науково-дослідних робіт; – відсоток нової продукції в загальному масиві товарної продукції; стан власного фінансування новаторських проектів.
Індикатори інвестицій	– структура залучених коштів підприємства; – відсоток вкладень у розвиток інноваційних напрямів підприємницької діяльності в загальному обсязі інвестицій; – структура інвестиційного портфелю та його динаміка; – співвідношення вкладень в основний капітал у загальних вкладеннях; відсоток вкладень в охорону довкілля в загальному обсязі витрат
Індикатор формування персоналу та рівня соціального захисту співробітників	– нераціональне використання робочого часу; – зміна кадрової структури, мобільність трудових ресурсів; – вікова характеристика персоналу суб'єкта господарювання; – освітній рівень співробітників; – співвідношення заробітної плати на підприємстві, в галузі та вцілому в промисловості; – стан заборгованості з виплати заробітної плати; – заборгованість по відпусткам; наявність на підприємстві баз відпочинку для співробітників та членів їх сімей, центрів дитячого дозвілля
Наукові та інноваційні індикатори	– стан інноваційної активності (обсяг вкладень у новації); – відсоток НДДКР у загальному обсязі реалізованої продукції; – відсоток витрат на науково-дослідну діяльність у загальних витратах підприємства; – відношення вкладень у інноваційну сферу до вартості науково-дослідних робіт; – відсоток нової продукції в загальному масиві товарної продукції; стан власного фінансування новаторських проектів.

Основні етапи управління інформаційними ризиками (рис. 7.1)

1. **Ідентифікація ризиків**

   Перший крок – визначення всіх можливих загроз для інформаційних ресурсів підприємства.

2. **Оцінка ризиків**

   Визначення ймовірності виникнення ризиків і їхнього потенційного впливу.

3. **Розробка стратегій управління ризиками**

На основі оцінки визначаються оптимальні стратегії для зниження рівня ризиків.

4. **Реалізація заходів захисту**
   Впровадження практичних заходів для мінімізації ризиків:
5. **Контроль та моніторинг**

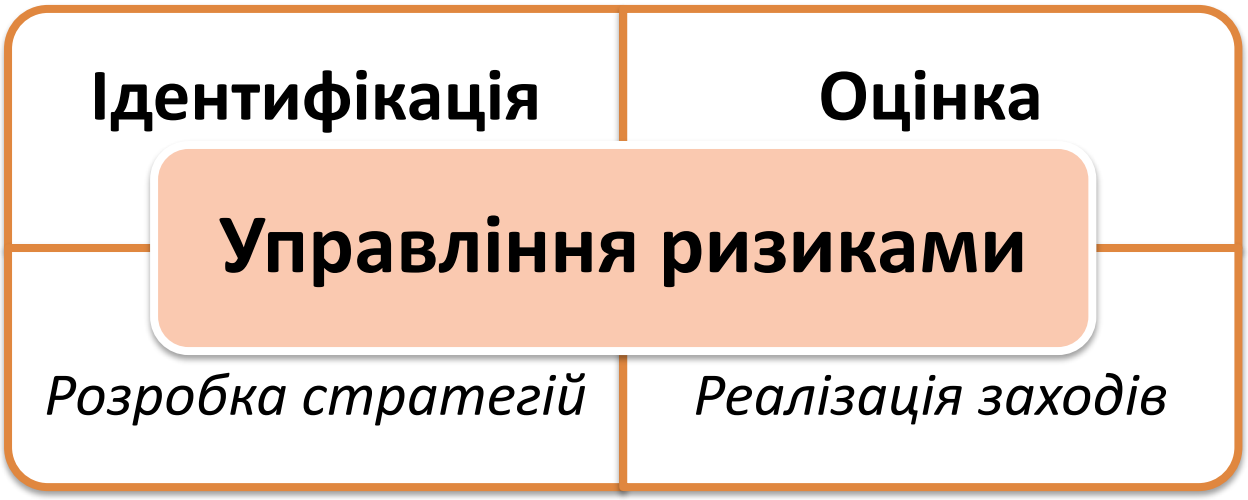

Рисунок 7.1 – Етапи управління інформаційними ризиками

Інструменти управління інформаційними ризиками

6. **Аналітичні інструменти**
   - Програмне забезпечення для аналізу ризиків (RiskWatch, RSA Archer).
   - Інструменти моніторингу кіберзагроз.
7. **Фінансові інструменти**
   - Страхування інформаційних активів.
   - Формування резервного фонду для покриття можливих збитків.
8. **Технологічні засоби**
   - Використання SIEM-систем для моніторингу та аналізу подій.
   - Автоматизовані системи резервного копіювання.

Ефективне управління інформаційними ризиками:

- Знижує ймовірність фінансових втрат.
- Забезпечує безперервність бізнес-процесів.
- Підвищує рівень довіри клієнтів та партнерів.

Управління інформаційними ризиками є важливим елементом стратегії забезпечення інформаційної безпеки. Використання сучасних інструментів, комплексного підходу та регулярного моніторингу дозволяє підприємствам захистити свої інформаційні ресурси та зберегти конкурентоспроможність.

Перелік питань:

1. Що таке інформаційна безпека, і чому вона важлива для підприємства?
2. Назвіть основні складові інформаційної безпеки.
3. У чому полягає значення конфіденційності в інформаційній безпеці?
4. Як можна забезпечити цілісність інформації на підприємстві?
5. Чому доступність інформації є критичною для ефективності бізнесу?
6. Які основні загрози інформаційній безпеці існують?
7. Наведіть приклади кібератак та їх можливих наслідків для підприємства.
8. Що таке витік інформації, і які причини його виникнення?
9. Як технічні збої можуть вплинути на інформаційну безпеку підприємства?
10. Чому людський фактор є однією з основних загроз інформаційній безпеці?
11. Які методи шифрування використовуються для захисту інформації?
12. Як резервне копіювання сприяє збереженню інформації?
13. Що таке багатофакторна аутентифікація, і чому вона важлива?
14. Як міжмережеві екрани допомагають у забезпеченні інформаційної безпеки?
15. У чому полягає роль політики безпеки в управлінні інформаційними ризиками?
16. Як проводиться ідентифікація ризиків у сфері інформаційної безпеки?
17. Які основні стратегії управління інформаційними ризиками існують?
18. Що таке передача ризиків, і як вона реалізується у сфері інформаційної безпеки?
19. Які інструменти моніторингу ризиків використовуються у сучасному бізнесі?
20. Як регулярний аудит сприяє ефективному управлінню інформаційними ризиками?

Тести:

1. **Що є основною метою інформаційної безпеки підприємства?**
   а) зменшення витрат на інформаційні системи;
   б) забезпечення конфіденційності, цілісності та доступності даних;
   в) автоматизація бізнес-процесів;
   г) створення нових інформаційних ресурсів.

2. **Що таке конфіденційність у контексті інформаційної безпеки?**
   а) захист даних від втрати;
   б) захист даних від несанкціонованого доступу;
   в) забезпечення безперебійного доступу до даних;
   г) оптимізація зберігання даних.
3. **Який основний принцип забезпечує захист даних від несанкціонованих змін?**
   а) конфіденційність;
   б) доступність;
   в) цілісність;
   г) резервування.

4. **Який із наведених методів є технічним засобом захисту інформації?**
   а) проведення тренінгів для персоналу;

б) використання антивірусного програмного забезпечення;
в) розробка політики безпеки;
г) виконання законодавчих вимог.

5. **Що таке багатофакторна аутентифікація?**
   а) введення складного паролю;
   б) використання кількох способів підтвердження особи;
   в) створення резервної копії паролю;
   г) шифрування особистих даних.

6. **Який тип загрози відноситься до кібератак?**
   а) пошкодження обладнання;
   б) використання слабких паролів;
   в) DDoS-атака;
   г) ненавмисне видалення даних.

7. **Що є основним фактором виникнення витоку даних?**
   а) використання сучасних технологій;
   б) несанкціонований доступ або людська помилка;
   в) перевантаження серверів;
   г) регулярне оновлення програмного забезпечення.

8. **Який документ є основою організаційного захисту інформації?**
   а) політика безпеки;
   б) сертифікат відповідності;
   в) контракт із партнерами;
   г) інструкція для клієнтів.

9. **Який метод управління ризиками передбачає передачу відповідальності іншій стороні?**
   а) зниження ризиків;
   б) прийняття ризиків;
   в) передача ризиків;
   г) уникнення ризиків.

10. **Який із наведених інструментів використовується для моніторингу загроз інформаційній безпеці?**
    а) SIEM-системи;
    б) аналітичні звіти;
    в) платіжні системи;
    г) ERP-системи.

11. **Що таке резервне копіювання даних?**
    а) зберігання даних у зашифрованому вигляді;
    б) регулярне створення копій даних для їхнього відновлення;

в) оновлення програмного забезпечення;
г) розподіл доступу до даних.

12. **Що є основною метою міжмережевих екранів (Firewall)?**
а) оптимізація доступу до мережі;
б) захист від несанкціонованих доступів до локальної мережі;
в) зменшення кількості серверів;
г) використання хмарних технологій.

13. **Як людський фактор впливає на інформаційну безпеку?**
а) покращує конфіденційність даних;
б) є джерелом більшості загроз;
в) зменшує потребу у використанні антивірусів;
г) підвищує доступність даних.

14. **Який стандарт регулює захист персональних даних у Європейському Союзі?**
а) ISO/IEC 27001;
б) GDPR;
в) NIST;
г) COBIT.

15. **Що таке фішинг?**
а) вид кібератаки, спрямованої на отримання конфіденційних даних через підроблені
повідомлення:
б) вірусна атака, спрямована на сервери;
в) захист даних від несанкціонованого доступу;
г) резервування копій даних.

16. **Як контролюється доступ до інформаційних систем?**
а) через моніторинг серверів;
б) використання прав доступу та ідентифікації;
в) встановлення антивірусів;
г) оновлення програмного забезпечення.
17. **Що таке SIEM-системи?**
а) програмне забезпечення для резервування даних;
б) інструменти для аналізу та моніторингу безпекових подій;
в) системи управління обліковими записами;
г) сервіси для розподілу доступу.

18. **Що є ключовим завданням аудиту інформаційної безпеки?**
а) виконання фінансового аналізу;
б) перевірка ефективності заходів безпеки;
в) оновлення обладнання;
г) впровадження політик конфіденційності.

19. **Як шифрування допомагає захистити дані?**
    а) приховує конфіденційні дані від сторонніх;
    б) автоматизує моніторинг загроз;
    в) зберігає дані у хмарних сховищах;
    г) видаляє зайві файли.

20. **Який метод забезпечує швидке відновлення даних у разі їхньої втрати?**
    а) шифрування;
    б) резервне копіювання;
    в) використання SIEM-систем;
    г) фільтрація трафіку.

Практичні завдання:

Завдання 1. Аналіз загроз інформаційній безпеці

Мета: Навчитися визначати основні загрози інформаційній безпеці та їхній вплив на діяльність підприємства.

1. Використовуючи наведені дані, визначте типи загроз:
   - несанкціонований доступ до баз даних клієнтів;
   - DDoS-атака на веб-сайт компанії (Distributed Denial of Service – це розподілена атака на відмову в обслуговуванні, яка спрямована на перевантаження веб-сайту або сервера компанії великою кількістю запитів з багатьох джерел одночасно);
   - пошкодження серверного обладнання;
   - витік інформації через помилкові дії співробітників.
2. Розподіліть загрози за категоріями:
   - кібератаки;
   - людський фактор;
   - технічні збої.
3. Опишіть наслідки для підприємства від кожної загрози.

Завдання 2. Оцінка ризиків інформаційної безпеки

Мета: Провести оцінку ризиків та розробити план заходів щодо їх мінімізації.

1. Розгляньте наступні ризики:
   Фішингові атаки: ймовірність 50%, потенційні втрати — 100 000 грн.
   Відмова серверів: ймовірність 30%, потенційні втрати — 200 000 грн.
   Витік даних через людські помилки: ймовірність 20%, потенційні втрати — 50 000 грн.
2. Обчисліть рівень кожного ризику.
3. Запропонуйте заходи для зменшення кожного ризику.
4. Представте результати у вигляді таблиці:

5.

Ризик	Рівень ризику (тис. грн.)	Заходи
Фішингові атаки		Навчання співробітників
Відмова серверів		Регулярне резервне копіювання
Витік даних		Впровадження політик безпеки

Завдання 3. Створення політики інформаційної безпеки

Мета: Розробити основні елементи політики інформаційної безпеки для підприємства.

1. Уявіть, що ви працюєте менеджером із кібербезпеки. Розробіть політику, яка включає:
   - цілі інформаційної безпеки;
   - основні принципи роботи з конфіденційною інформацією;
   - заходи для контролю доступу до інформаційних ресурсів.
2. Визначте:
   - які співробітники матимуть доступ до критичних даних;
   - як перевірятиметься виконання політики.
3. Представте політику у вигляді структурованого документа.

Завдання 4. Оцінка ефективності заходів безпеки

Мета: Аналіз ефективності заходів захисту інформації, впроваджених на підприємстві.

1. Розгляньте впроваджені заходи:
   - встановлення антивірусного програмного забезпечення;
   - використання багатофакторної аутентифікації;
   - резервне копіювання даних.
2. Оцініть:
   - зниження рівня ризиків;
   - економічний ефект від впровадження заходів (зменшення збитків).
3. Представте результати у вигляді таблиці:

Заходи	Рівень зниження ризику (%)	Економічний ефект (тис. грн.)
Антивірусне програмне забезпечення		
Багатофакторна аутентифікація		
Резервне копіювання		

Завдання 5. Впровадження технічних засобів захисту

Мета: Розробити план впровадження технічних засобів захисту для підприємства.

1. Ви отримали інформацію про вразливості підприємства:
   - відсутність антивірусного ПЗ;
   - ненадійні паролі в системах управління;
   - відсутність резервних копій даних.
2. Розробіть план дій:
   - виберіть антивірусне програмне забезпечення;
   - опишіть процедуру створення резервних копій;
   - впровадьте багатофакторну аутентифікацію.

3. Оцініть очікувану ефективність кожного заходу.

Завдання 6. Моніторинг і контроль інформаційних ризиків

Мета: Навчитися проводити моніторинг ризиків та оцінювати їхній вплив на діяльність підприємства.

4. Визначте ключові метрики для моніторингу ризиків:
   - кількість заблокованих кібератак;
   - час відновлення даних після технічних збоїв;
   - частота виникнення витоків даних.
5. Розробіть план моніторингу ризиків:
   - інструменти, які будуть використовуватися;
   - частота проведення моніторингу.
6. Представте результати у вигляді звіту із графіками або таблицями.

ТЕМА 8. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ВРАХУВАННЯ ВПЛИВУ ЗАГРОЗ НА ФУНКЦІОНУВАННЯ ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

8.1 Визначення комерційної таємниці та інтелектуальної власності.

8.2 Юридичний захист інтелектуальних прав та комерційної інформації.

8.3 Протидія тіньовій економіці та корупції в системі економічної безпеки підприємства.

8.4 Функціональний зміст та особливості сучасного рейдерства як фактора впливу на захищеність бізнесу.

8.1 Визначення комерційної таємниці та інтелектуальної власності

Комерційна таємниця — це інформація, яка має комерційну цінність для підприємства, оскільки вона невідома стороннім особам і забезпечує конкурентну перевагу. Ця інформація є об'єктом спеціального захисту, щоб уникнути витоків або зловживань.

Основні характеристики комерційної таємниці:

1. **Конфіденційність** (доступ до інформації мають лише уповноважені особи);
2. **Комерційна цінність** (інформація дає змогу підприємству отримувати конкурентні переваги);
3. **Юридичний захист** (інформація захищається на основі законодавства або внутрішніх політик підприємства).

Приклади комерційної таємниці:

- бізнес-плани та маркетингові стратегії;
- інформація про клієнтів і постачальників;
- рецепти, формули, технології виробництва.

Інтелектуальна власність

Інтелектуальна власність (ІВ) — це результати творчої діяльності людини, які мають економічну цінність і захищаються законодавством.

Основні об'єкти інтелектуальної власності:

1. **Авторські права:** Літературні, музичні, художні твори, програмне забезпечення.
2. **Патенти:** Винаходи, корисні моделі, промислові зразки.
3. **Торговельні марки:** Логотипи, назви, слогани.
4. **Комерційні найменування:** Назви підприємств.
5. **Ноухау:** Унікальні знання, досвід, методики.

Для забезпечення належного рівня захисту та використання відповідних процедур перш за все потрібно ідентифікувати відмінності між комерційною таємницею та інтелектуальною влістністю (табл. 8.1):

Таблиця 8.1 – Відмінності між комерційною таємницею та ІВ:

Параметр	Комерційна таємниця	Інтелектуальна власність
Захист	Внутрішні політики, конфіденційність	Законодавчий захист
Об’єкти	Інформація, бізнес-дані	Твори, винаходи, марки
Строк захисту	Без обмежень при збереженні конфіденційності	Встановлюється законодавством
Приклади	Бізнес-стратегії	Логотипи, наукові відкриття

Сутність захисту комерційної інформації

Захист комерційної інформації — це комплекс заходів, спрямованих на запобігання несанкціонованому доступу, викриттю, або використанню інформації, що має стратегічну або економічну цінність для підприємства. Ефективний захист дозволяє зберегти конкурентну перевагу та уникнути фінансових втрат.

Ефективний захист комерційної інформації дозволяє підприємствам:

- забезпечувати безпеку стратегічно важливих даних;
- мінімізувати ризики витоків і фінансових втрат;
- підвищувати довіру партнерів і клієнтів.

Захист комерційної інформації є комплексним процесом, що вимагає використання технічних, організаційних та юридичних заходів. Такий підхід забезпечує збереження конфіденційності, зменшує ризики та сприяє сталому розвитку бізнесу.

Значення комерційної таємниці та ІВ

1. **Конкурентна перевага:** Збереження інновацій та бізнес-стратегій у конфіденційності.
2. **Фінансова вигода:** Монетизація інтелектуальної власності (ліцензування, продаж патентів).
3. **Захист інновацій:** Недопущення незаконного використання результатів творчої діяльності.

Юридичний захист комерційної таємниці та ІВ

1. **Законодавчий захист:** Регулюється міжнародними стандартами (TRIPS) і національним законодавством.
2. **Договори конфіденційності:** NDA (Non-Disclosure Agreement) захищає інформацію від розголошення.
3. **Реєстрація ІВ:** Патенти, авторські права та торговельні марки реєструються у відповідних органах.

Комерційна таємниця та інтелектуальна власність є важливими активами підприємства, які забезпечують його конкурентоспроможність та фінансову стабільність. Їхній захист повинен бути частиною загальної стратегії економічної безпеки.

Приклади порушень у сфері комерційної інформації та інтелектуальної власності та їх наслідки

1. **Несанкціоноване використання торговельної марки**

Приклад: справа компанії "Adidas"

- **суть порушення:** Порушення прав на торговельну марку "Adidas" шляхом використання схожого логотипу (три паралельні смуги) іншими компаніями;
- **наслідки:**
  - судові позови на сотні мільйонів доларів;
  - вилучення контрафактної продукції з ринку;
  - підвищення обізнаності про захист торговельних марок;
- **юридична основа:** Регламент ЄС №2017/1001 про торговельні марки ЄС.

2. **Крадіжка комерційної таємниці**

Приклад: справа компанії "Google" проти "Uber" (Waymo v. Uber)

- **суть порушення:** Колишній співробітник компанії Waymo (дочірня компанія Google) передав Uber секретні дані про технології для створення безпілотних автомобілів;
- **наслідки:**
  - судове рішення зобов'язало Uber виплатити 245 млн доларів як компенсацію;
  - репутаційні втрати для Uber;
  - підвищення стандартів безпеки для конфіденційної інформації;
- **юридична основа:** Закон США про комерційну таємницю (Defend Trade Secrets Act).

3. **Порушення авторських прав**

Приклад: Справа компанії "Oracle" проти "Google"

- **суть порушення:** Використання Google API Java без відповідного дозволу Oracle для створення операційної системи Android;
- **наслідки:**
  - тривалий судовий процес (більше 10 років);
  - потенційні збитки для Google на мільярди доларів;
  - підвищення обізнаності про авторські права у сфері програмного забезпечення;
- **юридична основа:** Закон США про авторське право (Copyright Act).

4. **Витік конфіденційних даних**

Приклад: Справа компанії "Facebook" (Cambridge Analytica)

- **суть порушення:** Незаконний збір даних мільйонів користувачів Facebook для використання в політичних кампаніях;
- **наслідки:**
  - штраф у розмірі 5 млрд доларів від Федеральної торгової комісії США;
  - репутаційні втрати для Facebook;
  - впровадження жорсткіших регуляцій у сфері захисту даних;
- **юридична основа:** Загальний регламент захисту даних (GDPR).

Порушення у сфері комерційної інформації та інтелектуальних прав мають значні наслідки як для порушників, так і для постраждалих сторін. Ефективний захист є необхідною умовою для збереження бізнесу, фінансової стабільності та репутації.

8.2 Юридичний захист інтелектуальних прав та комерційної інформації

Сутність юридичного захисту інтелектуальних прав

Юридичний захист інтелектуальних прав (ІП) – це комплекс заходів, спрямованих на забезпечення правомірного використання, охорону та захист результатів творчої діяльності та засобів індивідуалізації. В сучасних умовах, коли ІП стає важливим активом підприємства, ефективний юридичний захист є критично важливим.

Юридичний захист ІП включає етапи, подані на рисунку 8.1:

Рисунок 8.1 – Етапи захисту інтелектуальної власності

Законодавча база захисту інтелектуальних прав:

1. **Національне законодавство України:**
   - **Цивільний кодекс України** – регулює права на результати інтелектуальної діяльності, зокрема авторські права, патенти, торговельні марки;
   - **Закон України "Про авторське право і суміжні права" –** охоплює права авторів, виконавців, виробників фонограм;
   - **Закон України "Про охорону прав на знаки для товарів і послуг" –** регулює питання реєстрації та захисту торговельних марок;
   - **Закон України "Про патенти на винаходи і корисні моделі" –** встановлює порядок патентування винаходів.
2. **Міжнародні стандарти:**
   - **Паризька конвенція про охорону промислової власності –** гарантує охорону торговельних марок, промислових зразків, патентів;
   - **Бернська конвенція:** Регулює охорону авторських прав на міжнародному рівні;
   - **Договір ТРІПС (TRIPS):** Встановлює стандарти захисту ІВ в рамках Світової організації торгівлі (СОТ).

3. **Європейські стандарти. Для підприємств, орієнтованих на ринок ЄС, ключовими документами є:**
   - Регламент ЄС №2017/1001 (про торговельні марки ЄС).
   - Регламент ЄС №1257/2012 (про єдиний патент ЄС).
   - Директива ЄС №2001/29 (про авторське право в цифрову епоху).

Механізми юридичного захисту (табл 8.2):

1. **Реєстрація прав інтелектуальної власності**
   - **авторські права –** реєстрація в Міністерстві економіки України для забезпечення доказів авторства;
   - **патенти –** подання заявки до Українського інституту інтелектуальної власності (Укрпатент);
   - **торговельні марки** – реєстрація у національних органах або через систему Мадридської угоди.
2. **Ліцензування та передача прав**

   Підприємства можуть передавати права на використання ІВ через ліцензійні договори. Це дозволяє монетизувати об’єкти ІВ. Так, наприклад, українські ІТ-компанії активно продають ліцензії на використання програмного забезпечення закордонним партнерам.
3. **Судовий захист**

   У випадку порушення прав ІВ передбачено звернення до суду для:
   - заборони використання об’єктів ІВ;
   - відшкодування збитків;
   - вилучення контрафактної продукції.

   Наприклад, у 2023 році українська компанія "Розетка" виграла справу проти контрафактних продавців, які незаконно використовували її бренд.
4. **Міжнародна співпраця**

   Україна співпрацює з:
   - Європейським патентним офісом (EPO);
   - Всесвітньою організацією інтелектуальної власності (WIPO).

   Це дозволяє українським компаніям отримувати міжнародний захист своїх прав.

Таблиця 8.2 – Порівняння юридичних механізмів захисту

Механізм	Переваги	Недоліки
Реєстрація прав	Забезпечує доказ авторства	Вимагає часу та витрат
Ліцензування	Монетизація об’єктів ІВ	Залежність від умов договору
Судовий захист	Відновлення порушених прав	Тривалість розгляду справ
Міжнародна співпраця	Захист на глобальному рівні	Висока вартість міжнародної реєстрації

Юридичний захист інтелектуальних прав дозволяє підприємствам:
- зберігати унікальні бізнес-інновації;
- забезпечувати конкурентну перевагу;
- захищати від контрафактної продукції та порушень прав.

Юридичний захист інтелектуальних прав є критично важливим елементом економічної безпеки підприємства. Сучасне законодавство, міжнародні стандарти та інструменти захисту забезпечують ефективне управління інтелектуальними активами та їх охорону.

8.3 Протидія тіньовій економіці та корупції в системі економічної безпеки підприємства

Немає жодних сумнівів, що сучасна економіка нашої держави складається з легальної та тіньової.

Якщо легальна економіка входить до народногосподарського комплексу України та існує в чітко визначеному правовому полі та в тісній співпраці з різними державними інституціями, то наявність тіньового сектора в економіці країни зумовлена виключно корисливими інтересами, нестримним намаганням будь-яким способом налагодити підпільне виробництво, забезпечити протизаконну торгівлю товарами та послугами, приховування від держави доходів, застосування методів недобросовісної конкуренції на всіх рівнях, монополізації та інших шляхів для отримання неоподатковуваних надприбутків.

Саме поняття «тіньової економіки» походить від англ. «Black economy», «Ghost economy», «Shadow economy» і означає такий вид господарської діяльності, яка формується та розвивається, оминаючи державний контроль та облік, завдяки чому не включається в офіційній статистичній базі. Підприємства, які задіяні у «тіньовому» секторі не беруть участі у наповненні державного бюджету та різноманітних цільових фондах. Завдяки уникання сплати податків їм вдається суттєво збільшувати власні прибутки.

У науковій літературі використовуються найрізноманітніші назви: чорна, тіньова, незаконна, нелегальна, підпільна, прихована, не відображена, кримінальна, нерегламентована, неофіціальна – хоч сутність цього явища залишається незмінною. У сучасному світі доходи від тіньової економічної діяльності сягають величезних розмірів, вони обчислюються десятками мільярдів доларів, але заходи, яких вживають правоохоронці виявляються дуже незначними і не дозволяють чітко встановити масштаби проблеми.

Відносно терміну «тінізація» виробничої сфери України можна констатувати наявність певних принципових розбіжностей. Мається на увазі, на що саме уряд дає дозвіл, а на що накладає заборону. Відповідно, наявні заборони урядовому рівні лежать в площині моралі та ділової етики, або заборони є жорсткішими, зокрема перебільшеними, може мати місце заборона того, що не суперечить морально-етичним нормам, або навпаки, нехтувати усталеним морально-етичним принципам, надаючи певні дозволи.

З позицій пересічного громадянина торгівля наркотичними засобами, продаж зброї масового ураження, заняття проституцією належать до неприйнятних, вважаються такими, що принижують людську гідність, є недопустимими та повинні бути заборонені. У такому випадку відбувається збіг морально-етичних та адміністративно-правових засад, які одностайні в тлумаченні подібних дій.

Проте зазвичай до тіньового сектора урядовцями відноситься широкий спектр дій: від засуджених з точки зору моралі та етики до інших. Насамперед, діяльність малого бізнесу не відноситься до забороненої на морально-етичному рівні та не порушує адміністративно-

правових норм. В той же час, коли така діяльність лежить в площині завищеного оподаткування, то виробник керуючись не прагненням до власного збагачення, а лише можливістю до ймовірного виживання, ставиться в рамки уникнення сплати непомірних податків. Тому таке явище набуває статусу нелегальної економіки.

З огляду на це можна констатувати, що адміністративно-правові норми далеко не завжди співзвучні моральним та етичним критеріям.

Якщо має місце очевидна узгодженість з адміністративно-правовими нормами морально-етичних, людська спільнота загалом підтримує їх, як наслідок – покращується продуктивність протистояння тіньовій економіці. Громадськість у даному контексті розуміє детінізацію як вимушені дії урядових структур покликані захистити широкі верстви населення.

За умов більш жорсткої заборони на адміністративно-правовому рівні, спільнота демонструє нейтральне сприйняття, розцінюючи ініціативи уряду не в площині інтересів громадян, а швидше за все як захищеність безпосередньо урядових інституцій. Це повною мірою відноситься до посилення податкового тиску на високоприбуткові сфери, зокрема виробництво тютюну, яке обґрунтовується шкідливими наслідками тютюнопаління, хоч ймовірніше зумовлене не опікуванням проблемою збереження здоров'я населення, а цілком корисливою метою – збільшенням надходжень до державного бюджету. Таким чином створюється сприятлива база для нелегальної економічної діяльності, як от контрабанда значно дешевших українських цигарок до європейських країн, зокрема до Польщі.

У випадках, коли уряд постійно і неконтрольовано вводить жорсткі обмеження та ініціює заборони, тоді подібну економічну діяльність громадяни сприймають як необґрунтовану політику, що сприяє подальшому збагаченню олігархічних кіл та одночасному різкому падінню рівня життя населення країни. Ефективність протистояння тіньовому секторові у такому випадку є вкрай незадовільною, так як пересічні громадяни можливість виживання ототожнюють з функціонування наявної нелегальної економічної діяльності. Водночас, привертає увагу те, що подібний стан короткочасовий, незважаючи на те, що тіньова економіка динамічно розширюється, проникає у різні економічні сфери, включаючи промислову діяльність. Для пересічного громадянина це не вихід із складної ситуації, проте є ефективним джерелом протизаконного непомірного збагачення порівняно невеликого прошарку високопосадовців, які прагнуть потрапити до владних державних органів задля просування та забезпечення власних вигід, унеможливлюючи достойне життя переважної частини населення країни.

Потребує всебічного розгляду сутність тіньової економіки. З погляду економіко-статистичного підходу тіньова економіка включає різні види економічної діяльності, які належним чином не відображені в офіційній статистиці. В юридичній площині тіньовими можна вважати такі економічні процеси, які відбуваються поза межами правового поля. Етичний бік полягає в тому, що така діяльність порушує усталені морально-етичні норми та закони, в результаті чого не піддається моральному осуду. В економічному аналізі варто виходити із економіко-статистичного розуміння тіньової економіки.

Загальновідомо, що наразі немає жодної сфери економіки, у якій би не існував нелегальний сектор і не відчувався його вплив. Обсяги «тіньової економіки» залежать від економічного порядку в державі: чим сильніша державна влада, досконаліша законодавча платформа й оптимальніша система державного управлінні, тим менш значимим є тіньовий

сектор економіки, і навпаки. Наявність «тіньової» складової в економіці тісно пов'язана з проблемою стану економічної безпеки країни, що зумовлює її актуальність.

На жаль, існування тіньових економічних відносин залишається найбільш суттєвою перешкодою на шляху формування стійкого економічного поступу, покращення добробуту, підвищення загального рівня та якості життя населення держави та, відповідно, посилення національної безпеки.

Процес переходу від доіндустріального суспільства до епохи індустріальної створив сприятливі умови для виникнення тіньової ділової активності в багатьох сферах і різновидах. Зокрема, окремі форми, що мали місце у процесі капіталістичному виробництві, – такі, як «розпорошена» мануфактура, існували як нелегальна конкуренція цілком легальній цеховій організації. Водночас піратство як явище активно поширювалося впродовж XVI–XVIII ст. у басейні Середземного та Карибського морів, на водному просторі Індійського океану, створюючи реальну та масштабну загрозу морським перевезенням, а розкрадання державної скарбниці та поширення корупційної складової притаманні були всім абсолютистським державам. Цілком ймовірно, що таке тіньове ділове пожвавлення стало своєрідною відповіддю на зміцнення влади вельмож, що не була закріплена на інституційному рівні. По суті капіталізм у сучасному розумінні закріпився тільки після того, коли «протестантська етика» проголосила та схвалила прагнення до збагачення лише у вигляді «чесного бізнесу», який засновувався на конкурентній основі та не допускав насильства. Окреслений період нового часу узаконив певні форми тіньового сектора, зокрема лихварство перетворилося на банківську діяльність, та водночас розпочав жорстку боротьбу з криміналізованими його різновидами у вигляді комп'ютерного піратства та корупції.

Глобальні трансформаційні процеси у світовому економічному просторі спричинили появу якісно нової стадії розвитку нелегальної економіки у другій половині XX ст. Як наслідок – у розвинених країнах явище іллегалізація економіки, що спостерігалось у середині XX ст., пришвидшила їх перехід до постіндустріального етапу та інформаційного суспільства. У країнах соціалістичного табору стрімке розширення тіньового сектора економіки було спричинене існуванням директивно-планової економіки, яка мала численні вади і поступалася ринковій моделі. Стислий виклад причин масштабної та стрімкої тінізації у соціалістичній економіці надано американським вченим-економістом М. Олсоном, за його словами, у разі відсутності інституту приватної власності, у всіх громадян виникає матеріальна зацікавленість у неконтрольованому розкраданні державної власності, оскільки ніхто не мотивований до його збереження».

Існування тіньової складової в економіці залишається поширеною та значною вадою світового масштабу, проте найбільш виразно це виявляється в країнах з перехідною економікою. Наявність нелегальної економіки є болючою проблемою для політиків, оскільки у населення немає довіри до офіційних показників: масштабів безробіття, частки економічно активного населення, рівня доходів громадян і масового споживання.

Побутує поширена думка, що спад легальної економіки тісно пов'язаний з обсягами тіньового виробництва: спад легальної економіки відбувається на фоні підйому тіньової. Проте це не звичайна лінійна залежність, де розширення тіньової складової відбувається завдяки переходу значних економічних ресурсів з легальної площини в нелегальну. Зростання легальної сфери економіки гальмується динамікою тіньової, яка ефективно використовує власні переваги. Наразі в тіньовій площині економіки створено оптимальний інвестиційний клімат, що дозволяє досягти значного сумарного зростання, яке перевищує

відповідні показники легального сектора. Все це дає підстави стверджувати про невигідність легальної економічної діяльності через її низьку продуктивність.

Загалом, нелегальна економічна діяльність значно гнучкіша та динамічніша порівняно з легальною, адже вона оперативно займає нові ніші та доволі швидко створює відповідні умови для використання трудових ресурсів. Сьогодні тіньова економіка активно наповнює внутрішній та зовнішній ринок різними товарами та послугами, суттєво підвищує доходи певної частини населення країни, пожвавлює конкуренцію і тим самим гальмує на якийсь період руйнівні процеси в соціальному середовищі. Попри зазначені переваги не варто применшувати й негативний вплив нелегальної складової на економіку держави, адже через наявність тіньової економіки значною мірою зменшуються надходження до державного бюджету, постійно збільшується зовнішній і внутрішній борг країни, нагромаджується нелегальний капітал, втрачається інвестиційна привабливість окремих галузей та держави в цілому, зменшуються інтегративні можливості. В умовах, коли держава не виконує свої контрольно-регулятивнч і низку інших функцій, через неможливість впоратися з тіньовим сектором, посилюється криміналізація суспільства та спостерігається швидке зростанням організованої злочинності. В результаті чітко налагоджена схема тіньового обігу ВВП спрямовується, насамперед, на відтік капіталу, в той час, як суттєво скорочується частка капіталу, яка залишається або інвестується у національне виробництво у формі прямих іноземних інвестицій, що може бути розцінено як відмивання нелегального капіталу.

Аналізуючи причини стрімкого розширення тіньового сектора економіки, Кухоль І.М. пов’язує цей процес з економічними, соціально-правовими та державними факторами (рис. 8.2).

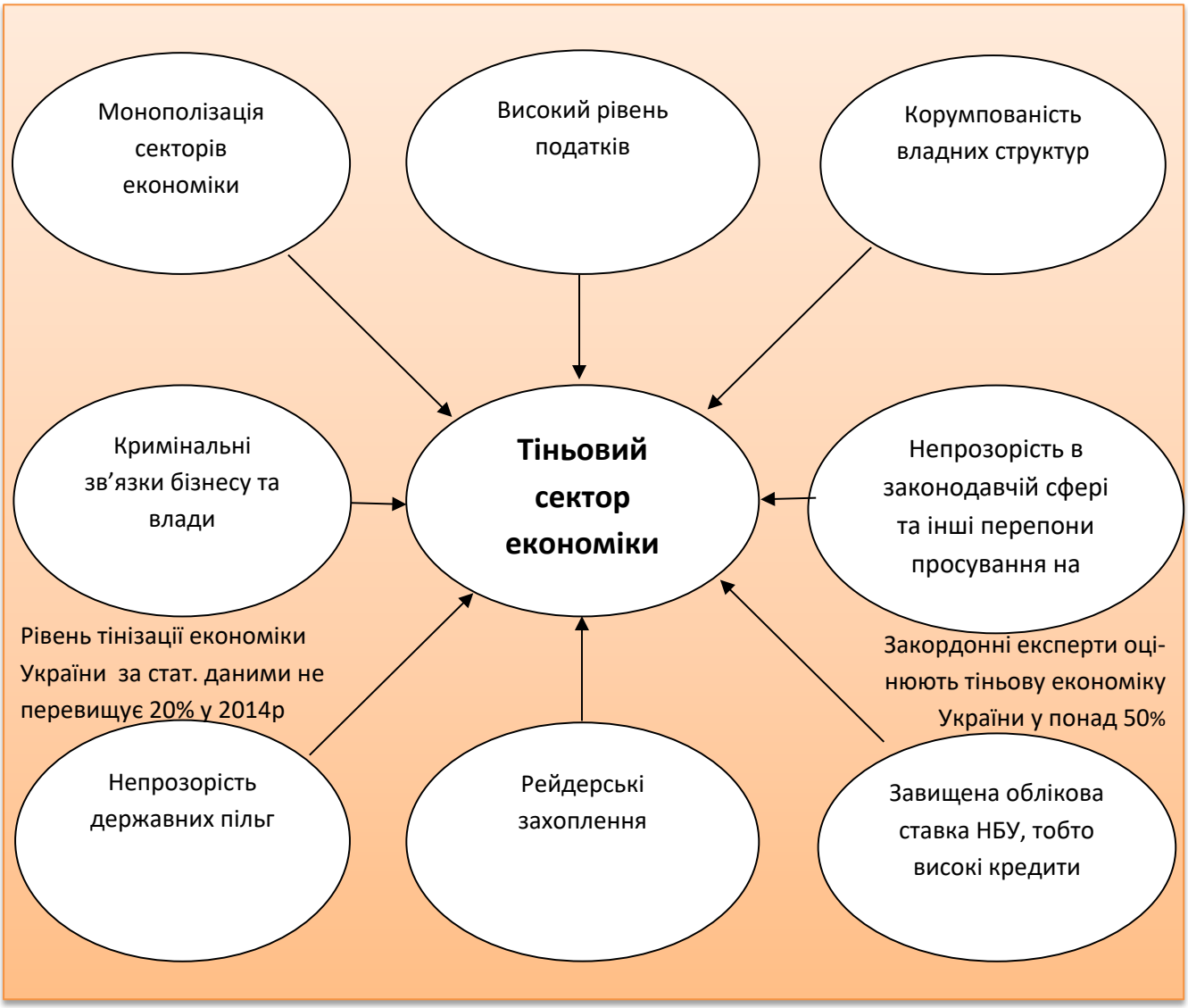

Рисунок 8.2 – Чинники тінізації бізнесових структур

У наукових джерелах виділяють, як правило, тіньову економіку трьох типів.

Перший тип (так звана «**неформальна економіка**») є наслідком недосконалої системи господарювання. зокрема, в період СРСР існував «торг» між підприємствами та органами планування за отримання необхідних ресурсів.

«Другий» тип тіньової економіки («**фіктивна**») наданий економічною діяльністю кадрів легальної економіки, яка здійснюється поза правовим полем і базується на прихованому перерозподілі національного доходу, який сформовано раніше. Крізь суспільну призму такий тип тіньової економіки не продукує жодної товарної продукції чи послуг, тому зиск від «другої» економіки, отримують одні, в той час як інші зазнають збитків.

Третім типом тіньової економіки є «**сіра**» – це такий різновид економіки, коли відбувається процес виробництва та продажу традиційних товарів і послуг, що не заборонені законом, який належним чином не фіксується. Така діяльність має місце переважно в сфері дрібного бізнесу. Суттєвою відмінністю другого типу від третього, є нерозривний зв'язок з легальною економікою, за рахунок якої він і існує тоді, як «сіра» економіка існує сама по собі. Ця площина ґрунтується на усвідомленому ухилянні виробників від належного обліку з

метою мінімізації витрат на ліцензування, сплату податків тощо чи відсутності вимог щодо обов'язкового звітування про таку виробничу діяльність.

Отже, що «чорна» тіньова економіка – це заборонена законом економічна діяльність організованої злочинності, яка являє собою виробництво та продаж недозволених товарів і послуг. До «чорної» економіки можна віднести таку діяльність, яка не надана в звичайному економічному просторі через те, що є абсолютно несумісною з ним і має на нього деструктивний вплив. Найбільш поширеними формами «чорної» економіки є наркобізнес, торгівля людьми, пограбування тощо).

Слід зазначити, що різні складові неформальної економіки по різному впливають на суспільно-економічне життя держави.

Вплив держави на економічну сферу виявляється через реалізацію бюджетної, грошово-кредитної, податкової політики тощо, тому, ґрунтовно вивчивши методи взаємодії тіньової складової вітчизняної економіки з легальною сферою, можна виробити та втілити в життя політику детінізації економіки.

Треба наголосити, що застосовувані державою у різні періоди і в різних формах покарання виявляються неефективними через те, що процес вилучення значних коштів зі сфери тіньового виробництва спричинює капіталізацію економіки, наслідком якої є суттєве зниженням рівня зайнятості населення, спад сукупного попиту та сукупної пропозиції. Це врешті-решт призведе до зниження інвестиційного потенціалу подальшого економічного розвитку в державі.

Як правило, тіньова економіка супроводжується тими соціальними явищами, які зумовлюють застосування тіньових схем господарювання та є свого роду основою виникнення тіньових відносин. Це стає можливим завдяки тому, що певний соціальний індивід є членом якихось легальних соціальних об'єднань, що може стати основою для виникнення тіньової економіки, яка може бути наслідком вчинків, якими вдалося уникнути, «обійти» існуючі народногосподарські інститути: офіційної звітності, процедури ліцензування, здійснення податкових операцій. В таких умовах сама тіньова економіка інтегрована до інституціонального простору, але нехтує формальними інститутами.

З-поміж найбільш вагомих соціально-економічних наслідків існування тіньового сектора економіки виділяються:

1. Суттєве зменшення реальних доходів населення країни. Доходи понад 33% населення нижчі за встановлений прожитковий мінімум. В результаті цього суттєва частина населення може стати потенційним джерелом розширення «трудових ресурсів» кримінального середовища, водночас через вкрай низький рівень життя такі громадяни стоять осторонь від значимих економічних процесів.

2. Критичне зниження можливостей до відтворення. На сучасному етапі відбувається активний процес значного знецінення й так званого «проїдання» наявних основних та оборотних фондів. Лібералізація цінової політики та приватизація в нашій державі відбувалися так, що врахування основного капіталу в фінансовій звітності здійснювалося за залишковою вартістю станом на початок року, тоді як сировина та енергоносії виражались у вільних ринкових цінах; це спричиняло штучне завищення показників про прибуток, а в

подальшому «проїдання капіталу». Така «економія», що формується в результаті «безкоштовного» користування основними коштами може бути домінуючою характеристикою сучасного етапу.

3. Зниження інвестиційної активності, вичерпання внутрішніх джерел надходжень. Відбувається безперервний процес зменшення капітальних вкладень, а в їх структурі – інвестицій у виробництво. Водночас, спостерігається суттєве погіршення фінансового стану промислових підприємств, згідно зі статистичними даними загалом по Україні кількість збиткових підприємств складає 43%, а в окремих сферах цей показник становить 60–80% у 2014 р.

4. Дисбаланс і відсутність чіткої продуманої державної фінансової політики та стабільної грошової систем. Впродовж останнього періоду вітчизняна економічна система демонструє руйнування внутрішніх зв'язків і не дотримання необхідного балансу, в результаті цього відбувається широкомасштабне перекачування капіталу зі сфери виробництва у сферу обігу з подальшим переведенням значних коштів за межі країни.

5. Глибока криза на рівні соціально-економічного управління. Категорично відмовившись від усталених методів централізованого управління, Україна не змогла налагодити дієві механізми регулювання соціально-економічних процесів. Як наслідок – процес приватизації відбувався на фоні жорсткої боротьби за контролювання державної власності та державних фінансів; а після її завершення відбулася легалізація кримінальної діяльності, злиття урядових і «придворних» комерційних структур. Найбільш відчутним це стало у бюджетній сфері, наразі повністю ліквідовано можливість суспільного контролю влади.

Відійшовши від планової економіки і вступивши в перехідний етап Україна зіткнулась з величезною проблемою тіньової економіки – виробництва, розподілу, обміну та споживання різноманітних товарно-матеріальних цінностей та користування послугами, які не контролюється суспільством. В результаті цього тіньова економіка в нашій державі переросла у масштабну загрозу національної безпеки, адже її вплив на людську спільноту й державу характеризується системністю та комплексністю.

На макроекономічному рівні з проблемою тінізації економіки довелося мати справу практично всім країнам. Це сформувало хибну думку про те, що тіньова економіка є результатом жорсткого державного контролю в економічній галузі, що змусило з більшою увагою підійти до розуміння та осмислення цього явища.

У середовищі науковців можна виділити цілий спектр підходів, які засвідчують, що тіньова економіка являє собою економічну діяльність, яка суперечить чинному законодавству, комплекс незаконних господарських операцій, які фінансують кримінальні структури.

Існує й інший підхід, за яким під «тіньовою економікою» прийнято розуміти невідображені в офіційній статистиці виробництво, обмін, розподіл і споживання матеріальних благ, що не підпадають під суспільний контроль.

Натомість нерідко до тіньової економіки зараховують види діяльності, які спрямовані на стійке формування або повне задоволення потреб, що спричиняють виникнення в людини ниць характеристик і потягів до задоволення подібних потреб.

Зазначені підходи певною мірою мають сенс, адже вони враховують, щоправда різною мірою, реальні економічні процеси, описують тіньову економіку з різних сторін і не суперечать одне одному.

У період колишнього СРСР виникли тенденції, які значною мірою сприяли тінізації економіки, зокрема потужним поштовхом можна вважати культивовану пріоритетність «суспільної» (колективної) власності. За таких умов не було реального, зацікавленого у збереженні майна та розвитку підприємництва, корпоративного власника, на якого була б покладена чітка відповідальність за капіталізоване майно, з огляду на це у людини з радянським мисленням сформувалося відчуття безкарності або навіть заохочення до розкрадання зазначеного майна за допомогою використання посадовими особами свого службового становища з корисливою метою. Законодавча база колишнього СРСР, зокрема Закон «Про кооперацію в СРСР», дозволяв організовувати приватні підприємницькі структури, найчастіше – кооперативи, тому державні підприємства та установи, нехтуючи установленим порядком в сфері законного використання як державної, так і приватної власності, створювали на своїй базі кооперативи. Власне, керівники суб'єктів господарювання державної форми власності організовували кооперативи в якості комерційних структур на самому підприємстві, яке вони очолювали, що дозволяло використовувати різноманітні тіньові схеми переведення державного майна в кооперативну власність. Така зміна форми власності відбувалася зі злочинним використання посадовцями своїх владних і службових повноважень.

З часом запроваджений державою процес приватизації набував характеру криміногенного, що було зумовлено низкою сприятливих обставин: свідоме заниження реальної вартості пакета акцій, стислі терміни, які не дозволяли належним чином підготуватися, проведення аукціонів з порушенням умов ринку, відсутність під час проведення аукціонів реальної конкурентної боротьби, що перетворювало такі заходи у простий переділ державної власності. Водночас власники акцій нехтували своїми інвестиційними зобов'язаннями, подавали документи, які містили недостовірну інформацію тощо. На базі радянської тіньової приватизація подальшому сформувалася потужна тіньова економіка в масштабах величезної держави, а згодом і на всьому пострадянському прості, в тому числі і України.

Як показують дослідження, здійснені Ф. Шнайдером, тіньова економіка представляє собою середню частку 41% ВВП в країнах, які розвиваються, 38% в країнах з перехідною економікою, і 17% в країнах Організації економічного співробітництва і розвитку (ОЕСР).

На підставі аналізу господарської діяльність суб'єктів господарювання з валовим доходом більше одного мільйона гривень, виявлено, що тіньовий сектор вітчизняної економіки має до 17% обігу коштів великого та середнього бізнесу. Наукові розробки, присвячені проблемам регіональної економіки, засвідчують, що найбільші масштаби нелегальної економічної діяльності спостерігаються в Дніпропетровській, Харківській, Одеській, областях і в Києві. В цьому контексті дуже висока частка підприємств, які вдаються до мінімізації податків і мають оборот більше одного мільйона гривень працюють у Харківській області – 16,7% загального обороту, порівняно високу частку в структурі економіки регіонів тіньовий сектор має в Одеській (15,2%) та Черкаській (13,4%) областях.

Разом з тим, із 22 мільйонів соціально активного населення нашої держави регулярно та в повному обсязі сплачує податки лише 14 млн осіб.

Хоч побутує думка щодо значних обсягів тіньової економіки, її місце в системі розподілу ресурсів і ринковому середовищі до кінця не встановлене, а через це має суперечливі оцінювання. За переконанням Шнайдера Ф. та Енсте Д., загальні обсяги, головні

причини та найбільш вагомі наслідки тіньової економіки суттєво відрізняються у різних державах. Тому слушною й аргументованою є думка Ткаченко В.Г., яка стверджує, що потрібний диференційований підхід до зупинення процесу тінізації економіки потрібно, варто брати до уваги усіх можливі загроз і прогнозовані наслідки.

Вагомий внесок у систематизацію наявних наукових підходів до вивчення основних дієвих механізмів, на яких ґрунтується тіньова економічна діяльність, зробив Турчинов О.В. На його переконання «тіньова економіка – це такий вид економічної діяльності, який зовсім не враховується і належним чином не контролюється відповідними державними інституціями, а також економічна діяльність, яка полягає у отриманні максимально можливого доходу через порушення норм чинного законодавства». Однак, запропоноване визначення можна застосувати практично для більшості злочинів, зокрема пограбування, розбій, вимагання, тому таке бачення неприпустимого розширює рамки тіньової діяльності. Академік Богачов В.І., всебічно вивчаючи загальний стан тіньової економіки в державі, пропонує таке тлумачення тіньової економіки – це не лише сторони суспільного життя, які виходять за рамки економіки, зокрема, незаконний продаж зброї, торгівля наркотичними засобами, проституція тощо, а насамперед, нехтування законами, уникання сплати податків, що можуть мати місце у будь-якій сфері господарської діяльності.

Сам факт існування та постійне зростання обсягів тіньової економіки спричиняє цілу низку складних проблем. Наслідком може бути недостовірність офіційних статистичних даних про рівень безробіття в країні та його динаміку, рівень добробуту, ВВП, соціально-економічні умови людського існування та домашніх господарств. З огляду на це офіційна статистика про кількість безробітних не враховує тих, хто власне задіяний у виробничій діяльності на чорному ринку, за що отримує певний неврахований прибуток. В результаті такі статистичні похибки не дають повної інформаційної картини, що не дозволяє об’єктивно оцінити реальний стан і може вплинути на політичну державну систему.

Між показниками масштабів тіньової економіки й офіційно зафіксованим рівнем безробіття існує взаємозалежність, адже у середовищі безробітних певну частину складають задіяні на підпільних роботах працівники.

Дослідження, здійснені Ф. Шнайдером і Д. Енсте показують, що рушійними силами тіньової економіки є інтенсивність регулювання та витрат на оплату праці, що також може розглядатись в якості причини зростання тіньової економіки. В цьому контексті дуже часто обмірковуються два головних аспекти – скорочення кількості робочого часу на тиждень і рівень безробіття.

З огляду на розбіжності в офіційних і реальних даних щодо чисельності працездатного населення, варто зауважити, що якщо загальна кількість працездатного населення залишається без змін, то падіння даного показника в легальній економіці є сигналом до його зростання в тіньовому секторі. Проте слід зважати й на те, що велика кількість працездатного населення задіяна одразу і в офіційній і в тіновій економіці.

Можна переконливо стверджувати, що тіньова економіка – це значною мірою явище об’єктивне, воно існувало в усі часи: від виникнення товарно-грошових відносин і запровадження державою певних заборон і введення обмежень, інакше кажучи – тобто нормативно-законодавчих правил економічної діяльності. Суспільний досвід засвідчує відсутність доброї волі до їх неухильного дотримання, через це викорінити тіньову економіку практично нереально, можна вводити для неї певні обмеження, використовуючи державні економічні механізми, або створювати несприятливий клімат для її розвитку.

Вкрай важливо усвідомлювати, що різні сфери тіньової економіки непропорційні до ступеня загроз економічній безпеці, як правило, вони відрізняються можливостями та масштабами процесів тінізації.

Формування продуктивної системи безпеки сучасного економічного розвитку в контексті глобалізації процесів як методу ефективної протидії розширення масштабів тіньової економіки та поступового ліквідування цього руйнівного елітного сектора ґрунтується передусім на системі чинників, де ключова роль належить формі державного устрою.

Сучасні реалії функціонування та головні причини, що спонукають до розвитку тіньової економіки в певних галузях національних економічних систем, узагальнені у наукових розробках Зінов'єва Ф.В. та Рутова В.Є. На наш погляд, їх варто розширити з урахуванням домашніх господарств (табл. 8.3).

Таблиця 8.3 – Сектори економіки, інструменти та причини тінізації

Сектори економіки	Інструменти тіньової діяльності	Причини тінізації
1	2	3
Матеріальний сектор виробництва	– уникнення офіційної реєстрації господарської діяльності; – надання недостовірної інформації під час реєстрації господарських договорів; – заниження обсягів вироблення товарної продукції задля ухилення від оподаткування реального прибутку; – продажа товарної продукції за готівку; – виплата заробітної плати «у конвертах»; – готівковий розрахунок за послуги постачальників	– необґрунтовано високі ставки оподаткування; – несталість, недосконалість та суперечливість вітчизняного податкового законодавства; – продаж не облікованої товарної продукції; – непрозорість та бюрократична заплутаність в ліцензуванні виробничої діяльності
Зовнішньоекономічний сектор	– незаконний експорт-імпорт; – фіктивні постачання та договори; – викривлення контрактних цін; – експортування продукції за демпінговими цінами; – реєстрування суб'єктів господарювання в офшорних зонах; – недотримання термінів платежів за експортування та імпортування товарів; – нехтування митними нормами; – запровадження процедур фіктивного нарахування і повернення НДВ; – нестача, втрата чи «псування» товарної продукції за кордоном; – приховування імпорту під виглядом транзитних перевезень митною територією держави; – експортування продукції з високою ліквідністю із залученням офшорних компаній	– нестабільність вітчизняного законодавства; – недосконалість та корумпованість митного контролю; – постійна зміна курсу національної валюти; – відсутність державного захисту та гарантій у збереженні заощаджень; – умови для безакцептного списання або беззаперечного стягнення заборгованостей; – постійна змінюваність митних тарифів; – ускладнена процедура ліцензування.

Продовження таблиці 8.3

1	2	3
Банківський сектор	– неефективність депозитів; – привласнення відсотків по дивідендах та вкладах (або цінних паперах) контрагента; – незаконні оборудки з цінними паперами; – використання незабезпечених чеків; – застосування платіжних доручень, що супроводжуються фіктивними кредитними авізо; – використання незабезпечених кредитних карток; – шахрайство в сфері операцій з векселями й акредитивами	– недосконаліть контролюючих структур нагляду за банківською сферою; – не розробленість нормативної бази з окремих питань роботи банківської системи; – нестійкість, непрогнозованість і неправильне розуміння чинної нормативної бази; – відсутність градації банківської інформації за рівнем конфіденційності та доступності для органів державного контролю
Приватизаційний сектор	– заниження реальної вартості об'єкта, який приватизується; – свідоме доведення до банкрутства підприємства з подальшою його приватизацією; – відсутність контролю за зберіганням та ефективним використанням державної власності під час приватизації; – застосування посередницьких схем під час продажу товарної продукції	– відсутність концепції та певна неоформленість процесу роздержавлення; – недоліки в методиці оцінювання реальної вартості підприємства, яке приватизується; – приватизації значної частини об'єкту без оплати; – залучення інвестицій на безконкурсній основі
Державний сектор	– спотворення даних про результати виробничої діяльності; – хабарі для вирішення питань виробничо-господарської діяльності; – використання неформальних зв'язків для вирішення виробничих проблем; – неофіційний обмін ресурсами; – ліцензування на безконкурсній основі	– відсутність продуктивної системи обліку; – недоліки у розподілі та наданні пільг; – недосконаліть нормативно-законодавчої бази господарської діяльності
Сектор домашніх господарств	– застосування засобів для задоволення власних потреб і для продажу залишків на ринку; – використання найманої робочої сили	– нерозробленість процедури обліку отриманої пропозиції; – недосконаліть нормативно-законодавчої бази господарської діяльності

Стійкість та розширення тіньової складової в економіці нашої держави спричинена незадовільним станом реалізації економічної політики, включаючи недосконаліть нормативно-правової бази для ефективної господарської діяльності. У зв'язку з численними розбіжностями між цивільними та господарськими законодавчими нормами створюються сприятливі умови для нехтування ними, а як наслідок – формування в державі неофіційної та прихованої економіки. Разом з тим, суттєвим чинником, який спричиняє тінізацію економічної діяльності, є вітчизняна система оподаткування фіскального характеру, яка забезпечує значні відрахування до бюджету шляхом завищених податкових ставок. Процес формування вітчизняної податкової системи припав на період кризи, що спричинило певні труднощі з надходженнями до державного бюджету. Тим не менш відбувається постійне збільшення державних видатків. Цей стан зумовлюється потребою у неухильному виконанні державою певних функцій, спрямованих на розвиток ринкової економіки, на державну підтримку виробничої діяльності, запроваджену радянською системою. Загалом впродовж 1992–1999 рр. державні видатки, за винятком витрат на оборонний комплекс, збільшилися в 3,6 разів в той час, як обсяги виробництва знизилися вдвічі. Власне це свідчить про те, що витрати з держбюджету значно перевищували економічний потенціал країни. Наслідком такого дисбалансу стало приховування реальних прибутків суб'єктами підприємництва.

За умов поширення девальваційних і цінових шоків, ескалації військового конфлікту Мінекономіки зазначає, що з початку 2015 року спостерігалося подальше суттєве збільшення тіньового сектору, що розпочалося в 2013 р. Відповідні красномовні дані подані в аналітичному огляді тіньової економіки в Україні. Крім того, в цьому документі зазначено, що показник тінізіції на рівні понад 40% у розрізі окремих регіонів характерний для країн Африки та Латинської Америки. Згідно даних Мінекономіки, три з чотирьох методів оцінювання рівня тінізації, показали її збільшення. Так, за методом збитковості підприємств зафіксовано зростання тіньової економіки на 8 п. п., за методом «витрати населення-роздрібний товарооборот» – на 5 п. п., до 56%, до 50%, за електричним методом – на 6 п. п. до 38%. І лише за монетарним методом зафіксовано зниження рівня тіньової економіки на 1 п. п. (до 35%).

Держкомстат України впродовж останніх років зазначає, що тіньовий сектор – це в середньому 15%–18% валового внутрішнього продукту. Ці цифри значно різняться від даних, що мають інші служби та науковці. Так, відповідно до розрахунків Мініекономіки України обсяг тіньової економіки нашої держави за 5 років становить 28%–39% валового внутрішнього продукту. Цей показник було розраховано різними методами: «витрати населення – роздрібний товарообіг», електричним, монетарним, фінансовим (табл. 8.4).

З таблиці 8.4 видно, що динаміка тіньової економіки в Україні за останні два десятиліття демонструє постійну і структурну присутність прихованих економічних процесів, які варіюються в межах від 15% до понад 50% ВВП — залежно від обраної методології. В умовах перманентної політичної нестабільності, економічної вразливості та війни, тіньовий сектор не лише зберігається, а й періодично загострюється. Оцінка за Держкомстатом є найнижчою серед усіх, оскільки відображає суто офіційний адміністративний підхід до оцінки тінізації. Частка знизилася з 18,9% у 2004 році до 15,1% у 2008, що відповідало періоду економічного зростання. Проте після кризи 2008–2009 рр. та особливо з початком війни у 2014 році показники зростають, досягаючи 33,5% у 2022 році. Це є важливим сигналом: офіційна економіка втратила контроль над частиною господарських процесів. Метод “витрати населення – роздрібний товарообіг” стабільно демонструє високі значення тіньового ВВП: 40–50%, що вказує на значне розходження між офіційно облікованими доходами та реальними витратами домогосподарств. Особливо тривожним є зростання після 2022 року, яке може бути зумовлене сплеском готівкових розрахунків, бартеру та допомоги, що не враховується статистикою. Міжнародна методика професора Шнайдера, заснована на MIMIC-моделі, традиційно дає найвищі значення. Її пік припадає на 2014 рік – 52,8%. Це підтверджує: війна, анексія Криму, падіння банківської системи призвели до втрати контролю над великими економічними потоками. Інтегральний показник Мінекономіки є компромісним і дає збалансовану оцінку, прийняту в урядових документах. У 2012–2013 рр. – на рівні 34–35%, у 2014–2015 – різкий стрибок до 40–42%, з подальшим коливанням довкола 35–38%, і знову зростання до 47% у 2022 році, що підкреслює реакцію тіньового сектору на військову агресію, мобілізацію, зміну структури зайнятості та розрив логістичних ланцюгів.

Таким чином ми отримуємо досить неочікувані структурні висновки. Так, тінізація має політико-економічну природу – на неї чинять вплив війна, політичні кризи, падіння довіри до інституцій, при тому методи оцінки обсягу тіньового сектору суттєво впливають на результати: від 16% до 52% – колосальний розрив, що ставить питання про якість статистичної бази. Нажаль 2022–2023 роки стали новим стрибком тінізації, хоч і не таким драматичним, як 2014–2015. Це може свідчити про адаптацію економіки до умов війни та зростання ролі цифрових технологій, які частково витісняють готівкові схеми.

Таблиця 8.4 – Динаміка частки тіньового сектору економіки України, % ВВП

Роки	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Оцінка за методикою Держкомстату	18,5%	19,0%	22,0%	23,5%	22,4%	21,0%	20,5%	20,0%	30,0%	31,0%	33,5%	32,0%	30,0%
Метод “витрати населення – роздрібний товарообіг”	43,0%	42,5%	46,0%	47,5%	45,0%	44,0%	42,0%	41,0%	50,0%	48,0%	52,0%	50,0%	48,0%
Електричний метод	37,0%	36,0%	38,0%	39,5%	37,0%	36,0%	35,0%	34,0%	40,0%	39,0%	42,0%	41,0%	39,0%
Монетарний метод	26,0%	25,5%	28,0%	30,0%	28,5%	27,0%	26,0%	25,0%	35,0%	33,0%	36,0%	34,0%	32,0%
Метод збитковості підприємств	32,0%	31,0%	33,0%	34,0%	33,5%	31,5%	30,0%	28,5%	38,0%	36,0%	39,0%	37,0%	35,0%
Метод сукупного попиту – сукупної пропозиції	36,0%	35,0%	38,0%	40,0%	38,5%	37,0%	36,0%	34,0%	42,0%	40,0%	44,0%	43,0%	41,0%
Оцінка проф. Ф. Шнайдера	44,0%	48,0%	52,8%	50,5%	46,2%	44,5%	43,0%	42,0%	50,5%	49,0%	52,5%	51,0%	48,5%
Інтегральний показник Мінекономіки	34,0%	35,0%	40,0%	42,0%	38,0%	35,0%	33,0%	32,0%	45,0%	43,0%	47,0%	45,0%	42,0%

При порівнянні рівня тіньової економіки України з відповідними даними Європейського співтовариства – отримуємо невтішні дані (рис. 8.3).

У п’ятірку галузей економіки, що мають найбільшу частку тіньової складової, увійшли добувна та переробна промисловості, транспорт і торгівля, операції з нерухомим майном.

Саме тіньовий сектор в нашій державі є ключовою перепоною на шляху економічного поступу, підвищення стандартів життя населення країни, посилення конкурентних переваг та входження до європейського співтовариства. Тіньова економіка є відбиттям корумпованості державних органів влади, криміналізації економічних процесів та незадовільної правової та податкової культури підприємців. Розв’язання цих проблем стало ще більш важким завданням після політичних зрушень останніх років.

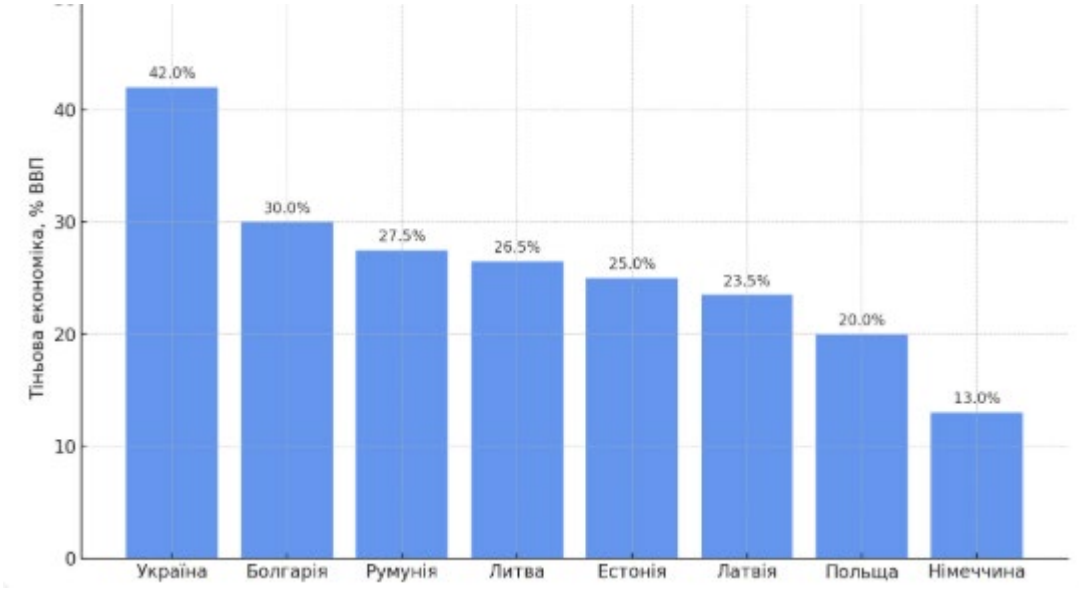

Рисунок 8.3 – Частка тіньової економіки в Україні та деяких інших європейських країнах станом на 2024 рік

Практично всі держави мають проблеми через тіньову економіку: подекуди її обсяги знаходяться в межах, що не загрожують стабільному функціонуванню держави, решта ж країн – це свідчення наявності відтворювальної системи тіньового сектору. Саме до другої категорії належить наша держава, оскільки обсяги тінізації за різними джерелами сягають рівня 20-50% від валового внутрішнього продукту.

Збільшення частки тіньового сектору негативно відбивається на дієвості інструментів та механізмів управління. Беззаперечними сучасними проблемами тінізації економіки у світовому вимірі є тіньові фінансові потоки та тіньова зайнятість.

За розрахунками, що базуються на інтегральних оцінках Мінекономіки та провідних аналітичних центрів, обсяг тіньової економіки в Україні у 2024 році перевищує 1,2 трлн гривень, або близько 30% офіційного ВВП. Структурно ця сума розподіляється таким чином:

- «зарплата в конвертах» – приблизно 500 млрд грн, що свідчить про стійку популярність схем неофіційної оплати праці в умовах зростання податкового навантаження та низького рівня довіри до пенсійної системи;

- переведення безготівкових коштів у готівку, «скрутки» та виведення коштів за кордон – орієнтовно 400 млрд грн, включаючи операції через псевдоекспортерів, інвойсингові схеми та криптовалютну анонімізацію;
- неофіційні платежі (хабарі, «відкати», чорна готівка в держсекторі) – близько 100 млрд грн, за оцінками антикорупційних ініціатив;
- матеріальні ресурси, тіньові послуги, обіг нерухомості без декларування – ще 200 млрд грн.

У сфері публічних фінансів рівень непрозорості залишається критично високим. За даними громадських аудиторських груп, до 60% державних закупівель на місцевому рівні у 2023–2024 роках здійснювались без повноцінних процедур Prozorro або з ознаками маніпуляцій. Збитки бюджету від корупційних практик у системі держзакупівель оцінюються на рівні 100–150 млрд грн щороку, або до 12% видаткової частини держбюджету.

Міжнародні експерти, зокрема аналітики Global Financial Integrity, оцінюють щорічне виведення капіталу з України через корупційні та тіньові схеми в межах 10–12 млрд дол. США. Суттєву частку таких втрат (до 70%) становлять маніпуляції з трансфертним ціноутворенням, насамперед при експорті металургії, зерна та IT-послуг.

На ринку праці тіньова зайнятість охоплює, за оцінками Міжнародної організації праці, близько 8–10% працездатного населення. Проте за методикою Інституту економіки та прогнозування НАН України, до 18% українців задіяні в тіньовому секторі повністю або частково. Конфедерація роботодавців України оцінює цю цифру у 5–6 млн осіб. Поширеною залишається гібридна модель оплати праці: «біла» частина – мінімальна, решта – готівкою «на руки».

За оцінками Федерації профспілок, загальний обсяг зарплат «у тіні» у 2024 році перевищує 600 млрд грн, а бюджетні втрати лише від несплати ЄСВ та ПДФО становлять понад 150 млрд грн щорічно.

Крім того, метод «витрати населення – роздрібний товарообіг» і надалі свідчить про високий рівень тінізації доходів домогосподарств, який у 2024 році оцінюється на рівні 40–43%. За таких умов, держбюджет щороку втрачає до 70 млрд грн ПДВ та понад 100 млрд грн соціальних внесків.

У 2024 році оцінювання економічної свободи України було тимчасово призупинено через повномасштабне вторгнення Росії, що триває з 24 лютого 2022 року. Останній доступний показник індексу економічної свободи для України становив 54,1 у 2022 році, що класифікується як "переважно невільна" економіка. Також за даними Transparency International, у 2024 році Україна отримала 35 балів зі 100 можливих у Індексі сприйняття корупції, посівши 105-е місце серед 180 країн, що на один бал менше порівняно з 2023 роком, коли Україна мала 36 балів. Таким чином попри деякі позитивні зрушення у сфері цифровізації та спрощення процедур ведення бізнесу, корупція та слабкі інституції залишаються ключовими перешкодами для економічного розвитку України. Відсутність оновлених даних щодо індексу економічної свободи ускладнює повну оцінку прогресу в цій сфері. Проте, зниження балів у Індексі сприйняття корупції свідчить про необхідність посилення антикорупційних заходів та реформування державних інституцій для забезпечення сталого економічного зростання та інтеграції до європейського простору.

У політичній сфері нашої держави значну роль відіграє боротьба з нелегальною економікою. Цей процес увиразнюється в період виборчих процесів різного рівня. Зокрема нещодавні парламентські вибори в Україні продемонстрували активність правоохоронців у порушенні кримінальних проваджень, де фігурантами були кандидати опозиційного блоку. З іншого боку опозиція ініціювала публічні депутатські запити з клопотанням про розслідування випадків корупції з боку вищого керівництва країни.

На жаль, розширення обсягів тіньового сектора не сприяє формуванню позитивного іміджу України в міжнародній спільноті, що суттєво гальмує залучення зовнішніх інвестицій. На думку міжнародних фахівців, одним з негативних чинників, який визначає інвестиційний клімат нашої держави, є високий рівень владної корупції. Це підтверджують дані опитування, за якими близько 80% респондентів головною причиною та перешкодою для розвитку іноземного бізнесу в державі є урядова корупція, яка разом з рівнем криміналізації економіки перешкоджають міжнародному співробітництву, встановленню тісних зв'язків на міжнародному рівні, що зрештою може спричинити поступову суттєву ізоляцію Україн.

Одним з найбільш значимих питань соціально-економічного поступу є рівень корупції. Окремі фахівці дійшли думки, що вона набула масштабів головної політичної вади сучасності. Беручи до уваги різні підходи до визначення сутності корупції, очевидним є те, що надзвичайно актуальне питання, яке потребує негайного вирішення на державному рівні. Це насамперед має відношення до нашої країни з очевидною для політиків, законодавців, міжнародної спільноти констатацією корумпованості.

Аналітики роблять наголос щодо варіативності ґенези категорії «корупція». Деякі науковці переконані, що вона є похідною від латинських «correі» (декілька суб'єктів, пов'язаних відносинами на базі зацікавленості в одному предметі) та «rumpere» (пошкоджувати, ламати щось, порушувати певний порядок, скасовувати). Таким чином, виник окремий термін «corrumpere», значення якого полягає в колективній участі в певній діяльності, спрямованої на перешкоджання звичному перебігу судового розгляду або управлінського процесу щодо суспільно значимих справ. Тотожне бачення даної категорії висловлює С.І. Ожегов, який вважає, що корупція полягає в організації підкупу, дачі хабара, в продажності високопосадовців і політиків.

Наукові школи, які вивчають питання, пов'язані з тіньовою економікою та її наслідком – корупцією, виділяють три її основні аспекти:

- соціальний та економічний, що полягає в перекрученні рішень держави в цій сфері корумпованим владним апаратом;
- політичний – інтегрування криміналітету в політичну систему задля задоволення власних інтересів;
- правовий – просування власних вигід, перешкоджання прийняттю оптимальних рішень, спонукання до таких дій, що уможливлюють необмежене лобіювання своїх інтересів, що лежать в кримінальній площині.

В умовах сьогодення корупція залишається однією з найбільших загроз національним економічним інтересам нашої країни. Зазвичай широке розуміння цього явища має на увазі антисоціальний процес, що проявляється на рівні формування нелегальних економічних стосунків між посадовцями різних ланок, які мають за мету, перш за все, просування власних

інтересів шляхом комерціалізації загальних суспільних благ. Звужене бачення корупції полягає у комерціалізації високо посадовцями, покладених на них владних повноважень.

Традиційно виокремлюють три найбільш поширених типи корупційних порушень, які з правової точки зору визначають як корупційні діяння або подібні порушення, зокрема кримінального характеру, адміністративні чи цивільно-правові. До них також можна віднести порушення ділової етики посадовцями у процесі учинення порушень.

Слід зазначити, що зазвичай корупційні діяння надані різними типами:

- зловживання наданими владними чи посадовими повноваженнями, перевищення допустимих меж використання влади чи вихід за межі своїх повноважень, інші злочини посадових осіб, які скоюються в корисливих цілях;
- протиправне отримання різнопланових благ, незаконних пільг або якихось інших преференцій;
- одержання пільгових кредитів, позик, матеріальної або іншої допомоги, купівля прав інтелектуальної власності, придбання рухомого й нерухомого майна на пільгових умовах, а також незаконних преференцій;
- хабарництво;
- отримання можливості для підприємницької діяльності через підставних осіб, використовуючи владні чи посадові можливості та повноваження;
- надання допомоги для злочинного використання можливостей посадовців безпосередньо суб'єктам підприємницької діяльності, що дозволяє в обхід чинного законодавства отримати переваги чи якісь блага;
- протизаконне використання владних повноважень для впливу на роботу державних інституцій чи окремих посадовців, яке заважає якісному виконанню покладених на них обов’язків, чи спрямування дій посадовців на прийняття не зовсім законних рішень;
- використання інформаційного масиву, здобутого в результаті професійної діяльності, з корисливою метою;
- безпідставне ненадання запитуваної інформації чи порушення строків її надання, а також оперування службовою фальсифікованою чи обмеженою інформацією;
- нормативно-правове закріплення шляхів для отримання безпідставних преференцій фізичними чи юридичними особами або їх обґрунтування на управлінському рівні;
- надання протекції з корисливою чи іншою подібною метою під час прийняття на роботу особи, яка не має переваг, виходячи з ділових якостей, порівняно з іншими претендентами.

Значна частина вчених, для яких корупція є предметом їх наукових інтересів, зазначають, що діяльність корумпованих посадовців негативно позначається на виході товаровиробника на ринок. В той же час варто пам’ятати, що діяльність даних чиновників не обмежується лише ліцензуванням, а й передбачає виконання ними низки інших суспільно важливих обов’язків. З огляду на це подолання явищ корупції шляхом призупинення втручання в процес регулювання економіки, ліквідація ліцензій чи звільнення потенційних посадовців-корупціонерів, відповідальних за виконання цих функцій, не вирішить проблеми, а лише створить нові труднощі. Також ліквідація ринкового регулювання на бюрократичних засадах у вигляді скасування ліцензування певною мірою матиме негативний сплив на загальний стан ринкових економічних відносин.

Слушною є думка О.М. Литвака щодо головних факторів, які продукують формування корупційних схем у площині тіньової економіки:

- недосконаліть нормативно-правового поля та належних організаційних умов для продуктивної роботи вітчизняного товаровиробника, зокрема в площині оподаткування, обов'язкових надходжень до бюджетів всіх рівнів, труднощі з наданням бюджетних кредитів тощо, що спонукає до пошуку протиправних шляхів для розв'язання зазначених проблем;
- співпраця криміналітету із суб'єктами господарювання;
- відсутність правового захисту товаровиробників від певних зловживань та наявність ефективної протидії потенційному хабарництву держслужбовців всіх рангів;
- недосконаліть законодавства в площині стабільності та збалансованості, що дозволило б регулювати підприємницьку сферу та підтримку товаровиробника;
- відсутність адекватної інвестиційної заміни «тіньовому» капіталу;
- нехтування історичним досвідом, морально-етичними засадами як підґрунтям для належного ставлення до інституту власності;
- суттєва соціальна диференціація населення країни за рівнем добробуту через корупційні прояви, коли статки державних службовців не йдуть у порівняння з середнім рівнем життя.

Масштаби сучасної корупції створюють суттєву загрозу для формування національної безпеки й загалом усього конституційного ладу країни. Ці прояви мають негативний вплив на всі сфери життя суспільства: соціально-економічну, політико-правову, управлінсько-організаційну, суспільно-громадську свідомість і міждержавні зв'язки. Корупція поступово підмінює правові та етичні відносини, із виключення переходить в розряд звичної моделі поведінки.

Впродовж останнього часу в нашій країні у площині боротьби з корупцією досягнуто чимало: набув чинності антикорупційний закон, створено низку інших нормативно-правових актів антикорупційного характеру, розроблено ефективну концепцію боротьби з корупцією, сформовано відповідну антикорупційну програму, політикумом задекларовано курс на боротьбу з цим негативним явищем, на найвищому рівні розроблено план організаційних заходів із залученням керівництва правоохоронних структур та інших державних інституцій, спрямованих на ефективну протидію корупційним проявам тощо.

Проте, усі ці та інші заходи, що впроваджуються в державі та у суспільстві, не мали суттєвих зрушень у боротьбі з корупцією. Це стало наслідком об'єктивних і суб'єктивних причин. Зокрема, впродовж періоду незалежності антикорупційні явища не осмислювалися науковою спільнотою в Україні. Тому сучасні підходи до проблеми подолання корупції базуються на трьох якісних характеристиках, вже наявність яких викликає протиріччя: насамперед, це очевидна актуальність для всього суспільного життя та для юридичної практики та науки зокрема; до того ж, вона є предметом постійної уваги з боку політиків, журналістів та інших громадян; зрештою, вона має недостатній рівень наукового осмислення.

Вивчення корупції в нашій державі набуває своєчасності як крізь призму дослідження продуктивності реформ у податковій сфері, так і в площині формування громадської думки в напрямі її відповідності сучасним економічним процесам. Деформована суспільна думка щодо антикорупційних зрушень може стати причиною їх недостатньої ефективності.

У зв'язку з непрозорістю, непрогнозованістю та складністю у втіленні реформ відповідного уявлення про корупцію вимагає держава та громадськість. Поглиблення корупційних проявів спричиняє втрату інституційного балансу, тобто призводить до виникнення економічної небезпеки. З огляду на це потрібно детінізувати економіку: цілеспрямовано долати прояви корупції шляхом реалізації низки відчутних економіко-правових та організаційно-адміністративних крокі.

Для підвищення ефективного протистояння тіньовому сектору та створення системи економічної безпеки в нашій державі доцільно:

- відділення владних інституцій та бізнесових структур;
- перевести у правове поле раніше приховані від сплати податків доходи підприємств, які здобуті некримінальним способом;
- надати відповідні умови для підприємництва, які зробили б недоцільною тіньову економічну сферу;
- боротися з нелегальною економікою за допомогою не тільки економічних важелів, але й адміністративно-директивними.

До головних чинників, що перешкоджають швидкому переходу економіки нашої держави в легальну площину, є:

- недосконаліть податкової системи, зокрема, коли фіскальна політика спрямована перш за все на збільшення надходжень до бюджетів всіх рівнів, без прогнозування ймовірних негативних впливів суттєвого тиску на товаровиробника та пересічних громадян.
- не сформованість належного ринкового простору, що спричиняє гальмування модифікації нормативно-правового поля, структурних і соціально-економічних перетворень, суттєві вади ринкового середовища, наслідком чого є незбалансованість сучасної соціально-економічної політики держави з урахуванням потреб підприємницьких структур, які мають власними силами формувати комунікативні механізми;
- посилення позицій корупційних структур і непрофесіоналізм працівників державних інституцій, для яких корумпованість стала основним пріоритетним напрямом розвитку держави та перешкодою для сприяння входженню до міжнародного співтовариства);
- постійна змінюваність правил гри в площині інвестицій і формуванні підприємницької діяльності (індикатором цього процесу є падіння індексу економічної свободи нашої держави у рейтингу американської громадської установи «The Heritage Foundation», де Україні відведено 152 місце із 179 держав станом на 2009 рік;
- незахищеність капітальних вкладників (за даними рейтингу «Doing business» наша держава з поміж 181 країни посіла такі позиції за такими параметрами індексу: за показником реєстрації власності – 140; за показником захищеності вкладників – 142; за показником прозорості процедури отримання дозвільних документів на будівництво – 179, за показником податкового тиску – 180 місце);
- постійно змінюване політичне поле тощо.

Попри певний поступ у сфері методології з питань вивчення нелегальної економіки як суттєвого сектора, на жаль не можна стверджувати про наявність чіткого визначення його

масштабності. Адже більшість підходів щодо оцінювання розмірів тіньових процесів та окреслення обсягів прибутковості від тіньової економічної діяльності характеризуються певною умовністю та суб'єктивністю. У протилежному випадку галузь, що є об'єктом економічного аналізу, зокрема в частині її обсягів, швидко б трансформувалась би із «тіньової» чи прихованої в легальну, а при окресленні розмірів кримінально-чорної економічної сфери переміщується в конспіративну площину.

Хоч визначити ширину охоплення тіньовою економікою вкрай важко, очевидним є той факт, що її сучасні масштаби в нашій країни дуже суттєві. У зв'язку з цим першочерговим завданням стає детінізація економічної сфери, яка є пріоритетним напрямом у звуженні обсягів тіньової економіки. У процесі боротьби з нелегальною економічною діяльністю доцільно опиратись на об'єктивну можливість і міжнародний досвід, який свідчить по неможливість повного подолання тіньового сектора економіки в існуючих політичних, соціально-економічних реаліях. Тактичним завданням може стати, перш за все, її звуження до обсягів, які наявні в промислово розвинених державах. Як наслідок, економічна політика на державному рівні повинна спиратись на оптимізацію системи владних структур в державі для того, щоб стало недоцільним працювати у тіньовій сфері економіки даної країни.

Головними чинниками, що уможливлюють формування тіньового сектора економіки є низка взаємопов'язаних елементів. Насамперед, це кризовий стан управлінської системи, неузгодженість розвитку продуктивних сил, високі ставки податків на всіх рівнях, непропорційний їх розподіл, значна розбіжність між олігархічно-владними колами та пересічними громадянами країни, несформованість середнього класу, що дозволив би певною мірою стабілізувати ситуацію в суспільстві, тотальний контроль у підприємницькій сфері, недосконалість нормативно-правової бази, завищений відсоток за користування кредитами, непродуктивне керування майном держави, низький рівень культури підприємницької діяльності, значна корумпованість, недосконалість належним чином обґрунтованої та продуктивної політики у напрямі детінізації вітчизняної економіки.

Загалом, з метою поступового звуження тіньової економічної діяльності в нашій країні варто зосередити увагу на таких ключових напрямах:

- зміцнення системи оподаткування та удосконалення роботи податкової служби за допомогою внесення відповідних змін у податкове законодавство України;
- забезпечення прозорості функціонування податкової системи та систематичний контроль операційної діяльності державних інституцій;
- розробка та забезпечення ефективної роботи правового механізму та мережі інституцій для протидії нелегальним схемам, зокрема відмиванню коштів, здобутих протизаконним способом, і сприяння поверненню капіталу, нелегально вивезеного за межі країни;
- зміцнення та широке використання дієвих методів державного управління, суттєве покращення роботи органів державної влади та всієї системи загалом.

Треба пам'ятати, в нашій державі тіньова економіка оперативно здатна адаптуватися до кризових умов і політики в сфері оподаткування, що власне і зумовлює реальне перевищення її окреслених обсягів. Процес суттєвого посилення тінізації економічної діяльності в 2008-2009 рр. був спричинений, перш за все, різкою реакцією на кризові явища у світовій економіці, а в подальшому – реакцією на запроваджену державою фіскальну політику.

Цілком логічно, що глобальна проблема детінізації економіки взаємопов'язана з головними труднощами у реалізації економічних реформ у нашій державі, формуванням соціально-орієнтованої моделі ринкової економіки. Досягти суттєвого звуження розмірів тіньового сегменту вітчизняної економіки нереально без якомога швидшого виконання реформи податкової сфери, покращення існуючої банківської системи, гарантованого правового захисту суб'єктів підприємницької діяльності. Нелегальний сектор економічної діяльності значною мірою впливає на перебіг всіх без винятку соціально-економічних процесів суспільного розвитку. Лише за належного урахування зазначених обставин можна здійснити науковий економічний аналіз на рівні держави та підприємства, прийняти продуктивні управлінські рішення. Неналежна увага до такого різноаспектного та дискусійного процесу, як тіньова сфера економіки, зумовлює виникнення суттєвих вад при формуванні показників макроекономічної діяльності, неадекватне оцінювання найбільш значимих тенденцій, прорахунки в оперативному та стратегічному плануванні. Дана сфера економічної діяльності суттєво і всебічно впливає на економіку та суспільно-політичне життя.

Варто констатувати, що досягти помітних змін у корупційно-тіньовій сфері реалізацією системи законодавчих чи певною мірою репресивних кроків неможливо через відсутність відповідних суб'єктів, на яких було б покладено ці завдання. Водночас, не слід не враховувати ймовірність таких перетворень під зовнішнім впливом, безпосередньо при узгодженні нормативно-законодавчих і розпорядчих документів стосовно боротьби з узаконенням тіньових доходів.

Тому суттєве зменшення обсягів тінізації економічної діяльності є обов'язковою ланкою стратегічного реформування. Беручи до уваги ймовірність виникнення потенційних ризиків при реалізації окресленої мети реформ, першочерговими заходами виведенню економіки з тіні є боротьба з нелегальними фінансовими потоками, приведення у нормативне поле ринку праці та узаконення земельних відносин. Створення державними інституціями таких умов, коли існування тіньового сектора стає досить ризиковим і надмірно високовартісним, сприятиме формуванню стимулів для легального використання капіталів, виведення з тіні земельного ринку та ринку праці. Легалізація фінансових надходжень, соціально-трудових відносин і земельного ринку створюють умови для всебічного використання можливостей прогресивних реформ і забезпечує стабільність економіки нашої держави та знижує негативний вплив кризи.

У 2024 році боротьба з корупцією та тіньовою економікою залишається одним із ключових стратегічних пріоритетів державної політики України, що зумовлено як внутрішнім суспільним запитом, так і зобов'язаннями в межах євроінтеграції та співпраці з міжнародними партнерами (ЄС, МВФ, Світовим банком).

Протягом останнього десятиліття відбувся перехід від декларативно-розпорядчого до системного інституційного підходу у сфері протидії корупції. Низка застарілих указів і концепцій 1990–2000-х років втратила чинність. Натомість Україна сформувала цілісну архітектуру антикорупційних органів і нормативно-правових інструментів, серед яких:

- Закон України «Про запобігання корупції» (№ 1700-VII від 14.10.2014, чинний станом на 2024 рік із численними змінами), який визначає правові та організаційні засади формування та реалізації антикорупційної політики в Україні;

- Національне агентство з питань запобігання корупції (НАЗК) — відповідальний орган за перевірку декларацій, моніторинг способу життя посадовців, контроль фінансування партій тощо;
- Національне антикорупційне бюро України (НАБУ) — орган досудового розслідування злочинів, пов'язаних з корупцією вищого рівня;
- Вищий антикорупційний суд (ВАКС), який з 2019 року здійснює розгляд справ високопосадової корупції;
- Закон України «Про засади державної антикорупційної політики на 2021–2025 роки» (Антикорупційна стратегія), ухвалений 20 червня 2022 року.
- У 2023–2024 роках реалізується Державна антикорупційна програма на 2023–2025 роки (затверджена постановою КМУ № 149 від 4 березня 2023 року). Ця програма охоплює 800+ конкретних заходів у 12 пріоритетних сферах: оборона, держзакупівлі, будівництво, митниця, податки, екологія тощо.

Суттєвою новацією стало впровадження системи електронного декларування з автоматичними ризик-модулями (оновлене в 2024 році після ухвалення Закону № 3385-IX), а також відкриття реєстрів публічних бенефіціарів і державної власності.

На рівні міжнародного співробітництва Україна:

- у 2023 році приєдналась до Групи держав проти корупції (GRECO) як учасник п'ятого раунду оцінювання;
- продовжує реалізовувати Угоду про спільну антикорупційну оцінку з Європейською Комісією в рамках Плану дій щодо членства в ЄС;
- співпрацює з OECD Anti-Corruption Network, отримуючи технічну підтримку та аналітичні рекомендації.

У підсумку, у 2024 році Україна поступово переходить від фрагментарної боротьби з корупцією до системної, однак ефективність реалізації політик залишається критично залежною від незалежності судової системи, політичної волі та реального притягнення до відповідальності осіб, залучених до високопосадової корупції.

Безумовно, головною складовою використання зовнішніх і внутрішніх конкурентних переваг макроекономічної української економіки є узгодження нормативно-законодавчої бази та затвердження основоположного принципу верховенства права, продуктивна діяльність правоохоронних органів, забезпечення виконання рішень судів. Розбудова вітчизняної правової системи за сучасними європейськими нормами виконує роль вельми вагомого первинного чинника поштовху до системних перетворень в нашій країні, а досвід здійснення прогресивних реформ у сучасній Грузії це констатує. На часі формування в Україні нової системи захисту інтересів всіх верств населення, яка базується на передових європейських засадах державного управління.

Надмірно високий рівень прояву тінізації соціально-економічного розвитку, утворення розбіжностей між намаганнями здійснення системних реформ на державному рівні та проявами негативного ставлення певних верств населення до розширення втручання управлінсько-адміністративних структур в повсякденне життя громадян вимагають ґрунтовного ємного дослідження тенденцій формування певних структурних механізмів, які в свою чергу зумовлюють виникнення такого негативного явища, як тіньова економіка.

Станом на 2024 рік обсяг тіньової економіки в Україні досягає критичного рівня, що становить пряму загрозу сталому розвитку промислового сектору, зокрема таких стратегічно важливих галузей, як металургія. Збереження масштабних тіньових потоків капіталу перешкоджає інвестиційному зростанню, скорочує податкові надходження та підриває довіру до інституцій.

Для виведення капіталу з тіні першочерговим завданням державної політики має бути зменшення фіскального тиску на підприємства, включаючи перегляд рівня податкового навантаження та зниження облікової ставки НБУ, що наразі залишається однією з найвищих у Європі. Важливим є також забезпечення прозорості механізмів державної підтримки, зокрема процедур повернення ПДВ, які часто супроводжуються корупційними ризиками.

Окрему увагу слід приділити усуненню загроз рейдерських захоплень та припиненню зрощування політичного і бізнесового капіталу, що призводить до формування тіньових альянсів і паралельних управлінських структур.

З огляду на те, що окремі галузі мають високу ступінь монополізації, держава повинна вживати заходів для стримування антиконкурентної поведінки на внутрішньому ринку та стимулювання рівних умов доступу до інфраструктури, сировини і фінансування.

У цьому контексті пропонуються наступні стратегічні рекомендації:

1. Модернізація системи обліку та моніторингу економіки — з акцентом на використанні індексів мобільних транзакцій, цифрових платформ, електронних платіжних систем і обліку електроенергії як індикаторів реальної господарської активності.
2. Підвищення довіри до інститутів та податкової політики — шляхом забезпечення передбачуваності фіскального регулювання, цифрової прозорості та мінімізації ручного втручання в процеси адміністрування.
3. Підтримка мікро- і малого бізнесу через перехід від репресивного до сервісного формату державного нагляду, зменшення адміністративного тиску та розширення доступу до фінансування, що в сукупності зменшить мотивацію до ухилення від офіційної діяльності.

Комплексна реалізація вищезазначених заходів створить передумови для реального зменшення масштабів тіньової економіки, відновлення довіри інвесторів і забезпечення стійкого розвитку промисловості в умовах сучасних викликів.

8.4 Функціональний зміст та особливості сучасного рейдерства як фактора впливу на захищеність бізнесу

Прихована площина тіньової економічної діяльності виявляється у вигляді рейдерства – поглинання суб’єкта господарювання всупереч згоди їх менеджерів або власників, що має суттєвий вплив на товаровиробника, спричиняє деструктивні зміни в трудових колективах, знижує інвестиційну привабливість країни в цілому.

В перекладі з англійської термін «the raid» розуміють як захоплення. У довідковій літературі економічна сутність поняття «рейдер» подається так: певна фізична чи юридична

особа, яка право на власність промисловим підприємством отримує в обхід волевиявлення її акціонерів, адміністрації, співробітників і застосовує для цього механізм придбання на відкритих аукціонах, активно формує власний контрольний пакет акцій.

Як правило, всі договори щодо поглинання, злиття та корпоративної агресії у формі недружнього поглинання чи безпосередньо рейдерського захоплення компанії дають можливість фактичного володіння суб'єктом господарювання. Так звані дружні злиття ймовірні в умовах, коли існуючий корпоративний контроль над суб'єктом господарювання здійснює поглинач з власної волі, виходячи з домовленості з органами управління та акціонерами, які здійснюють контроль. Водночас, кожне недружнє поглинання являє собою різновид невдалого дружнього договору про злиття або безпосереднє поглинання. За традиціями, які сформувалися у вітчизняному підприємництві, переважна більшість власників роблять пропозицію щодо продажу бізнесу (тут ціна не має ключового значення, важливою є сама пропозиція), а згодом, у разі незгоди, ініціюються радикальні дії, що призводять до зміни безпосереднього власника промислового підприємства.

У практиці суб'єктів господарювання зарубіжних країн правове поле недружнього поглинання визначається процесом купівлі акцій підприємства на ринку, яке відбувається поза бажанням неефективної управлінської ланки та відсутністю належного контролю з боку акціонерів-власників великих пакетів акцій. Широке тлумачення поглинання розглядається як процес, який забезпечує добровільну передачу активів суб'єкта господарювання новому власнику, а не силовими методами. Поглинання відбувається у випадку, коли власник одного підприємства поширює свій контроль на інше. Український контекст недружніх поглинань зазвичай реалізується у формі отримання можливості контролювати суб'єкт господарювання за допомогою застосування протиправних дій та засобів, що, як правило, відбувається в умовах привласнення акцій підприємства проти волі їх фактичних власників.

Життєві цикли й поглинання постійно є невід'ємною складовою розвитку як міжнародного економічного простору, так і вітчизняного, проявом якого є наявність щорічного зростання кількості укладених договорів різного рівня у ринковому середовищі, зокрема угод про об'єднання та поглинання.

Формування процесів злиття та поглинання в умовах сьогодення є свідченням пошуку вітчизняними товаровиробниками можливості збільшення масштабів їх виробничої діяльності, покращення продуктивності ведення бізнесу, посідання свого місця на міжнародних ринках, а окрім того збереження позицій зайнятих у ринковому середовищі з жорсткою конкурентною боротьбою, динамічним зовнішнім простором та адаптування до проявів кризових явищ і глобальних тенденцій економічного розвитку.

За світовими статистичними даними, менша частина підписаних договорів щодо об'єднання та поглинання виявляються перспективними, що спричинено низкою умов, зокрема: невизначеність на перспективу (хибний вибір стратегії на етапі до та після злиття), неправильний підхід до вибору найбільш важливого партнера, недостовірні обчислення ймовірного прибутку, термінів обігу активів, розбіжності у формуванні корпоративних відносин, гальмування інтеграції, неналежне оцінювання критичного стану, відсутність чіткості та прозорості у розподілі отриманих доходів тощо. Проте найвагомішим індикатором успішності укладених договорів є окреслення мети та мотивації здійснення процесів об'єднання чи поглинання, тому що відсутність бачення того, що доцільно

отримати в результаті даного процесу, суб'єкт господарювання певною мірою ризикує втратити продуктивність у подальшому.

На думку вченого Полушкіна О.А. про те, що такі явища, як «недружнє поглинання», «протизаконне отримання можливості контролю над суб'єктом господарювання», «корпоративний шантаж» це не просто синоніми рейдерства, а спроби нелегального переділу майна власників тощо. Купівля акцій, доведення до банкрутства, повторна приватизація, захоплення силовими методами, фальсифікація документів і шахрайство – це все є проявами рейдерства. В той же час категорія «рейдерство» та термін «недружнє поглинання» недоцільно ототожнювати.

У вітчизняній економіко-правовій терміносистемі поняття «рейдерство» досі чітко не окреслене, тому переважно сприймається як синонім до «недружнього поглинання». Українські науковці тлумачать категорію «рейдерські атаки» як логічні, взаємопов'язані кроки окремих угруповань злочинного характеру, спрямовані на незаконне отримання доступу до керування або інших дій з розпорядженням власністю суб'єкта господарювання за допомогою провокування бізнес суперечностей, зазвичай із залученням силових відомств. Іншими словами, рейдерство – це свого роду недружнє поглинання поза межами цивільних правовідносин, покликане всупереч бажанню власника заволодіння чужими активами в інтересах третьої особи, забезпечення тотального контролю над захопленим майном (в нормативно-правовому чи фізичному плані) з боку нового власника, опираючись на корумпованості посадовців або на використання силових методів. Українські спеціалісти з питань безпеки бізнесу наголошують, що поняття «рейдер», а також «недружнє (вороже) поглинання» є певною мірою близькими, а відмінності лежать лише в процесній площині, адже «рейдерство» – це певний процес, а поглинання є наслідком чи результатом.

Сутність рейдерства полягає у чіткій спрямованості. У ролі учасників цього процесу, на яких покладені функції плануванням комплексу дій, у вітчизняних реаліях можуть виступати самі власники або третя сторона. Здійснювати рейдерське захоплення рейдер може як самотужки, так і із залученням рейдерських компаній.

У міжнародній практиці рейдерство сприймають як показник недоліків у політико-правових державних структурах владних інституцій, прогалин у чинному правовому полі, не створенні сприятливого мікроклімату з метою належного захисту бізнесових інтересів, майнових та інших прав власників і рівноправних конкурентних позицій. Той факт, що в нашій країні існує рейдерство, свідчить про наявність суттєвих системних проблем у економіці України.

Термін «рейдерство» з'явився в Англії на позначення нападів і захоплень морськими суднами, які самотужки брали участь у виконанні бойових завдань, кораблів торгівельного флоту інших держав.

Спочатку рейдерство з'явилось як форма протиправного захоплення, пограбування та привласнення морських кораблів. Згодом, у XX ст. стали застосовувати як привласнення контрольного пакета цінних паперів суб'єкта господарювання або як фальсифікацію документації чи застосування фізичної сили для захоплення. Надалі, коли більш частими стали дружні поглинання або об'єднання декількох підприємств для подальшого ефективного співробітництва в інтересах обох сторін. Наслідком цього стало те, що кожний співвласник не тільки не втратив управління своїм підприємством, а ще й здобув відчутні

преференції в поєднанні виробничого потенціалу, врахуванні передового досвіду, залученні додаткових капіталовкладень і розширенні збутових ринків.

Рейдерство має тривалу, кілька століть, історію, хоч сама категорія почала використовуватися в ділових колах на рубежі XIX–XX ст. Статус злочину воно набуло одночасно з появою акцій, що створило умови для захоплення промислового підприємства всупереч волі її законного власника. Найбільш відомим прикладом з історії рейдерства вважається намагання захопити французьку Ост-Індійську монопольну компанію на той час добре відомим шахраєм Жаном де Батцом. У період Великої Французької революції саме він спонукав до висвітлення у доповіді проблеми доцільності знищення компанії. Такий крок мав на переконання авторів спричинити ажіотаж з метою швидкого продажу акцій компанії з одногу боку, та їх купівлі за безцінь з іншого.

З погляду англосаксонського розуміння «вороже поглинання» – це звичайне скуповування акцій компанії на ринку, яке відбувається всупереч волі власників, тобто – це процес наслідком якого є перехід активів підприємства у власність іншого покупця.

Хронологія ворожих поглинань компаній США ведеться з часів відомого підприємця Джона Дейвісона Рокфеллера, який розпочав свою кар'єру в період громадянської війни 1861–1865 рр., що суттєво вплинула на формування сучасної Америки. Стартовий капітал Дж. Рокфеллер сформував, виконуючи замовлення військових і реалізуючи нафту для задоволення потреб американської армії. Пізніше, у 1867 р., разом з Генрі Флеглером вони заснували корпорацію, яка отримала назву Standart Oil Company, зі статутним капіталом в 1 мільйон доларів, яка згодом виконала роль першої рейдерської компанії в світі. Дж. Рокфеллер спрямував свою діяльність не на складний пошук і видобуток нафти, а на її перероблення та постачання нафтопродуктів, отримавши на це у 1877 р. монопольне право. Задля протизаконного отримання контрольних функцій над транспортуванням нафти територією США підприємець, опираючись на підставних осіб, заволодів контрольними пакетами акцій американських залізничних компаній, що дало змогу їх захопити та створити нову структуру - Union Tanker Car Company. Впродовж тривалого періоду майже ніхто в США не міг припустити, що саме Дж. Рокфеллер володіє даною корпорацією, що дало змогу Standart Oil Company максимально знизити витрати на транспортування. Таким чином, використовуючи рейдерський підхід, була заснована могутня нафтова імперія.

Історичний досвід недружніх поглинань в Англії має початок з 1950-х. Внаслідок післявоєнних інфляційних процесів нерухомість швидко зростала в ціні, тоді як Законом про компанію 1948 року посилилася відповідальність за якість фінансової звітності всіх акціонерних товариств. Завдяки цьому інвестори, зокрема Чарльз Клор, отримали можливість для успішної реалізації намірів першого недружнього захоплення в 1953 році, коли усвідомили, що окремі компанії суттєво недооцінювали наявні торгові площі, заносячи до бухгалтерського обліку вартість, що в рази відрізнялася від ринкової. З'ясувалося, що цей факт ще не встиг вплинути на формування ціни акцій, оскільки вкладники англійських акціонерних товариствах вже встигли звикнути до оцінювання вартості акцій на основі вкрай звуженої фінансової інформації. Ці власники розцінювали систематичні дивіденди як свого роду свідчення дотримання зобов'язань по відношенню до інвесторів. Як наслідок – прибутки за дивідендами вважалися головним детермінантом вартості акцій. Відразу після Другої світової війни в Англії було запроваджено обмеження нарахування дивідендів на цінні папери суб'єктів господарювання з метою стимулювання реінвестування у власні

компанії. Обраний шлях формування вартості цінних паперів спричинив зниження котирування акцій. Сукупність зазначених обставин забезпечила оптимальні умови для придбання акцій, адже курси цих цінних паперів, які базувалися на обмежених нарахуваннях дивідендів, знизилися значно нижче за реальну ринкову вартість нерухомості цільових компаній.

В Англії порівняно з США передумови для захоплення (ворожого чи дружнього) зовсім не пов'язані з фінансовим становищем суб'єкта господарювання та ефективністю менеджменту. Зазвичай посилений інтерес англійських рейдерів викликали не лише фінансово стабільні, але й збіднілі компанії. В тож же час для англійської економіки не притаманне залучення до недружніх захоплень спеціалізованих фірм, які працюють над перерозподілом наявних активів попри зацікавленість і всупереч правам інших суб'єктів господарювання.

Узагальнення досвіду масових захоплень суб'єктів господарювання в Англії впродовж останніх десятиліть дозволяє констатувати, що специфіка здійснення рейдерських поглинань фірм (обсяг акцій, способи їх продажу) значною мірою зумовлюється політико-правовими та інституційними умовами в країні. Варто зауважити, що існування дуже розгалуженої структури власності певною мірою сприяє зростанню числа недружніх поглинань у державі. Привертає увагу те, що в англійській економіці домінують дружні поглинання суб'єктів господарювання, через те, що ворожі захоплення не схвалюються бізнесовими колами та суспільною думкою. Це, насамперед, визначається тим, що для країн Європи, зокрема Великобританії, до кожного суб'єкта господарювання відносяться не лише як до виняткової власності акціонерів, а також як до самостійного соціально-економічного утворення, відповідальність за відповідне визнання якого лежить безпосередньо на співробітниках фірми, постачальниках, державних інституціях і всього суспільства.

У Німеччині відсутній активний простір для недружніх захоплень, тому можна констатували лише одиничні випадки за всю історію. В числі перших об'єктів уваги рейдерів була німецька компанія Continental AG у 1990 році, коли Italian Pirelli Group разом з низкою італійських союзників придбали акції в обсязі меншому за 50 відсотків наявного акціонерного капіталу, але достатньому для простої переваги на зборах власників. Pirelli з компаньйонами врешті-решт зазнали поразки в їх намаганні зняти обмеження у прийнятті рішень на п'ять відсотків Continental AG. Правова колізія визначалася тим, що акційний пакет союзників належав Pirelli на таких засадах, що можливість участі в колективному було знижено до п'яти відсотків усіх наявних акцій, що були в обігу. Економічне підґрунтя визначалося тим, що Pirelli не отримував суттєвої підтримки Deutsche Bank та інших німецьких інвесторів, які лобіювали інтереси Continental AG в його прагненні залишитися автономними. В результаті тендерної пропозиції жоден з акціонерів так і не отримав.

Найбільш значне об'єднання сталеливарної промисловості Німеччини веде початок з 1992, коли Fried Krupp AG розпочала поглинання Hoesch AG. Намір купити 30-відстоткової частини в Hoesch було озвучено в ультимативній формі головою Krupp. До оприлюднення пропозиції, керівництво Hoesch припинило спротив, тому обидві корпорації почали діяльність з проведення законного об'єднання.

Fried Krupp AG Hoesch Krupp зазначала прицільного удару повторно в 1997р. В цей час було поширено інформації щодо того, що Krupp, яка перебувала під захистом власника контрольного пакета акцій Krupp Foundation, має намір поглинути значно більшу

конкуруючу корпорацію Thyssen AG. Лише після низки перемовин на високому рівні, в яких брали участь працівники Північної Рейн-Вестфалії, намагання щодо захоплення були припинені, а обидва суб'єкти господарювання розпочали ґрунтовне вивчення спільних перспектив. В результаті цього у 1998 р. відбулося об'єднання сталеплавильних компаній, а повне об'єднання зазначених холдингів було завершене у 1999 році.

Загалом для німецького корпоративного ринку притаманне використання дружніх форм злиття суб'єктів господарювання, а розбіжності, що є наслідком насамперед ворожих поглинань, трапляються дуже рідко. Безконфліктність функціонування системи корпоративного контролю у ФРН є результатом високого рівня концентрації власності, порівняно незначною частиною акцій, які наявні у вільному обігу, дієвістю продуктивних механізмів належного захисту від можливих ворожих захоплень.

Поштовхом до зростання попиту на використання рейдерських послуг став перехідний період у вітчизняній економіці до ринкової моделі та процес активного широкомасштабного поділу наявної власності. Впродовж останнього часу популярність таких послуг набуває рис усвідомленості, організованості та масовості, що можна пояснити кількома чинниками:

- недостатньою розробленістю чинного нормативно-правового поля, заангажованістю різних гілок влади : виконавчої та судової;
- розбалансованістю політичної системи та переділом сфер впливу різних фінансових і промислових структур;
- запозиченням рейдерських механізмів і капіталів із-за кордону, перш за все з Росії, які не користуються попитом у себе через оптимізацію чинного правового поля.

Варто зауважити, що з аналогічним феноменом мали справу практично всі держави з перехідною економікою. Зокрема, у найближчого сусіда України – Польщі на початку 90-х рр. XX століття рейдерство називалось «торпедуванням». Вітчизняний тип рейдерства подібний до російського за певними ознаками структурою, використовуваними методами та впливом на економічну ситуацію в країні.

Слід зазначити, що в Росії впродовж 1988-1991 рр. приватизація фінансової сфери мала характер практично міжкланової, що суттєвим чином вплинуло на подальший перерозподіл різного типу власності та наділило владними повноваженнями фінансові олігархічні кола. Протягом 1992-1995 рр. була поширена приватизація на основі ваучерів. Процес масової трансформації промислових підприємств за допомогою акціонування та у вигляді публічних товариств відбувався в умовах несформованості ринку цінних паперів. Мало місце привласнення керівною ланкою виставлених на приватизацію суб'єктів господарювання державної форми власності. Яскравим проявом рейдерства були спроби злочинних угрупувань отримати контроль над промисловим сектором держави. У період з 1993-1995 рр. у Російській Федерації точилася жорстка конкурентна боротьба за володіння фінансовими потоками суб'єктів господарювання (силове захоплення підприємств, «приватизація» управлінських функцій, злочинний рекет). Фактично на 2003 р. повністю сформувалося сучасне рейдерство Росії у формі прибуткового бізнесу фізичних та юридичних осіб, діяльність яких спрямована суто на привласнення суб'єктів господарювання з метою майбутнього перепродажу. За порівняно короткий термін їм вдалося нагромадити певний капітал, завдяки використанню адмінресурсів і низки інших складових атрибутів власного бізнесу.

В Україні термін рейдерства почав використовуватися наприкінці XX століття. Наслідком приватизації за ваучерами сформувалась ціла мережа різноманітних акціонерних товариств, акціонери яких не мали жодного уявлення про механізми та специфіку корпоративного менеджменту. Управлінці вищої ланки акціонерних товариств робили акцент на можливості використовувати повною мірою адмінресурс, штучний монополізм та інші фактори, невластиві ринковому середовищу, адже вони й впливали на рентабельність бізнесу. У таких умовах важелі продуктивного використання акціонерного капіталу не дали бажаного результату. До того ж, зважаючи на трудомісткість та потребу у значних капіталовкладеннях для узгодження дій (як правило, це підготовка та проведення низки зборів співвласників; узгоджувальні процедури в державних інституціях; витрати значних коштів) традиційні для багатьох держав підходи до об'єднання та привласнення суб'єктів господарювання не знайшли широкого застосування в нашій країні. З огляду на це, вітчизняні рейдери замість опанування легальними способами привласнення віддають перевагу протизаконним формам захоплення, так як це дозволяє оперативно привласнити майно.

Вітчизняне рейдерство у своєму розвитку пройшло два основних етапи. Перший припадає на кінець XX століття (суб'єкти господарювання відкрито привласнювались за допомогою кримінальних схем з доволі поширеним застосуванням фізичних методів.

Початок другого етапу, який припадає на 2000-й рік і продовжується й зараз, відзначається застосуванням напівлегальних способів привласнення суб'єктів господарювання, дещо більш законними формами конкуренції та певним спротивом рейдерським атакам.

У нашій державі наразі має місце сучасний підприємницький ризик, який полягає у можливості протизаконного перерозподілу активів. Певною мірою він тотожний ризику банкрутства, тобто правовому ризику чи ризику загострення економічної кризи. За статистичними даними за 2005-2008 рр. за масштабами рейдерських поглинань вітчизняними правоохоронцями розпочато понад 750 кримінальних проваджень, в той же час до державного реєстру внесено більше 830 заяв з приводу спроби протиправного перерозподілу майна.

Не вникає жодних сумнівів, що ризиком рейдерства доцільно певною мірою управляти. Найпростіша форма ризик – менеджменту може мати кілька фаз: діагностика ризику, визначення шляхів і важелів управління, відстеження показників та оцінювання динаміки у вартості підприємства після реалізації заходів зі зниження чинників ймовірного ризику.

В нашій країни рейдерство як явище набуло значного поширення у зв'язку з тим, що з початку третього тисячоліття до наявних схем про законного захоплення приєдналися державні та правоохоронні структури, судова гілка влади та виконавча служба. Згідно з висновками експертів провідних інвестиційних організацій, річні показники захоплення та привласнення оцінюються біля 3 млрд. доларів, в той же час слід зазначити, що майже 70% зазначених поглинань є ворожими та мають ознаки рейдерства.

За словами президент УСПП Анатолія Кінаха, масштаби рейдерських захоплень стали загрозою для ефективного економічного розвитку та для всієї державної безпеки. На його думку, майже 17% звернень суб'єктів підприємницької діяльності до УСПП торкаються насамперед питань рейдерських поглинань.

Беззаперечним лідером ділових і наукових диспутів стало обговорення проблеми рейдерства, а саме - ворожого поглинання (у вітчизняних реаліях – протизаконне привласнення). Цей процес характеризується масовістю. Згідно з даними національного союзу промисловців і підприємців, рейдерські захоплення торкнулися понад двох тисяч суб'єктів господарювання. Певною сенсацією загальнодержавного значення стало рейдерське захоплення відомих промислових підприємств: Дніпропетровський олійноекстраційний завод, Київська фабрика технічного паперу, «Дніпрофарм», «Київськнафтопродукт» тощо.

Слід зазначити, що про масштаби рейдерства в нашій державі говорить те, що його об'єктами стають великі корпорації, де головним співвласником є держава. Впродовж останнього часу з проблемою рейдерства зустрілися зокрема Херсонський морський порт, ПАТ «НВП «Сатурн» тощо.

Зважаючи на значимість наслідків впливу загроз для промислових підприємств, найнебезпечнішими є рейдерські поглинання, тобто протизаконна діяльність окремих кримінальних угруповань.

Мінімізація зазначених ризиків можлива завдяки застосуванню правових важелів, використання новітніх методик, залучення до інформаційних суспільних процесів. Це є досить нагальним, виходячи з активізації міжнародної співпраці в умовах глобалізації.

На рис. 8.4 зображена класифікація рейдерських схем згідно з її видами.

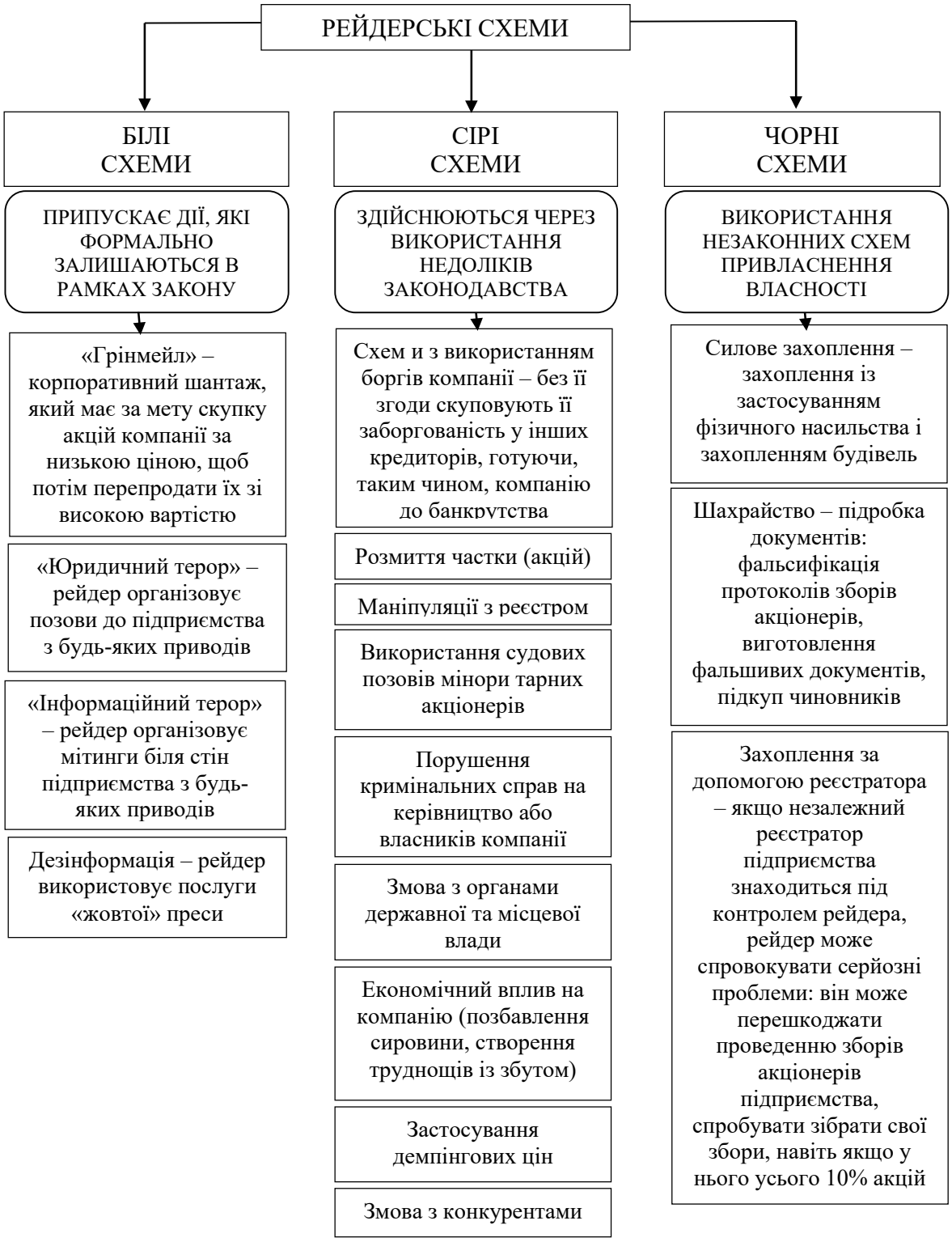

Рисунок 8.4 – Класифікація рейдерських схем

Напрями подолання рейдерських атак у різних державах світового простору базуються на загальних і конкретних допустимих межах операцій з цінними паперами, розробці та запровадженні правил корпоративного менеджменту, законотворчій діяльності, яка визначає процеси поглинання та злиття.

Найприйнятнішими формами боротьби з рейдерством є:

- зосередження капіталу акціонерів або придбання акцій у власників, що усунулися від управління суб'єктом господарювання; постійне відстеження змін власників акціонерного капіталу; реорганізаційні процеси в організаційній структурі; додаткова емісія та придбання контрольного пакета;
- окреслення правового поля власності, здійснення переоцінювання власного на ймовірність ризику, доречно здійснити оптимальну структуризацію
- власності з застосування дочірніх підрозділів, штучне формування заборгованості суб'єкта господарювання та передача активів під заставу;
- унеможливлення виникнення та несвоєчасного погашення заборгованості кредиторам;
- покращення управлінської діяльності (уникнення конфліктів, незаконного звільнення співробітників тощо);
- покращення загального рівня культури промислових підприємств (формування ділового іміджу, добросовісна конкуренція тощо);
- застосування службою економічної безпеки методів дозволеної конкурентної розвідки;
- співпраця з широким загалом і ЗМІ з питання протистояння рейдерству;
- підвищення якості управління;
- політична стабільність;
- прийняття законів щодо регулювання корпоративних правовідносин;
- прозорість приватизаційних процесів.

До головних документів, що визначає площину корпоративного контролю та регулює механізм стосовно поглинання суб'єктів господарювання в Сполучених Штатах Америки, належить Закон Вільямса. Згідно з цим документом, всі, хто має намір брати участь у підприємницькій діяльності, повинні своєчасно ставити до відома щодо власних намірів. Комісія з цінних паперів, надалі зобов'язана дотримуватися визначених строків, впродовж яких кандидатам не дозволяється чинити дії, які б забезпечували участь товаровиробника у бізнесі певного підприємства. На наш погляд, введення окреслених обмежень створює умови для зважання усіх аргументів на користь можливого введення до складу власників нових акціонерів та унеможливлення протиправного заволодіння управлінськими повноваженнями суб'єкта господарювання сторонніми особами.

Узагальнюючи досвід роботи американських суб'єктів господарювання можна наголосити, щодо найпродуктивніших механізмів запобігання ворожим захопленням у США належить своєчасна ротація керівної ланки, коригування статутів товаровиробника за умови пожвавлення «чорного» рейдерства в ринковому середовищі корпоративного контролю.

До найбільш яскравих ознак заборонних нормативно-правових актів з питань об'єднання чи поглинання відносять адресність наявних нелегальних угод. Насамперед, це

відноситься до великих компаній та монополій. Підтвердженням цьому є досвід Німеччини, де починаючи з 1960 р. застосовується «Закон Volkswagen», згідно з яким існує заборона на привласнення автоконцерну.

Крім жорстких обмежень чи заборон щодо можливого об'єднання або захоплення, державні інституції вдаються до іншого способу – відносне регламентування. Сутність відносності полягає в тому, що передусім на державному рівні визначається якась норма наявних активів промислового підприємства, яку дозволено купувати іншим власникам. Формування норми здійснюється на основі врахування різних аспектів: бути меншою за контрольний пакет цінних паперів того чи іншого суб'єкта господарювання; з метою унеможливлення заволодіння контрольним пакетом акцій підприємств, що поглинаються, на державному рівні надається допомога у додатковій емісії акцій. Розглянутий підхід, який поширений у різних країнах, іноді називають «гіркими пігулками» («poison pill»), що проявляються у різних формах. Так Міністерство економіки, торгівлі, промисловості Японії у 2004 році сформувало робочу групу, на яку було покладено завдання визначення прийнятної форми таких «гірких пігулок», яка б не суперечила чинному законодавству.

До визначення загальноприйнятих підходів щодо захисту суб'єктів господарювання від рейдерського захоплення залучені не лише урядові кола багатьох держав, а й низка приватних і громадських об'єднань. В той же час, якщо сфера інтересів державних інституцій поширюється перш за все на оптимізацію корпоративного нормативно-правового поля для констатації обов'язковості дотримання чинних нормативів у сфері конкуренції, оприлюднення даних про промислове підприємство, реалізації прав власників цінних паперів і забезпечення їх рівності, то сфера інтересів ділових кіл, а також приватних утворень полягає у встановленні вимог і механізмів корпоративного менеджменту, що були б схвалені бізнес-спільнотою, узгоджувалися з визнаними у світовій практиці підходами й опирались на національну специфіку. Внаслідок такої діяльності в багатьох країнах світу були розроблені Кодекси корпоративного керування, що являли собою сукупність добровільно визначених нормативів і внутрішніх стандартів, які визначають та регулюють особливості корпоративних взаємин.

Нормативно-правовий статус зазначених кодексів суттєво різниться. Так, зокрема, в окремих державах він належить до обов'язкових норм, виконання яких є беззаперечною вимогою для реалізації цінних паперів суб'єкта господарювання на фондовій біржі. Для інших – подібні кодекси не мають відношення до чинного законодавства.

Кодекси корпоративного управління базуються на таких принципах, як:

- покращення продуктивності роботи керівної ланки;
- дотримання контрольних функцій радою директорів, яка лобіює інтереси власників;
- контролювання діяльності суб'єкта господарювання та його управлінської ланки.

В той же час, окрім Кодексу корпоративного керування в провідних країнах світу застосовуються інші підходи до захищеності промислового підприємства від недружніх захоплень, значна частина яких включена до корпоративного нормативно-правового поля держави. Зокрема, у США певні значимі способи захисту суб'єкта господарювання знаходяться в межах корпоративного законодавства держави, що дозволяє їх використовувати автоматично чи за допомогою внесення до статутів всіх товаровиробників.

Більшість країн Європи прийняла закони, що спрямовані на спеціальне координування механізмів об’єднання та поглинання суб’єктів господарювання, водночас засудивши їх недружні поглинання. Безпосередньо в Італії існує кримінальна відповідальність у випадку злочинних дій по відношенню до корпоративних об’єднань. Сучасними нормативно-правовими актами Англії визначено, що існуюча Комісія з проблем добросовісної конкуренції в сфері підприємництва повинна здійснювати моніторинг даних про ймовірність об’єднання чи поглинання.

Рейдерство зазвичай поширене в країнах з економікою перехідного типу, де є широкі можливості здобути мільярдні статки, за демпінговою ціною отримати у власність стратегічний суб’єкт господарювання чи в цілому певну галузь. Сприятливі умови для рейдерських дій мають місце тоді, коли промислове підприємство приватизується з використанням протиправного механізму.

Ключовим завданням рейдерського захоплення є отримання повного контролю над суб’єктом господарювання з подальшим виведенням його майна з законної власності та реалізації зацікавленим особам. В такому випадку наявні активи зазвичай діляться та реалізуються частинами. Помінявши декілька формальних власників, майно вже немає безпосереднього зв'язку з рейдерами, які позбавили його початкових власників, внаслідок чого активи цілком законно можуть стати власністю замовника рейдерського поглинання.

У сучасному світовому просторі рейдерство, як правило, ототожнюють з передачею майна від непродуктивного власника до більш продуктивного. В нашій державі рейдерство розуміють як незаконне поглинання суб’єктів господарювання у неприйнятний та нецивілізований спосіб, що деформує імідж України на міжнародній арені та суттєво послаблює її привабливість для інвесторів, що спричиняє появу реальної загрози подальшому економічному поступу країни, протиставляється функціонуванню ринкових засад зміни власника майна. Як наслідок боротьба з проявами рейдерства повинна відбуватися не лише в межах певних суб’єктів господарювання, але й передусім на рівні держави в контексті функціонування прозорої програми взаємодії та залучення дієвих механізмів.

Після здобуття державного суверенітету в Україні почав впроваджуватися активний процес формування сучасних економічних ринкових відносин. Проте одночасно з появою інноваційних перспектив з’являються раніше невідомі проблеми, які з огляду на їх своєчасність та суперечливість вимагають оперативного вирішення. Серед них – абсолютно інноваційне для України, почасти не зовсім зрозуміле суспільно-загрозливе явище рейдерства, що створило серйозні перешкоди для нагального розвитку вітчизняних суб’єктів господарювання, зазвичай нехтуючи роллю таких суспільно важливих утворень, як приватна сфера, добросовісна конкурентна боротьба та вільний розвиток підприємництва.

Про обсяги поширення рейдерства в нашій державі свідчать численні факти. Зокрема, за висновками провідних фахівців Центру дослідження корпоративних відносин в умовах сьогодення в Україні діють близько 35–50 рейдерських утворень зі спеціальним практичним досвідом, які організовують та здійснюють привласнення майна.

До того ж, кожного року в нашій країні відбувається в середньому 35–40 рейдерських атак, водночас негативний вплив рейдерів на підприємництво суттєво знижує зростання ВВП у середньому на 1–2% на рік.

За таких умов формування продуктивної та цілісної системи захищеності вітчизняного бізнесового простору набуває більшого значення. В той же час, має місце заморожування лакун у чинному нормативно-правовому полі та відтермінування його оптимізації, які з успіхом використовуються рейдерськими групами. Така ситуація пояснюється бізнесовими інтересами та зацікавленістю посадовців у її існуванні, що дозволяє отримати преференції від окреслених оборудок. Загальновідомо, що будь-яка рейдерська атака відбувається з відома високопосадовців владних інституцій, а нерідко і депутатів, які лобіюють інтереси окремих промислово-фінансових кіл.

З метою боротьби з проявами рейдерства слід більш оперативно втілювати інноваційні суспільні технології, які потребують об'єднання зусиль української спільноти. З огляду на це, феноменальність Антирейдерського союзу підприємців є актуальною, оскільки це єдине вітчизняне громадське утворення самозахисту акціонерів, промисловців і підприємців, яке захищає інтереси товаровиробника, захопленого рейдерськими групами або знаходяться під загрозою поглинання. Ця громадська організація є ініціатором формування інституту уповноважених осіб майже у всіх гілках влади, які мають відношення до безпеки українського бізнесового простору. Зокрема, серед них Секретаріат Президента України, де функціонує підрозділ для створення національної програми у площині безпеки, Рада національної безпеки оборони України, при якій сформовано робочу групу, що займається питаннями імплементації сфери безпеки національного бізнесу в систему державної безпеки та перспективи її подальшого розвитку, Кабінет Міністрів України, який вивчає найбільш актуальні проблеми протистояння рейдерству, Верховна Рада України, яка виконує законодавчу роль та тим самим сприяє оперативному розв'язанню проблем, пов'язаних з рейдерством.

З метою ефективної боротьби з проявами рейдерства доцільно запровадити застосування антирейдерських механізмів всередині промислового підприємства. Зважаючи на гальмування процесу законодавчого врегулювання антирейдерської діяльності та запізнілий характер законотворчості в нашій державі, лише в площині суб'єкта господарювання можна досягти відчутних результатів боротьби з рейдерськими захопленнями.

Виходячи з зазначеного, промислове підприємство повинно бути готове до протистояння рейдерським атакам з використанням і впровадженням завчасної стратегії ефективної захищеності від проявів рейдерства. Перспективні запобіжні заходи доцільно спрямувати на формування ефективного підприємницького захисту та зниження загрози ворожого поглинання. Стратегічні засоби протистояння рейдерству мають на меті використання низки відповідних послідовних заходів. Передусім, це постійний контроль за інформаційним простором навколо суб'єкта господарювання для встановлення вияву сторонньої зацікавленості на основі низки характерних симптомів, що дозволить його власникам і керівництву оперативно застосувати доцільні захисні дії. До специфічних проявів можна віднести намагання придбати акції підприємства, ініціювання міноритаріїв позачергового проведення зборів співвласників, блокування акціонерами окремих договорів суб'єкта господарювання, раптові перевірки промислового підприємства контролюючими органами, наявність фактів об'єднання та захоплення суб'єктів господарювання в масштабах регіону або окремої галузі. Систематичне відстеження показників роботи товаровиробника повинне забезпечуватися власною ефективною службою економічної безпеки.

В сучасних реаліях захищеності від рейдерства в Україні приділено недостатньо уваги вченими-економістами. Основна суть питання пов'язана з тим, що значна більшість суб'єктів господарювання переконана у власній захищеності або непривабливості для рейдерів, що спричиняє певне ігнорування найпростішими елементами захисту та дієвою правовою профілактикою. В дійсності це зазвичай зумовлює ситуацію, коли власники акцій виявляють занепокоєння своїм захистом лише в тому випадку, коли має місце фактично завершене рейдерське захоплення, тобто повний контроль над промисловим підприємством вже остаточно втрачений.

Захоплення суб'єктів господарювання та майнових активів у нашій країні відбувається не в результаті прозорого поглинання на законних підставах, а за допомогою вчинення різних правопорушень самими виконавцями рейдерських дій та високопосадовцями судової та виконавчої гілки влади. Фахівці зазначають, що вітчизняний тип рейдерства майже на 100% немає жодного відношення до цивілізованих правовідносин (stock market acquisitions, proxy fight) не має.

Державна політика повинна сприяти розробці та якнайшвидшому втіленню антикорупційної програми, яка б була спрямована на посилення відповідальності високо посадовців за корупційні дії, ухвалення протиправних рішень, їх недостовірність, а також запровадження обов'язкової кримінальної відповідальності для учасників рейдерських технологій, зокрема. реєстраторів, арбітражних керуючих, осіб судово-виконавчої служби та ін.

Універсальної моделі ефективної захищеності суб'єктів господарювання від проявів рейдерства наразі не існує. Проте ймовірність успішного рейдерського захоплення суттєво зменшується в тому випадку, коли власник підприємства своєчасно продумає альтернативні способи захисту, оптимізує систему власності, запровадить систему прийняття оптимальних рішень.

Сучасний досвід свідчить, що найбільш дієвим захистом від рейдерства є реалізація запобіжних заходів, стратегічна мета яких полягає у максимальному зростанні вартості процедури захоплення суб'єкта господарювання, що здатне уможливити нерентабельність рейдерського поглинання. Таким чином власнику підприємства варто запровадити заходи у напрямі трансформації зацікавленості ймовірного рейдера в корпоративному поглинанні в правову площину злиття. З цією метою доцільно здійснити тотальну реструктуризацію бізнесового простору, що дозволить сформувати таку систему власності та керування найбільш цінними активами, яка унеможливить рентабельність рейдерського поглинання суб'єкта господарювання.

Перелік питань:

1. Що таке комерційна таємниця, і які основні її характеристики?
2. Які приклади інформації можуть вважатися комерційною таємницею?
3. Як визначається інтелектуальна власність, і які об’єкти вона охоплює?
4. У чому полягає відмінність між комерційною таємницею та інтелектуальною власністю?
5. Які законодавчі акти України регулюють захист комерційної таємниці?
6. Які міжнародні стандарти захисту інтелектуальної власності ви знаєте?
7. Що таке патент, і які права він надає власнику?
8. Як реєструється торговельна марка в Україні?
9. Які юридичні механізми використовуються для захисту інтелектуальних прав?
10. Що таке договір про нерозголошення (NDA), і яку роль він відіграє у захисті інформації?
11. Які технічні методи використовуються для захисту комерційної інформації?
12. У чому полягає роль політики безпеки у захисті конфіденційної інформації?
13. Що таке ліцензійний договір, і які переваги він надає власнику інтелектуальної власності?
14. Які наслідки може мати витік конфіденційної інформації для підприємства?
15. Як судовий захист допомагає у випадку порушення прав інтелектуальної власності?
16. Які приклади порушень у сфері інтелектуальної власності ви знаєте?
17. Як компанії можуть мінімізувати ризики втрати комерційної інформації?
18. Які інструменти контролю доступу до інформації є найефективнішими?
19. Як впливає витік даних на репутацію підприємства?
20. У чому полягає значення міжнародної співпраці у сфері захисту інтелектуальної власності?

Тести:

1. **Що є основною характеристикою комерційної таємниці?**
   а) вона доступна усім працівникам підприємства;
   б) її можна передавати без дозволу власника;
   в) вона має комерційну цінність і є конфіденційною;
   г) вона регулюється лише на рівні договорів.

2. **Який із наведених об’єктів є прикладом інтелектуальної власності?**
   а) річний звіт підприємства;
   б) логотип компанії;
   в) контракт із постачальником;
   г) перелік співробітників.

3. **Який законодавчий акт регулює авторські права в Україні?**
   а) закон України "Про авторське право і суміжні права";

б) закон України "Про охорону праці";
в) закон України "Про товариства з обмеженою відповідальністю";
г) закон України "Про ліцензування видів господарської діяльності".

4. **Що таке договір про нерозголошення (NDA)?**
   а) договір про передачу прав на об’єкт інтелектуальної власності;
   б) договір про заборону співробітникам розголошувати конфіденційну нформацію;
   в) договір про спільне використання інтелектуальної власності;
   г) договір про ліцензування програмного забезпечення.

5. **Який із наведених методів є технічним засобом захисту комерційної інформації?**
   а) підписання NDA;
   б) використання шифрування даних;
   в) проведення тренінгів для співробітників;
   г) реєстрація торговельної марки.

6. **Що є основною функцією політики безпеки на підприємстві?**
   а) реєстрація прав інтелектуальної власності;
   б) регулювання правил використання інформації та її захисту;
   в) забезпечення технічної підтримки;
   г) проведення аудитів фінансової діяльності.

7. **Яке порушення вважається крадіжкою комерційної таємниці?**
   а) витік інформації через недотримання політик безпеки;
   б) несанкціоноване використання торговельної марки;
   в) неналежне зберігання конфіденційної інформації;
   г) розголошення даних клієнтів конкуренту.

8. **Який із наведених прикладів належить до авторських прав?**
   а) рецепт приготування продукту;
   б) логотип компанії;
   в) літературний твір;
   г) список клієнтів.

9. **Яка функція патенту?**
   а) забезпечення конфіденційності інформації;
   б) надання виключного права на використання винаходу;
   в) визначення відповідальності за порушення;
   г) регулювання фінансової діяльності підприємства.

10. **Яке міжнародне регулювання стосується захисту інтелектуальної власності?**
    а) TRIPS;

б) GDPR;
в) ISO 9001;
г) Паризька конвенція.

11. **Що є основним наслідком витоку конфіденційної інформації?**
а) підвищення конкурентоспроможності;
б) зниження фінансових втрат;
в) репутаційні та фінансові збитки;
г) підвищення кількості клієнтів.

12. **Що таке ноу-хау?**
а) неформалізовані знання, які мають цінність;
б) офіційно зареєстровані авторські права;
в) інформація, доступна широкому загалу;
г) технології, що втратили актуальність.

13. **Що є наслідком порушення прав на торговельну марку?**
а) підвищення доходів;
б) вилучення контрафактної продукції з ринку;
в) підвищення цін на продукцію;
г) збільшення кількості клієнтів.

14. **Що є метою шифрування даних?**
а) полегшення доступу до конфіденційної інформації;
б) збереження інформації у зашифрованому вигляді для її захисту;
в) забезпечення аудиту безпеки;
г) розподіл інформації між співробітниками.

15. **Що таке торговельна марка?**
а) комерційна таємниця підприємства;
б) знак, що відрізняє товари та послуги;
в) технологічний процес виробництва;
г) фінансова стратегія підприємства.

16. **Як захищається інформація в електронному вигляді?**
а) через контроль фізичного доступу;
б) за допомогою шифрування даних і багатофакторної аутентифікації;
в) зберіганням на паперових носіях;
г) видаленням інформації після використання.

17. **Що може бути предметом договору про ліцензування?**
а) фінансовий звіт підприємства;
б) літературний твір або програмне забезпечення;
в) перелік працівників;

г) стратегія маркетингу.

18. **Що таке NDA?**
    а) договір про співпрацю між двома компаніями;
    б) договір про захист конфіденційної інформації;
    в) договір про продаж товарів;
    г) договір про аудит.

19. **Що таке TRIPS?**
    а) інструмент для створення політик;
    б) міжнародна угода про захист прав інтелектуальної власності;
    в) законодавство України про комерційну таємницю;
    г) інструкція щодо безпеки інформації.

20. **Що є основним завданням судового захисту інтелектуальних прав?**
    а) створення резервних копій інформації;
    б) відновлення порушених прав і компенсація збитків;
    в) використання нових технологій;
    г) надання конфіденційності інформації.

Практичні завдання:

Завдання 1. Ідентифікація комерційної інформації
Мета: Навчитися визначати, які дані можуть вважатися комерційною таємницею.

1. Оцініть фінансовий звіт та бізнес-стратегію на наступний рік й визначте, чи є дана інформація комерційною таємницею. Обґрунтуйте свою думку
2. Запропонуйте заходи для захисту кожного типу комерційної інформації.

Завдання 2. Оцінка ризиків витоку комерційної інформації
Мета: Провести аналіз ризиків і розробити план їх нейтралізації.

1. Проаналізуйте такі ризики:
   - несанкціонований доступ до бази даних клієнтів;
   - витік конфіденційної інформації через електронну пошту;
   - викрадення інформації про маркетингові кампанії.
2. Заповніть таблицю для оцінки ризиків:

Тип ризику	Ймовірність виникнення	Можливі збитки (тис. грн)	Рівень ризику
Несанкціонований доступ			
Витік через електронну пошту			
Викрадення інформації			

3. Розробіть заходи для мінімізації ризиків.

Завдання 3. Створення політики безпеки

Мета: Розробити основні положення політики безпеки комерційної інформації для підприємства.

1. Визначте ключові елементи політики безпеки:
   - розмежування доступу до інформації;
   - вимоги до використання електронних пристроїв;
   - регламентація передачі конфіденційних даних.
2. Сформулюйте правила поводження з комерційною інформацією:
   - для співробітників;
   - для партнерів підприємства.
3. Представте політику у вигляді структурованого документа.

Завдання 4. Аналіз порушень інтелектуальних прав

Мета: Навчитися ідентифікувати порушення інтелектуальних прав та аналізувати їхні наслідки.

1. Ознайомтеся з такими випадками:
   - використання логотипу без дозволу власника.
   - копіювання програмного забезпечення.
   - розголошення унікального рецепту виробництва.
2. Для кожного випадку:
   - опишіть наслідки порушення для власника.
   - запропонуйте шляхи вирішення конфлікту.
3. Представте результати аналізу у вигляді таблиці:

Порушення	Наслідки	Можливі рішення
Використання логотипу		
Копіювання програмного забезпечення		
Розголошення рецепту		

Завдання 5. Розробка ліцензійного договору

Мета: Навчитися створювати ліцензійний договір для передачі прав на об’єкт інтелектуальної власності.

1. Уявіть, що ваша компанія передає право на використання програмного забезпечення іншому підприємству.
2. Розробіть ліцензійний договір, який включатиме:
   - предмет договору (об’єкт інтелектуальної власності);
   - умови використання;
   - обмеження та зобов’язання сторін;
   - санкції за порушення договору.
3. Представте договір у вигляді текстового документа.

Завдання 6. Використання технічних засобів захисту

Мета: Оцінити ефективність технічних методів захисту комерційної інформації.

1. Проаналізуйте наступні заходи:
    - використання шифрування даних;
    - встановлення систем контролю доступу;
    - використання антивірусного програмного забезпечення.
2. Оцініть їх ефективність за такими критеріями:
    - вартість впровадження;
    - рівень захисту;
    - легкість використання.
3. Представте результати у вигляді таблиці:

Метод захисту	**Вартість**	**Рівень захисту**	**Легкість використання**
Шифрування			
Системи контролю доступу			
Антивірусне ПЗ			

РОЗДІЛ 3. УПРАВЛІННЯ ПЕРСОНАЛОМ ТА СТРАТЕГІЇ БЕЗПЕКИ

ТЕМА 9. УПРАВЛІННЯ ПЕРСОНАЛОМ У КОНТЕКСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

9.1 Вплив людського фактору на економічну безпеку.
9.2 Кадрові ризики та їх мінімізація.
9.3 Політики конфіденційності та лояльності персоналу.
9.4 Навчання та підвищення кваліфікації у сфері безпеки.

9.1 Вплив людського фактору на економічну безпеку

Роль людського фактора в економічній безпеці

Людський фактор є одним із ключових елементів, який впливає на рівень економічної безпеки підприємства. Співробітники можуть як сприяти забезпеченню безпеки, так і створювати потенційні загрози через недбалість, недостатню кваліфікацію чи свідомі дії. Розуміння природи людського фактора та впровадження відповідних заходів управління є важливими для захисту підприємства.

Необхідно зробити наголос, що вдала робота суб'єкта господарювання в ринковій економіці зумовлює вживання результативної системи заходів щодо захищеності. Зазвичай, переважна більшість ризиків суб'єкта господарювання продукуються його власними працівниками. Згідно статистичних даних, приблизно 51% економічних правопорушень вчиняє персонал підприємства (рис. 9.1), натомість вдала робота щодо посилення кадрової безпеки може зменшити прямі та непрямі втрати компанії, пов'язані з персоналом, на майже 60%.

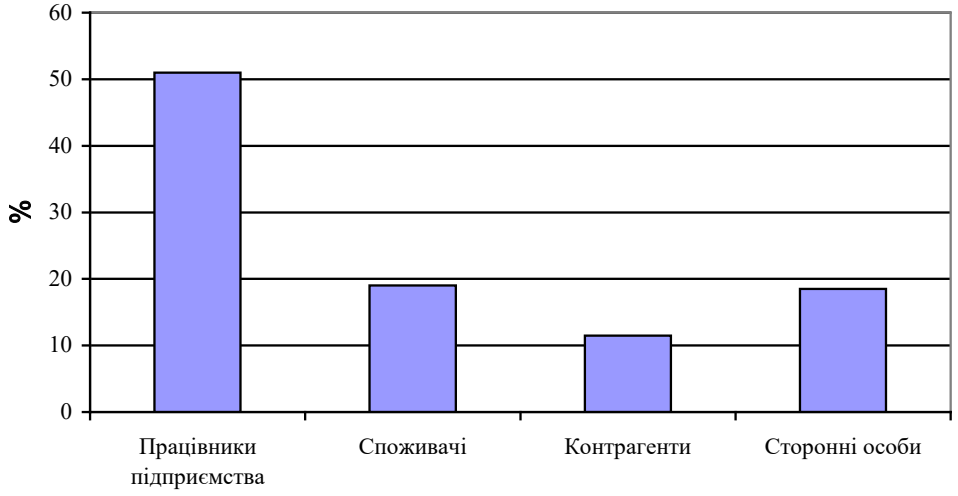

Рисунок 9.1 – Суб'єкти вчинення економічних правопорушень на підприємстві

Дані ресурсу Content Security говорять про те, що зовнішні та внутрішні загрози підприємницької діяльності мають таку структуру (рис. 9.2).

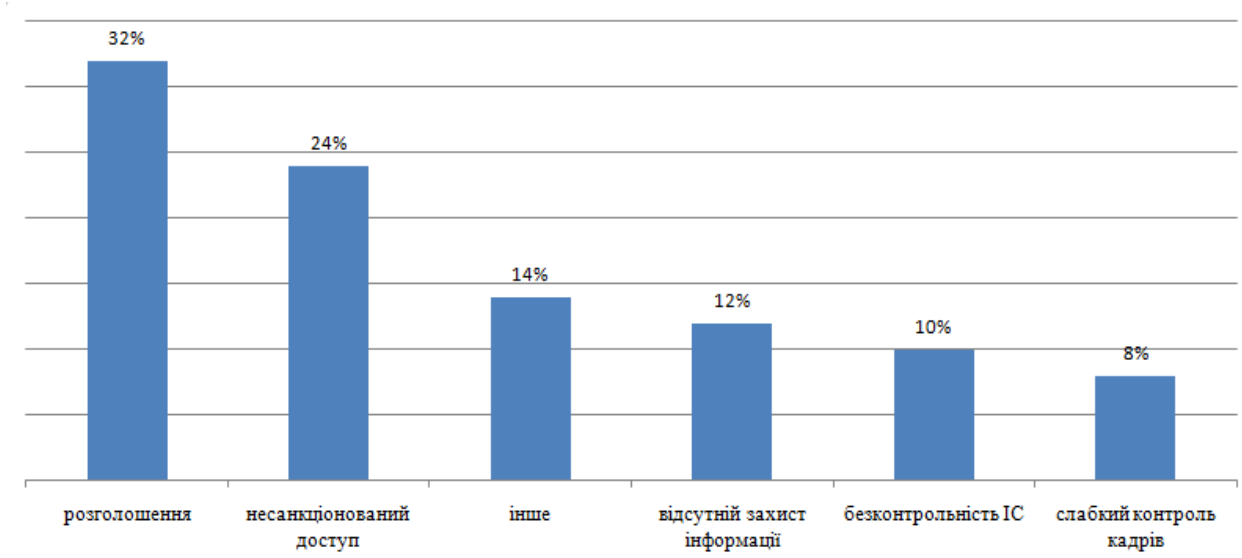

Рисунок 9.2 – Структура загроз підприємницької діяльності, пов'язаних з працівниками

Згідно приведених даних у переліку факторів, що складають усю сукупність економічних правопорушень левову частку займає саме людський чинник. Це ще більше висвітлює питання забезпечення кадрової складової безпеки на державному рівні. Ще одним підтвердженням цього висновку є дані, отримані компанією Ernst&Young, які свідчать, що в нашій державі рівень внутрішньокорпоративного шахрайства є вищим за показник країн, що розвиваються (20%), але дещо більшим за відповідний показник у розвинених країнах (13%). В Україні крім викрадення інформації, існує досить багато випадків «чорного» піару колишніми працівниками, судових позовів, які відбиваються на діловій репутації суб'єкта господарювання, помилки у кадрових документах, непрофесіоналізм працівника.

Розмір шкоди від впровадження заходів з кадрової безпеки є достаньо показовим (зокрема попередження внутрішньокорпоративноих крадіжок чи шахрайства), зокрема у США цей показник сягає позначки у 4,2 млрд. дол., тобто на кожного суб'єкта підприємницької діяльності припадає близько 2,4 млн. дол. збитків. Однак збитки від усунення загроз кадровій захищеності не обмежуються лише економічною стороною, вони спричиняють ще й значні нематеріальні втрати, зокрема зіпсованою репутацією, зниженням вартості його акцій, пригніченням морального духу працівників, порушенням ділових стосунків з контрагентами тощо. Отже, суб'єкти підприємницької діяльності стикаються зі збільшенням дій загроз з боку власних робітників, що пов'язано зі зростанням кількісних та якісних показників ризику в царині корпоративного менеджменту. Небажані наслідки цих процесів призводять до неефективного управління суб'єктом господарювання та відповідно даного майнового об'єкта його власником. Виходячи з вищесказаного, можна стверджувати, що обґрунтування загроз кадровій захищеності сприяє подоланню ризиків у виробничій та комерційній діяльності суб'єкта господарювання.

Формування кадрової безпеки суб'єкта господарювання, продуктивне використання трудових ресурсів взаємопов'язане з менеджментом якості персоналу, та дає змогу оптимізувати процес підвищення ефективності трудової діяльності, зростання кількості виготовленої продукції чи розширення комплексу наданих послуг, дотримання світових

стандартів якості власної продукції та розвитку промислового підприємства в цілому. Отже, від продуктивного функціонування персоналу буде значною мірою залежати не тільки ефективний поступ товаровиробника, але й його ринкові можливості та економічна захищеність. З огляду на це окреслення ролі кадрової безпеки в загальній системі економічної захищеності суб'єкта господарювання залишається нагальною проблемою, а її вивчення передбачає з'ясування цілого комплексу широкого кола питань. У зв'язку з цим потребує уваги визначення ролі кадрової безпеки як сегмента всієї системи економічної захищеності промислового підприємства.

Слушною є думка вітчизняної дослідниці Багрової І. щодо обґрунтування інтелектуальної трудової діяльності як роботи в напрямку формування інноваційних умов забезпечення сучасної програми одержання абсолютно нового програмного продукту в площині матеріального та нематеріального виробництва, що опирається на кардинально новаторські науково-технічні, теоретично-технологічні чи організаційно-економічні засади, основним наповненням яких є вирішення цілком нових продуктивних завдань, які суттєво відрізняються від повсякденних та сприяють підвищенню рівня соціального та економічного стану суспільства. В цьому ж напрямку відомий український вчений Колот А. обґрунтовує доцільність здійснення різноаспектних студій інноваційної трудової діяльності в площині створення в Україні сучасної економіки знань, що окреслюється ним як трудова сфера, яка визначається значною часткою знань, наявністю інтелекту, творчої складово.

На сучасній стадії розвитку нових методів менеджменту на підприємстві пріоритетну роль відіграє трудовий персонал, що являє собою найбільшу цінність та найважливіше знаряддя для продуктивної роботи суб'єкта підприємницької діяльності. Кадри визначають всі найвагоміші напрямки життєдіяльності підприємства, будучи тісно пов'язаними з економічною захищеністю. В той же час трудовому персоналу промислового підприємства властива динамічність, яка характеризується не лише процесом прискорення інноваційності професійних здобутків, знань, умінь та відповідних навичок, але й постійним зростанням значення професійно необхідних і ділових здібностей співробітників. Освітньо-кваліфікаційний рівень потенціалу професійних вмінь та навичок сьогодні є першочерговими компетенціями працівників. З огляду на це, існуючі на сучасному етапі системи менеджменту спрямовані на формування різнопланових характеристик персоналу з метою якомога ефективнішого подальшого їх використання у виробничій сфері. Посилення значущості соціального чинника виробництва спонукає до якісних трансформацій системи управління промисловим підприємством та реалізується в інноваційних моделях, методиках і природі менеджменту персоналу. Як наслідок – для гармонійного розвитку трудового потенціалу доцільно запровадити ефективні механізми управління кадрами, що дасть змогу сформувати належну економічну безпеку суб'єкта господарювання. Водночас окреслення загроз безпеці персоналу дозволить мінімізувати ризики підприємства у площині виробничо-господарської сфери.

Переважна більшість українських та зарубіжних науковців термін «безпека персоналу» розуміють по-різному. Проблеми безпеки персоналу в контексті економічної захищеності суб'єктів підприємницької діяльності розглядаються у дослідженнях провідних вчених і практиків.

Безпека персоналу являє собою певний процес уникнення негативної дії на економічну захищеність суб'єкта господарювання за допомогою тих ризиків і загроз, що прямо чи

опосередковано пов'язані з питаннями управління трудовими ресурсами, їх інтелектуальними можливостями та виробничими відносинами. В такій ситуації для запровадження заходів в напрямку уникнення, мінімізації, нейтралізації чи запобігання загрозам безпеці персоналу варто вирішити низку завдань, покладених на існуючу систему безпеки персоналу. У разі планомірного, чіткого, зваженого та комплексного підходу до окреслення ключових завдань, що стоять перед системою безпеки персоналу, з обов'язковим урахуванням особливостей та типології ймовірних загроз, що можуть мати найбільший вплив, можна досягти бажаних результатів.

Таким чином, можна вважати, що безпека персоналу представлена у вигляді певного механізму уникнення негативної дії на економічну захищеність суб'єкта господарювання за допомогою ймовірних ризиків та потенційних загроз, що мають відношення до персоналу в цілому та його інтелектуальної складової зокрема. Пріоритетом окресленого підходу є використання в якості бази превалюючої ролі безпеки персоналу по відношенню до інших складових системи економічної захищеності товаровиробника, оскільки вона прямо пов'язана з трудовими ресурсами, які в будь-якому з компонентів є головними.

У наявній теорії економічної захищеності наразі не існує одностайних чітко визначених підходів до формування безпеки персоналу, прозоро та логічно вибудуваної системи та окресленого механізму, що ускладнює продуктивне практичне застосування наявних можливостей та досягнення бажаного рівня безпеки персоналу внаслідок звуженого розуміння. Значна частина суб'єктів підприємницької діяльності практично нехтує заходами захищеності або звужує їх тільки до фізичного захисту.

Також першочерговість дослідження надалі саме безпеки персоналу зумовлене сучасним вагомим значенням людського чинника в міжнародній економіці. Зокрема, нова економіка, інформаційна економіка чи безпосередньо економіка знань, становлення якої відбувається на сучасному етапі, визначається досить вагомим внеском інтелектуальних та людських можливостей у порівнянні з матеріальною складовою.

Таким чином слід зазначити, що мають місце різнопланові підходи щодо трактування категорії кадрової безпеки (табл. 9.1).

Таблиця 9.1 – Трактування категорії «Кадрова безпека»

Автор	Визначення
1	2
О.А. Кіриченко	Інформаційно-правова база формування процесу кадрового менеджменту: правові аспекти трудових відносин, розробка регуляторних нормативних актів, забезпечення масивом необхідної інформації наявних структурних підрозділів керування кадрами.
А.В. Козаченко, В.П. Пономарев, О.М. Ляшенко	Механізми уникнення негативного впливу на безпеку суб'єкта господарювання за допомогою мінімізації загроз і ризиків, які мають відношення до інтелектуальних можливостей та трудової діяльності загалом.
М.А. Швець	Оптимізація трудових ресурсів промислового підприємства, забезпечення максимальної стійкості виробничої діяльності суб'єкта господарювання, формування підґрунтя для реалізації наявного потенціалу задля виконання ключових завдань.

Продовження таблиці 9.1

1	2
А.Я. Кібанов	Пріоритетний вектор роботи з персоналом, система наявних принципів, способів, моделей організації досягнення основних цілей, завдань, покликаних зберегти, посилити та удосконалити кадрові можливості, сформувати колектив однодумців, здатний брати на себе відповідальність за своєчасність та результативність роботи, оперативно реагувати на виклики динамічного ринкового середовища, опираючись на окреслену стратегію подальшого розвитку підприємства
Л.М. Томаневич	Складовими безпеки персоналу є: безпечні умови життєдіяльності, професійна, соціально-мотиваційна та психологічна захищеність, які необхідні для створення оптимальної моделі системи функціонування безпеки персоналу, задіяного у виробничо-господарській сфері.
І.П. Шульга	Наявність на промисловому підприємстві необхідних трудових ресурсів, створення продуктивної системи кадрового менеджменту та ефективної системи комунікації. Інтелектуальний чинник трудового потенціалу становить важливу частину кадрової безпеки.

Спираючись на викладені тлумачення дефініції безпеки персоналу та виходячи з постійно зростаючого значення персоналу у виробничо-господарській діяльності промислового підприємства, можна запропонувати таке визначення:

Кадрова безпека - це сукупність принципів, способів, моделей формування захисту працівників від проявів негативного впливу ймовірних ризиків та загроз, покликаних зберегти, посилити та удосконалити кадрові можливості, сформувати колектив однодумців, здатний брати на себе відповідальність за своєчасність та результативність роботи, оперативно реагувати на виклики динамічного ринкового середовища, опираючись на окреслену стратегію подальшого розвитку суб'єкта господарювання, пріоритетним завданням якої є лобіювання корпоративних інтересів з метою створення умов для найбільш ефективного управління персоналом як визначального ресурсу для забезпечення високого рівня конкурентоспроможності підприємства.

Дане трактування значною мірою узагальнює основні наукові підходи до розуміння економічної захищеності суб'єкта господарювання. В той же час слід виокремити пріоритетні ознаки безпеки персоналу, в якій у ролі об'єкта та суб'єкта виступає сам персонал:

– трудовий потенціал промислового підприємства належить до головних його ресурсів. Насамперед, персонал – це і є саме підприємство; по-друге, трудовий потенціал, на відміну від фінансових і матеріальних ресурсів є домінуючим джерелом при створенні додаткової вартості; по-третє, злагоджений колектив однодумців належить до пріоритетних конкурентних переваг;

– персонал прагне систематично вдосконалюватися та розвиватися, що може стати найбільш вагомим та постійним джерелом зростання продуктивності роботи суб'єкта господарювання;

– трудова діяльність працівника в сучасному суспільстві становить від 30 до 50 років, що свідчить про те, що відносини співробітником та роботодавцем можуть бути досить тривалими;

– у менеджменті людська складова – це найбільш складний компонент. Інтелектуальна складова дає змогу сформувати розмаїтість і непередбачуваність працівників, що значною мірою ускладнює їх аналіз, на відміну від інших складових;

– працівники формують не тільки конкурентні переваги суб'єкта господарювання, але й створюють певні загрози, потребуючи тим самим запровадження особливих підходів до забезпечення захищеності.

9.2 Кадрові ризики та їх мінімізація

Сутність кадрових ризиків

Кадрові ризики — це загрози, пов'язані з діяльністю персоналу, які можуть негативно вплинути на економічну безпеку підприємства. Вони виникають через недбалість, недостатню кваліфікацію, низький рівень лояльності співробітників або навіть їхні умисні дії.

Класифікація кадрових ризиків, а також вплив кадрових ризиків на підприємство подані в таблиці 9.2 та на рисунку 9.3:

Таблиця 9.2 – Вплив кадрових ризиків на підприємство

Ризик	Можливі наслідки
Висока плинність кадрів	Збільшення витрат на пошук і навчання нових працівників.
Недбалість співробітників	Витоки конфіденційної інформації, збої у виробничих процесах.
Низька лояльність персоналу	Втрата конкурентоспроможності через зниження продуктивності.
Конфлікти в команді	Зниження ефективності роботи та ризик втрати ключових фахівців.

Організаційні ризики

- Недостатня кількість кваліфікованих працівників.
- Високий рівень плинності кадрів.
- Неефективна система управління персоналом

Поведінкові ризики

- Недбалість або помилки під час виконання обов'язків.
- Несанкціоновані дії, що завдають шкоди підприємству.
- Втрата мотивації та низька продуктивність

Комунікаційні ризики

- Відсутність ефективної взаємодії між працівниками та керівництвом.
- Конфлікти в команді

Технічні ризики

- Використання ненадійних паролів або пристроїв.
- Недотримання стандартів інформаційної безпеки

Рисунок 9.3 – Класифікація кадрових ризиків

Кадрова безпека на підприємстві включає усе, на що скеровуються зусилля відносно створення захищеного середовища. Через те що кадри – це первинна ланка для всіх інших складових економічної безпеки підприємства, то до її об'єктів слід віднести такі:

- партнери, акціонери, керівники, позаштатний та штатний персонал, які мають доступ до конфіденційної інформації, що є комерційною таємницею, або ж певних даних, що не підлягають розголосу;
- персонал, який має доступ до фінансових ресурсів суб'єкта господарської діяльності, який може привласнити кошти (розтратити, навмисно скеровати на певні махінації);
- власний персонал, який навмисно чи ненавмисно може завдати шкоди програмному забезпеченню та технічним засобам, які застосовуються при роботі;
- особи (зазвичай власний персонал), що можуть брати участь в корпоративній розвідці, у промисловому шпіонажі або ж навіть у знищенні об'єктів науково-технічної інформації, об'єктів авторського права та суміжних прав, засобів індивідуалізації та ноу-хау, об'єктів промислової;
- працівники, які можуть розкрадати або завдавати шкоду доступним матеріальним ресурсам підприємства;
- інформація з обмеженим доступом, захищені та вільно розповсюджувальні інформаційні ресурси, що є об'єктом захисту від викривлення, несанкціонованого вилучення, втрати, передачі третім особам, що зрештою може завдати збитків суб'єкту господарювання.

Фізичні та юридичні особи, служби, підрозділи, установи, організації, які безпосередньо беруть участь у забезпеченні захищеності є суб'єктами кадрової безпеки. Останні варто поділити на дві окремі групи:

а) **внутрішні**: кадрова служба, служба безпеки підприємства, юридичний відділ, окремі структурні підрозділи, персонал суб'єкта господарської діяльності;
б) **зовнішні**: державні органи влади, правоохоронні державні та недержавні структури, працівники служби безпеки інших підприємств (тобто будь-які суб'єкти, що безпосередньо не вступають у відносини з суб'єктом господарської діяльності).

Система забезпечення кадрової безпеки, як і будь-яка інша система, існує у нормативно-правовому полі діяльності (на сьогодні це є беззаперечною умовою її результативності). Правова та законодавча підтримка кадрової захищеності регламентовано законами, законодавчими, нормативно-правовими та підзаконними актами, а також внутрішіми положеннями та певними регламентами.

Кадрова безпека має бути забезпечена достовірною, аналітично вірно обробленою інформацією шляхом отримання, опрацювання й захисту інформаційних даних, які необхідні у вибудовуванні стратегії та тактики менеджменту, що, звичайно, вимагає отримання даних щодо відкритих та прихованих загроз існуванню кадрової безпеки. Власне це є першою сходинкою для подолання більшості небезпек, яким піддається система існуючої кадрової безпеки.

Механізм забезпечення кадрової безпеки діє на основі таких завдань:

- пошук, систематизацію та класифікацію типових загроз, через які у кадровій безпеці виникли певні дестабілізуючі та деструктивні явища;
- врівноваження системи мотиваційних важелів і штрафних заходів та механізму відшкодування матеріальних збитків;
- злагоджена робота зі створення злагодженого й високопрофесійного колективу на підприємстві;
- створення умов, за яких досягається бажаний рівень захисту всіх компонентів, що входять до кадрової безпеки;
- доведення до відома персоналу в формі бесіди щодо відповідальності за неправомірні дії на робочому місці (одержання хабарів, корупція, побори тощо);
- створення системи контролю за належним дотриманням нормативно-законодавчих документів в частині зловживань службовим становищем, хабарництвом та іншими подібними правопорушеннями з боку робітників підприємства;
- проведення ознайомчих та навчальних тренінгів, лекцій, семінарів на тему побудови кадрової безпеки суб'єкта господарювання й розкриття питання комерційної таємниці на підприємстві.

Створення моделі ефективної системи функціонування кадрової безпеки уможливлює побудову її оптимальної структури, дозволяє внести до неї відповідні складові, відбити певні стратегічні ланцюжки, що з рештою дозволить чітко окреслити підходи до бажаної моделі. Власне саме така система здатна піднести кадрову складову економічної захищеності на

якісно новий рівень забезпечивши її продуктивне функціонування без фінансових та матеріальних втрат, при цьому отримуючи позитивну динаміку власного капіталу та працюючи згідно єдиної підприємницької мети.

Кадрова безпека суб'єкта підприємницької діяльності є однією з найважливіших складових економічної захищеності. Саме працівники чинять вплив на всі сторони діяльності підприємства, вони нерозривно зв'язані з його продуктивною діяльністю. Отже, з-поміж систем економічної захищеності суб'єкта господарювання та менеджменту персоналу знаходиться кадрова складова безпеки як певна підсистема, що може забезпечити злагоджену та продуктивну роботу суб'єкта господарювання і високі динамічні результати на майбутнє, а ось визначення ролі, місця, а також певного рівня щодо впливу кадрового чинника в цілісній системі економічної захищеності суб'єкта господарювання вимагає значних зусиль.

Методи мінімізації кадрових ризиків

1. **Удосконалення процесів управління персоналом**
   - Чіткий розподіл обов'язків і зон відповідальності.
   - Регулярне оновлення посадових інструкцій.
2. **2. Навчання і розвиток персоналу**
   - Організація тренінгів із професійних навичок.
   - Навчання з питань інформаційної безпеки та ризик-менеджменту.
3. **Мотивація та підвищення лояльності**
   - Запровадження матеріальних і нематеріальних винагород.
   - Формування корпоративної культури, що підтримує ініціативність і відданість.
4. **Забезпечення ефективних комунікацій**
   - Відкритий діалог між керівництвом і персоналом.
   - Розробка програм підтримки співробітників.
5. **Використання технологій**
   - Впровадження систем контролю доступу до інформації.
   - Регулярний моніторинг діяльності працівників у робочих системах.

Таблиця 9.3 – Рекомендації щодо управління кадровими ризиками

Метод	Очікуваний ефект
Навчання співробітників	Підвищення професійної кваліфікації та зменшення кількості помилок.
Розробка програм лояльності	Зниження рівня плинності кадрів.
Аудит інформаційної безпеки	Виявлення вразливостей у роботі співробітників.
Регулярний аналіз ефективності	Підвищення продуктивності роботи персоналу.

При цьому структура кадрових ризиків може мати приблизно такий вигляд (рис. 9.4):

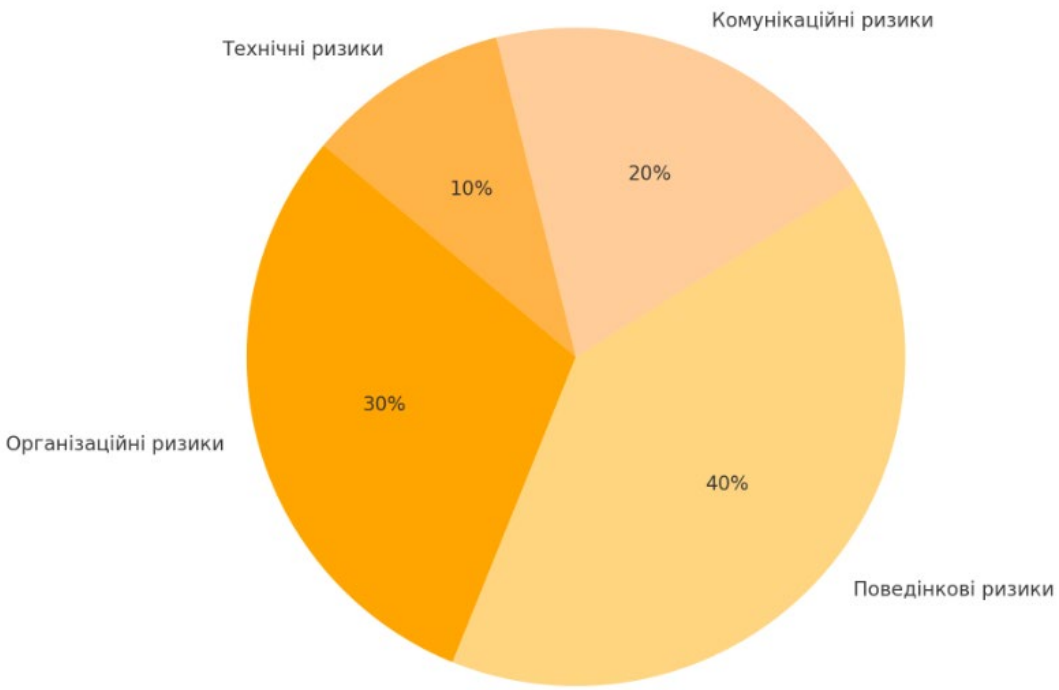

Рисунок 9.4 – Розподіл кадрових ризиків

Мінімізація кадрових ризиків дозволяє підприємствам:

- підвищувати ефективність роботи персоналу;
- зменшувати витрати на пошук і навчання нових співробітників;
- забезпечувати стабільність і розвиток компанії.

9.3 Політики конфіденційності та лояльності персоналу

Сутність політик конфіденційності та їх значення

Політики конфіденційності — це внутрішні нормативні акти, які визначають порядок роботи з інформацією, встановлюють права та обов'язки працівників у сфері захисту даних. Їх основною метою є забезпечення збереження конфіденційної інформації підприємства та мінімізація ризиків витоків даних.

Зазвичай класифікація мотивів (причин) вчинення злочинів співробітниками суб'єкта господарювання має такий вигляд:

- фінансові складнощі працівника, неспроможність щодо задоволення нагальних власних життєвих потреб;
- психологічна схильність (готовність) особи до посадових зловживань;
- порочні захоплення, вчинки та зв'язки;
- незадовільна кваліфікація менеджерів господарюючого суб'єкта;
- несприятливий клімат у колективі суб'єкта господарювання;
- недостатній рівень контролю керівництвом за діяльністю власних співробітників;
- наявність слабких ланок (так званих «дірок») в системі керування діяльністю суб'єкта господарювання;

– невідповідне управління кадрами, що дозволяє обіймати стратегічні посади працівникам-аферистам.

Значний вплив злочинів з боку працівників на діяльність підприємства вимагає глибокого вивчення та створення методичних основ щодо кадрової захищеності. Відповідно до здобутків вітчизняних та зарубіжних вчених, можна стверджувати що синтетичний характер кадрової безпеки, тобто симбіоз економічної теорії, теорії управління персоналом, економіки праці, політології, соціології на мікро- та на макрорівні дає змогу формувати продуктивну кадрову захищеність суб'єкта господарювання. Кадрова безпека – це комбінація складних та прихованих взаємопов'язаних складових (табл. 9.4).

Таблиця 9.4 – Складові кадрової безпеки суб'єкта господарювання

Складова	**Наповнення**
1	2
Життєзабезпечення	здоров'я – забезпечення належних умов праці із попередження травматизму та професійних захворювань в компанії; фізична – застосування необхідного комплексу заходів з метою уникнення порушень правил безпеки
Соціально-заохочувальна	фінансова – платоспроможність співробітників, їх впевненість у збереженні роботи; гідна оплата, що мотивує високоефективну працю; морально-етична – організація тренінгів, конференцій, семінарів, круглих столів, групових дискусій; мотивація до високих результатів власної праці; прагнення співробітників до покращення власного іміджу; адміністративно-незалежна – унеможливлення невідповідних посадових призначень, через родинні або інші зв'язки особистого характеру; кар'єрна – просування по кар'єрних сходинках талановитих працівників, моральне заохочення; можливість до самореалізації при виконанні професійних обов'язків.
Професійно-кваліфікаційна	праці – виважена система підходів, принципів, дій, які націлені на побудову відповідних умов праці (рівень заробітної плати, обладнання робочого місця, посада) з використанням новаторського досвіду на ринку праці; інформаційна – передбачення необхідної структури персоналу, встановлення потреби в персоналі, стратегічне, тактичне планування та залучення кадрів, оцінювання ефективності праці для встановлення можливостей кожного окремого працівника; пенсійно-страхова – соціальний супровід співробітників (медичне обслуговування, страхування); отримання сучасних знань – впровадження інноваційних технологій в роботі кадрів, підвищення кваліфікаційного рівня (знань, умінь, навичок, здібностей)

Продовження таблиці 9.4

1	2
Конкурентна	контрольна – заборонене зловживання домінуючим становищем деяких співробітників, захист прав працівників, усунення заборонених положень з контрактів; своєчасне інформування персоналу стосовно їх прав та обов'язків
Конфліктологічна	патріотична – створення відповідного морально-психологічного клімату на підприємстві через позитивне ставлення до роботи, із залученням психологічних прийомів які спонукають до згуртованості колективу, створюють узгодженість, внутрішньо корпоративну неконфліктність, відповідальність за результати праці, вимогливість в інтересах виробництва як до себе так і до інших, товариську допомогу; комунікаційно-психологічна – сприяння належним діловим комунікаціям та формування сприятливого клімату в колективі, врахування доцільних інтересів та побажань співробітників, їх особистісних можливостей, задоволеність вертикальною та горизонтальною системою менеджменту на промисловому підприємстві

Сутність кадрової безпеки полягає в характеристиці певного стану системи, коли можна спостерігати найбільш вдале поєднання її наявних функціональних складових, формування захисту та спроможність протидіяти як внутрішнім так і зовнішнім загрозам та впливам, що безпосередньо пов'язані з персоналом, належний структурний аналіз, дослідження та прогноз впливу професійної діяльності персоналу на імовірні внутрішні та зовнішні показники системи.

Управління кадровою безпекою є складним процесом і не лише через недосконаліть теоретичного опрацювання, але й по причині багатогранності цього процесу та наявності значної кількості чинників. Тому кадрову безпеку на підприємстві необхідно опрацьовувати системно та комплексно.

На сьогодні ринкові реалії вимагають чітко проробленої, конкретної, спрямованої, націленої на досягнення високого результату програми кадрової роботи, що з рештою позначиться на загальному стані економічної захищеності суб'єкта господарювання. Отже кадрова складова є визначальним чинником для процесу створення економічної захищеності підприємства, яка спирається на етику та трудові відносини, на інтелектуальний потенціал, що з рештою має створити стабільне середовище із високими економічними показниками, нівелюючи при цьому зовнішні та внутрішні загрози особистого та суспільного розвитку. Все це з рештою дозволить підвищити рівень та якісні показники життя, що властиві сучасному суспільству.

Кадрова безпека тісно пов'язана з заробітною платою відповідає трудовому внеску працівників, якості та результатам праці та є одним з компонентів добробуту населення. З кінця минулого сторіччя в Україні державне управління оплатою праці майже було відмінено, суб'єкти господарювання почали на власний розсуд вирішувати питання щодо заробітної платні, чисельності необхідного персоналу, нормування та організації праці. Прямий державний вплив був обмежений вимогою щодо розміру мінімальної заробітної оплати та переліком відповідних ставок для працівників бюджетної галузі. Перекладення на

розсуд підприємств розмірів та системи оплати праці було, звичайно, виправданим, оскільки за умов ринкової економіки суб'єкти господарювання почали самостійно відповідати за показники власної роботи і в тому числі й в питаннях соціального захисту власних співробітників та їх сімей. Тобто ефективність праці багато в чому визначається його оплатою. Заробітна плата при правильній організації забезпечує прямий і безпосередній зв'язок доходів з кількістю та якістю вкладеної праці. Безпосередньо через заробітну плату оцінюється кваліфікація, складність виконуваних робіт, обсяг та якість створених матеріальних благ. Оцінка праці керівної ланки, спеціалістів та службовців здійснюється не на пряму, а через результати роботи суб'єкта господарювання чи певних або структурно-виробничих підрозділів. Заробітна плата – це оцінка результів не лише особистої, але й колективної роботи. Вона є найбільш гнучкою та мобільною формою в наявній системі суспільного розподілу. Оскільки це частина валового національного доходу, який виражено в певній грошовій формі, то заробітна плата існує у відповідності до ринкових процесів, що мають місце в економіці в цілому.

Станом на 2024 рік проблема **розриву між офіційним і фактичним прожитковим мінімумом** в Україні залишається актуальною і є однією з головних ознак соціального дисбалансу в умовах воєнної економіки.

Згідно з даними **Міністерства соціальної політики України**, фактичний прожитковий мінімум для працездатної особи у квітні 2024 року становив близько **8 500 грн**, тоді як **офіційно встановлений прожитковий мінімум** у Державному бюджеті залишається на рівні **3 204 грн**, що **в понад два рази менше** за реальні витрати громадян на мінімально необхідний рівень життя.

Більше того, розрахунки профспілкових організацій, проведені з урахуванням чинного **податку на доходи фізичних осіб (ПДФО)**, демонструють, що **реальний післяподатковий прожитковий мінімум** для працездатної особи в 2024 році має становити не менше **9 300 грн**, щоб забезпечити фізіологічне виживання, оплату житла, транспорту, медикаментів, одягу, а також мінімальні потреби в освіті та культурі.

Цей системний дисбаланс між **нормативними гарантіями** та **фактичними економічними реаліями**:

- нівелює стимулюючу функцію мінімальної заробітної плати;
- посилює **тінізацію трудових відносин**;
- підвищує **міграційні настрої серед молоді та фахівців**;
- унеможливлює побудову ефективної системи **мотивації та утримання персоналу** на підприємствах.

У цьому контексті постає **необхідність перегляду системи управління персоналом** з урахуванням ринкових чинників, воєнного часу, гнучкості зайнятості, актуалізації підходів до оцінки праці, а також реального прожиткового мінімуму як базового індикатора справедливості в оплаті праці.

Рекомендовано:

- законодавчо прив'язати мінімальну зарплату до фактичного прожиткового мінімуму, розрахованого на незалежній основі;
- посилити роль колективних договорів і галузевих угод у формуванні систем винагород;
- впроваджувати адаптивні HR-стратегії, орієнтовані на **утримання персоналу в умовах дефіциту кадрів** та демографічного скорочення.

Таким чином, **реальне оновлення трудових та соціальних стандартів** є не лише соціальним імперативом, а й ключовим фактором збереження людського капіталу та економічної безпеки держави.

Управління персоналом багатогранний і виключно складний процес, який має свої специфічні властивості і закономірності, він повинен набути системного характеру і завершеності на основі комплексного вирішення кадрових проблем, впровадження нових і вдосконалення існуючих форм і методів роботи. Особливий інтерес становить дослідження оплати праці як фактора становлення та розвитку ринку праці в Україні. Розвиток цього ринку в країні супроводжується постійною зміною ролі його окремих елементів: пропозиції, попиту на робочу силу, розміру заробітної плати.

По-перше, величина зарплати стає найважливішою складовою мотивації працівників до участі трудовій діяльності, що оплачується. При переході до ринкової системи господарювання патерналістична поведінка держави, як і в попередні періоди полягає у наданні послуг освіти, житла, охорони здоров'я, певних інших послуг безоплатно чи на пільговій основі, стала слабшати. Надання цих благ на платній основі робить заробітну платню суттєвим чинником на ринку пропозиції праці.

По-друге, в умовах повної самоокупності підприємствами витрат на оплату праці їх величина починає відігравати суттєву роль у регулюванні попиту на працю.

Рівень та динаміка витрат на робочу силу є важливими факторами конкуренції в країні та за її межами, а також в міжнародній торгівлі. В світовій практиці така інформація також використовується при ведені колективних переговорів між соціальними партнерами: профспілками та працедавцями. Необхідність зі збирання країнами вказаної інформації не рідше ніж раз на п’ять років закріплено Конвенцією про статистику праці № 160, прийнятою Генеральною конференцією Міжнародної організації праці у 1985 р. У 1991 р. ця Конвенція була ратифікована Україною. Починаючи з 2007 р. обстеження витрат на робочу силу в Україні виконується вибірковим методом.

В умовах **воєнного стану та трансформації ринку праці** внаслідок повномасштабної агресії Росії проти України, динаміка витрат на робочу силу зазнала істотних змін. За оцінками Державної служби статистики України, у 2023 році середні витрати на одного найманого працівника становили понад 23 000 грн на місяць, включаючи заробітну плату, внески до соціальних фондів, премії, надбавки та інші витрати, пов’язані з персоналом. З огляду на інфляційний тиск, зростання цін на енергоносії, часткову втрату ринків і нестачу кваліфікованих кадрів, у 2024 році підприємства змушені переглядати структуру витрат на персонал – у бік збільшення гнучких форм оплати праці, індексацій, дистанційної роботи й

залучення внутрішньо переміщених осіб. Особливого значення набуває контроль за динамікою реальних витрат на робочу силу, що дозволяє не лише оцінювати конкурентоспроможність підприємств, а й формувати обґрунтовану державну політику у сфері праці та зайнятості. У 2024 році Україна активно адаптує **статистику праці до вимог ЄС**, у тому числі в контексті гармонізації з Регламентом Європейського парламенту щодо структури заробітної плати (Structure of Earnings Survey, SES), що є передумовою для **відкриття європейського ринку праці для українських компаній** та забезпечення соціальної справедливості всередині країни.

Безумовно, заробітна плата – це відображення властивостей системи кадрової захищеності, характерне для її цілей і особливостей стимуляції їх досягнення, а також політики держави щодо регулювання економічних відносин. В умовах планової економіки орієнтирами для підприємств були неякісні, а кількісні показники діяльності. У ринкових відносинах, в умовах гострої конкурентної боротьби з метою виживання підприємств доцільно виробляти продукцію такої якості, якої вимагає ринок. Необхідно працювати, орієнтуючись не на кількість, а на якість, яка забезпечить конкурентоспроможність продукції, тому слід знайти стимулятори праці, які дають можливість поєднувати інтереси підприємства і працівника, підвищити його зацікавленість у досягненні високих загальних і індивідуальних результатів. Ефективність управління кадровою безпекою – це систематичний, чітко формалізований процес, спрямований на вимірювання витрат і вигод, пов'язаних з програмами діяльності менеджменту персоналу і для співвіднесення її результатів з підсумками базового періоду, з показниками конкурентів і метою підприємства.

Для вирішення цих питань система стимулювання повинна бути побудована так, щоб кожнен працівник прагнув до реалізації головної мети підприємства – виготовляти та реалізовувати продукцію з максимальною ефективністю, як для виробника, так і для кожного працівника. Оцінювання ефективності управління захищеністю персоналу тісно пов'язано з усіма етапами процесу менеджменту та своїми результатами здатне спонукати керівника вносити необхідні корективи. При цьому оцінювання забезпечує функціонування на підприємстві безперебійного зворотного зв'язку і виступає потужним важелем зростання результативності управлінського процесу.

Важливою складовою є омпоненти політик конфіденційності (рис. 9.5):

Рисунок 9.5 – Основні компоненти політик конфіденційності

Зазначені властивості персоналу та й загалом його роль у побудові економічної безпеки підприємства потребують створення відповідної моделі системи функціонування кадрової безпеки. Методичне обґрунтування кадрової безпеки може частково розв'язати проблему в частині її теоретичного забезпечення. При створенні системи оптимального забезпечення кадрової безпеки підприємства доцільно спиратись на оптимальну елементну структуру, яка б уможливила найбільш ефективне її використання, а отже забезпечила б відповідний рівень захисту усіх об'єктів, знаходячись при цьому в динамічному розвитку.

Політики лояльності персоналу

Значення лояльності

Лояльні співробітники менше схильні до порушення політик конфіденційності та умисних дій, які можуть завдати шкоди підприємству. Формування політики лояльності персоналу як фактор економічної безпеки підприємства подано на рисунку 9.6.

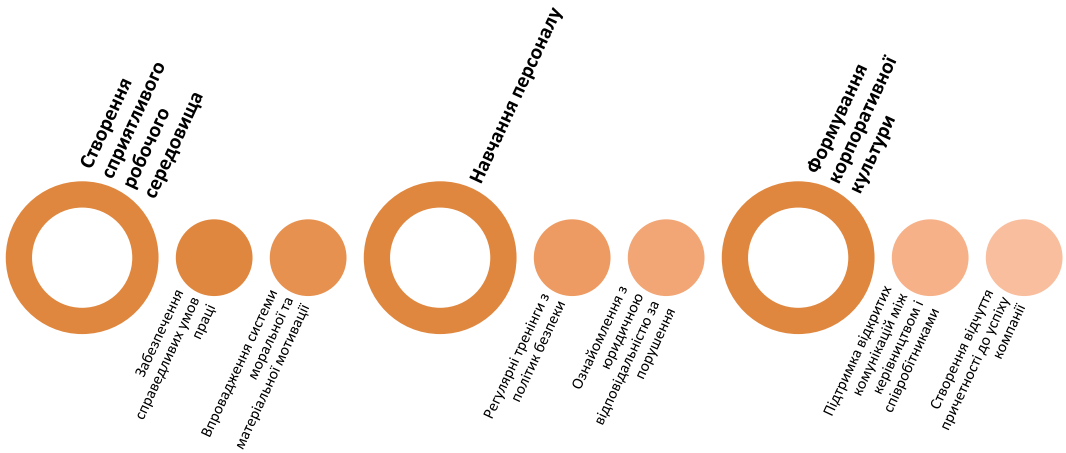

Рисунок 9.6 – Формування політики лояльності персоналу як фактор ЕБП

Впровадження політик конфіденційності та лояльності має низку суттєвих переваг (табл. 9.5):

Таблиця 9.5 – Переваги впровадження політик конфіденційності та лояльності

Переваги	Опис
Зниження ризиків витоків даних	Ефективна регламентація роботи з інформацією мінімізує можливість несанкціонованого доступу.
Підвищення довіри клієнтів	Захист даних клієнтів створює позитивний імідж компанії.
Формування позитивного клімату	Лояльний персонал підтримує стабільність і розвиток компанії.

Етапи створення політики конфеденційності та стратегії підвищення лояльності персоналу нерозривно пов'язані та йдуть паралельними процесами (рис. 9.7):

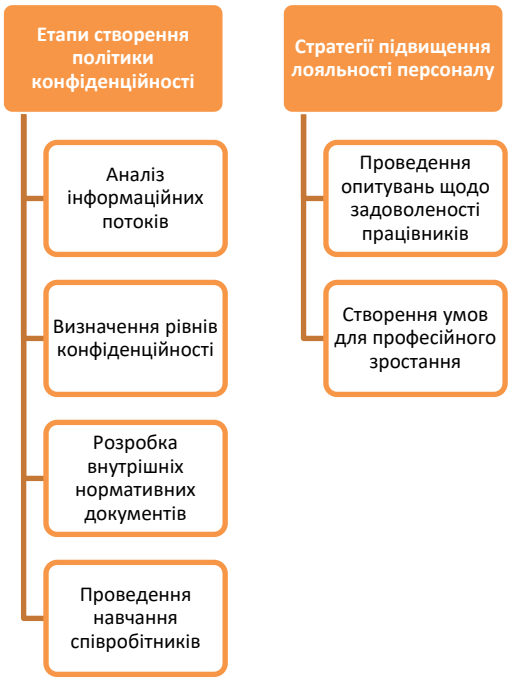

Рисунок 9.7 – Політики лояльності персоналу

При цьому увага має бути сконцентрована на трьох основних складових (рис. 9.8)

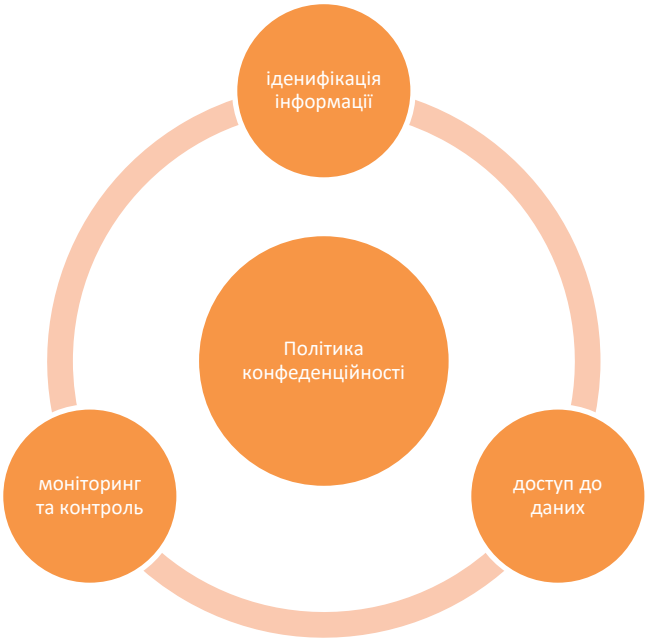

Рисунок 9.8 – Компоненти політики конфіденційності

Впровадження політик конфіденційності та лояльності:

- Забезпечує збереження інформації.
- Знижує ризики, пов’язані з людським фактором.
- Сприяє сталому розвитку компанії завдяки підтримці лояльного персоналу.

Політики конфіденційності та лояльності персоналу є ключовими елементами управління економічною безпекою підприємства. Вони сприяють зниженню ризиків, пов’язаних із людським фактором, і підвищують ефективність роботи компанії.

9.4 Навчання та підвищення кваліфікації у сфері безпеки

Сутність навчання у сфері безпеки

Навчання та підвищення кваліфікації співробітників у сфері безпеки — це важливий інструмент управління людським капіталом, спрямований на мінімізацію ризиків, підвищення професійної компетентності та формування культури безпеки на підприємстві.

Щоб оцінити, наскільки ефективна та чи інша система управління безпекою персоналу, потрібні певні критерії до її аналізу. Їх вибір залежить від того, що брати за точку відліку: діяльність конкретно взятого керівника, трудові показники колективу або особисті якості виконавців.

Аналіз публікацій в цій площині дозволяє виділити **дві основні концепції**, покладені в основу оцінювання ефективності управління захищеністю персоналу:

– відповідно до першої з них, ефективність управління оцінюється виходячи з органічної єдності менеджменту та виробництва, але при цьому внесок власне управління захищеністю персоналу в ефективності виробництва не виокремлюється;

– друга концепція акцентує увагу на визначенні внеску управління захищеністю персоналу в ефективність виробництва.

Кількісне оцінювання цього внеску є надзвичайно складним, оскільки відповідних звітних показників на сьогодні не сформовано. Тому більшість методик оцінювання ефективності управління захищеністю персоналу дотримується першого підходу. При цьому є доцільним оцінювати не стільки внесок управління захищеністю персоналу в ефективності виробництва, скільки якісний вплив його на цю ефективність.

Оцінювання ефективності управління захищеністю персоналу багато вчених-економістів, в тому числі Шекшня С.В., пропонують здійснювати в кілька етапів:

а) оцінювання досягнення цілей;
б) оцінювання компетенції;
в) оцінювання мотивації;
г) вивчення статистики людських ресурсів;
д) оцінювання витрат.

Варто відзначити, що оцінювання ефективності управління захищеністю персоналу здійснюється, здебільшого, суб'єктивно.

Це відбувається з двох причин: відсутність виробленої чіткої методики такого оцінювання і нерозуміння усієї важливості цього процесу. Основний наголос робиться на оцінювання продуктивності, такий підхід є у Д.С. Синка, проте він не акцентує уваги на «людському чиннику».

Ефективність функціонування системи управління захищеністю персоналу має визначатись її внеском у досягненні організаційних цілей. Управління захищеністю персоналу є ефективним настільки, наскільки успішно персонал підприємства використовує свій потенціал для реалізації цілей, що стоять перед ним. Так, справжнім критерієм її оцінювання слугує кінцевий результат праці всього колективу, в якому органічно поєднані результати праці та керівника і виконавців.

Що стосується конкретних **методів оцінювання продуктивності праці з метою дослідження захищеності бізнесових інтересів**, то їх доцільно розділити на три групи:

– кількісні – бальний, коефіцієнтний, метод рангового порядку, метод парних порівнянь, система графічного профілю, метод «експерименту» та ін.;
– якісні (або описові) – система усних і письмових характеристик, метод еталону, матричний і біографічний методи, метод групової дискусії;
– комбіновані (або проміжні) - метод стимулюючих оцінювань, угрупування працівників, тестування.

Найбільшого поширення набули кількісні методи оцінювання продуктивності праці, особливо бальний, коефіцієнтний та бально-коефіцієнтний. Їх перевагами є об'єктивність, незалежність ставлення експертів до фахівця, можливість формалізації результатів, порівняння параметрів, систематизації результатів і використання економіко-математичних методів.

Враховуючи особливості сучасного розвитку української економіки, високий рівень кадрової захищеності можна досягти, використовуючи сучасні напрацювання, коли навіть незначне прогресивне збільшення заробітної плати матиме стимулюючий характер.

Система матеріального стимулювання має сприяти підвищенню ефективності діяльності підприємства, оскільки кошти від зниження собівартості продукції які не використовуються на стимулювання, можуть бути спрямовані, зокрема, на освоєння і розробку нових видів продукції. Якщо такої необхідності немає, то отримана економія стане джерелом збільшення прибутку, або на цю величину можна зменшити ціну продукції, що є одним із способів підвищення її конкурентоспроможності. Для підвищення дієздатності механізму матеріального стимулювання праці необхідно також удосконалити систему формування фонду оплати праці. Вирішити можна, створивши на підприємстві механізм формування та розподілу коштів на оплату праці, який буде збільшувати внесок кожного працівника підрозділу в кінцеві результати діяльності підприємства. Такий підхід до формування та розподілу коштів на оплату праці можна пропонувати підприємствам, які застосовують традиційний тарифні системи, або використовують на підставі розглянутої багаторівневої тарифної системи.

Слід зазначити, що формування фонду оплати має відбуватися не згори вниз, як це було за часів планової економіки, коли централізовано визначалися величина фонду оплати праці та основні елементи організації праці – тарифні умови, норми праці, форми, а системи заробітної плати «підбудовувалися» під даний фонд знизу вгору, тобто від індивідуальних заробітних плат до загального розміру фонду. Тоді фонд оплати праці буде відображати сумарні витрати підприємства на оплату праці в собівартості продукції. Причому власник підприємства буде вирішувати, які кошти він може виділити на оплату праці, враховуючи вартість робочої сили на ринку праці, необхідність забезпечення конкурентоспроможності продукції на ринку товарів (послуг), рівень інфляції, державні, галузеві (регіональні) гарантії за відношенням до оплати праці та інші фактори.

У низці європейських країн набули поширення так звані центри оцінювання управлінського персоналу. Діяльність таких центрів полягає у виявленні за допомогою експертів і на підставі спеціального комплексу тестів і вправ потенційних здібностей працівників управління. Центри оцінювання можуть допомогти як просуванню управляючих працівників, так і підвищенню їх кваліфікації.

Удосконалення оплати праці сприяє:

- посиленню стимулюючої ролі заробітної плати у розвитку ринкової економіки і відповідно підвищенню трудового потенціалу як окремо взятого працівника, так і персоналу в цілому;
- пожвавленню платоспроможного попиту населення та підвищенню його інвестиційної активності;
- легалізації всіх видів трудових доходів; встановленню рівноважної ціни робочої сили, що відповідає витратам на її відтворення, попит і пропозиція на ринку праці;
- збільшення податкових надходжень і зменшенню навантаження на бюджети всіх рівнів;

– зниження масштабів бідності серед працездатного населення, створення стійкого суспільного укладу життя.

Говорячи про ефективність захищеності персоналу, не можна не сказати про оцінювання роботи служби управління персоналом, оскільки саме на неї покладено функції підбору кадрів, що має відповідати вимогам сучасності, а саме: мають відповідну освіту і професійні знання, гнучкий розум і практичну кмітливість, достатній стаж роботи на більш низькій посаді, знайомі з передовим вітчизняним і зарубіжним досвідом підприємництва і комерційної діяльності, тощо.

Ефективне управління захищеністю багато в чому визначається особистісними та професійними якостями безпосередньо самого керівника підприємства, ступенем усвідомлення ним доцільності вчитися самому і сприяти навчанню інших, щоб відповідно реагувати на сучасні динамічні соціально-економічні процеси.

Підвищення продуктивності функціонування системи економічної захищеності багато в чому зумовлене кардинальними зрушеннями структурного та кваліфікаційного характеру в роботі персоналу, діяльність якого передбачає наявність високого рівня інтелектуалізації, а також створює умови для гуманізації роботи. Для того, щоб дати об'єктивну оцінку функціонування системи захищеності персоналу з погляду її ефективності, вкрай важливим є системний розвиток теоретичних підходів та шляхів встановлення соціально-економічної доцільності новацій.

Зазвичай, продуктивність заходів із забезпечення економічної захищеності вважають отримання максимально допустимих показників економічного поступу шляхом створення сприятливих умов для якомога ширшої зайнятості працівників, надання їм можливості для формування високоефективної трудової діяльності, підвищення науково-освітнього та соціально-культурного статусу внаслідок застосування сучасних підходів, а також інтелектуалізації та гуманізації професійної діяльності.

Питання, пов'язані із забезпеченням захищеності персоналу, а також його вірогідним впливом на інтенсивність виробничої діяльності, розглянуто багатьма вітчизняними та зарубіжними науковцями, де проблема обґрунтування механізмів формування українського ринкового простору в контексті праці базується на окресленні теоретично-методичних засад у площині інноваційної природи щодо якості розвитку суспільства. Слід зазначити, що у наявних дослідженнях широко представлено основні методи, а також висвітлено витрати, пов'язані зі створенням робочого місця для однієї особи, розкрито демографічні чинники праці, скорочення кількості безробітних, викладено теоретичне підґрунтя інвестицій у формуванні трудових ресурсів. Водночас методологія з питань розвитку теорії економічної захищеності персоналу в даному векторі потребує нагального вдосконалення.

Продуктивну діяльність суб'єкта господарювання характеризує, зазвичай, рівень розвитку економічної захищеності персоналу. Зважаючи на динамічність сучасного середовища та прискорення старіння попередніх наукових здобутків, актуальних колись практичних напрацювань, кожен товаровиробник має постійно збагачувати накопичені знання персоналу, покращувати його якісні характеристики з метою посилення

конкурентних переваг промислового підприємства в ринкових умовах, і відповідно стабілізувати роботу суб'єкта господарювання в цілому та його співробітників зокрема.

Таким чином ми отримуємо цілі навчання у сфері безпеки

1. **Зменшення ризиків людського фактора:** попередження помилок і недбалості співробітників.
2. **Формування культури безпеки:** забезпечення відповідальності за дотримання політик і стандартів безпеки.
3. **Підвищення ефективності:** здатність ідентифікувати та реагувати на загрози.
4. **Адаптація до сучасних викликів:** розуміння нових типів загроз, таких як кібератаки, витоки інформації тощо.

Основні напрямки навчання

1. **Навчання з кібербезпеки**
   - Ознайомлення з основами кіберзахисту.
   - Використання сучасних інструментів захисту інформації (шифрування, двофакторна аутентифікація).
   - Навчання виявленню фішингових атак.
2. **Навчання з управління ризиками**
   - Оцінка ймовірності ризиків.
   - Розробка планів реагування на інциденти.
   - Мінімізація наслідків кризових ситуацій.
3. **Спеціалізовані тренінги**
   - Тренінги з безпечної роботи з конфіденційною інформацією.
   - Ознайомлення з законодавчими нормами у сфері економічної безпеки.
   - Вивчення міжнародних стандартів управління безпекою (ISO 27001, NIST).
4. **Лідерські програми**
   - Навчання менеджерів управління безпекою.
   - Формування навичок управління кризами.

Етапи навчання

1. **Аналіз потреб у навчанні**
   - Оцінка рівня знань співробітників.
   - Визначення пріоритетних напрямків навчання.
2. **Розробка навчальних програм**
   - Врахування специфіки діяльності підприємства.
   - Використання реальних кейсів і прикладів.
3. **Проведення навчання**
   - Лекції, тренінги, семінари.
   - Інтерактивні методи (симуляції, рольові ігри).
4. **Оцінка результатів**
   - Проведення тестування після завершення курсу.
   - Аналіз впливу навчання на ефективність роботи.

Таблиця 9.6 – Переваги навчання у сфері безпеки

Перевага	Опис
Зниження ризиків	Навчання співробітників допомагає уникнути людських помилок.
Підвищення продуктивності	Кваліфіковані співробітники працюють ефективніше.
Адаптація до змін	Співробітники готові до сучасних викликів і ризиків.
Формування корпоративної культури	Підтримка відповідальності та командної роботи.

Практичне значення

Інвестиції у навчання та підвищення кваліфікації співробітників:

- зменшують ризики, пов'язані з людським фактором;
- сприяють розвитку компетенцій і професійного зростання;
- підвищують рівень економічної безпеки підприємства.

Навчання та підвищення кваліфікації у сфері безпеки є ключовим елементом у мінімізації ризиків і забезпеченні стабільної роботи підприємства. Впровадження систематичних навчальних програм формує кваліфікований і відповідальний персонал, готовий до сучасних викликів.

Перелік питань:

1. Що таке людський фактор, і як він впливає на економічну безпеку підприємства?
2. Які позитивні та негативні аспекти впливу людського фактора ви можете виділити?
3. Що таке кадрові ризики, і як вони класифікуються?
4. Які поведінкові ризики можуть виникнути у співробітників підприємства?
5. Як високий рівень плинності кадрів впливає на економічну безпеку?
6. Які організаційні заходи спрямовані на мінімізацію кадрових ризиків?
7. Що включає в себе політика конфіденційності на підприємстві?
8. Як угоди про нерозголошення (NDA) допомагають захистити інформацію?
9. У чому полягає значення лояльності персоналу для економічної безпеки?
10. Які методи використовуються для підвищення лояльності персоналу?
11. Як психологічний комфорт на робочому місці впливає на економічну безпеку?
12. Які технічні заходи допомагають знизити вплив людського фактора?
13. Як побудувати ефективну систему навчання персоналу у сфері безпеки?
14. У чому полягає значення корпоративної культури для економічної безпеки?
15. Які аспекти включає навчання з кібербезпеки для співробітників?
16. Як можна оцінити потреби підприємства в навчанні персоналу?
17. Які тренінги необхідно проводити для управління ризиками на підприємстві?
18. Як оцінити ефективність навчальних програм з безпеки?
19. У чому полягає значення лідерських програм у забезпеченні економічної безпеки?
20. Які основні кроки впровадження систематичного навчання у сфері безпеки?

Тести:

1. **Що є основною метою управління персоналом у контексті економічної безпеки?**
   а) зниження витрат на навчання персоналу;
   б) формування корпоративної культури;
   в) забезпечення збереження конфіденційної інформації;
   г) створення нових робочих місць.

2. **Який із наведених ризиків належить до поведінкових ризиків?**
   а) використання ненадійних паролів;
   б) конфлікт між працівниками;
   в) висока плинність кадрів;
   г) недостатня кількість фахівців.

3. **Що включає політика конфіденційності на підприємстві?**
   а) контроль за використанням конфіденційної інформації;
   б) регулювання робочого часу працівників;
   в) проведення регулярних тренінгів із кібербезпеки;
   г) підписання трудових договорів.

4. **Що таке угода про нерозголошення (NDA)?**
   а) документ, що регулює заробітну плату співробітників;
   б) договір про конфіденційність інформації;
   в) угода про передачу прав на інтелектуальну власність;
   г) договір про спільне використання ресурсів.

5. **Як можна знизити ризик витоку інформації через людський фактор?**
   а) зменшити обсяг документів на підприємстві;
   б) забезпечити регулярний моніторинг діяльності співробітників;
   в) використовувати недорогі технічні засоби захисту;
   г) заборонити доступ до електронної пошти.
6. **Який із наведених аспектів є ключовим для формування лояльності персоналу?**
   а) підвищення зарплат;
   б) проведення регулярних звітів керівництва;
   в) забезпечення психологічного комфорту на робочому місці;
   г) обмеження доступу до конфіденційної інформації.

7. **Який із наведених ризиків належить до організаційних?**
   а) низька кваліфікація співробітників;
   б) недостатня кількість кваліфікованих працівників;
   в) використання ненадійних паролів;
   г) невмотивованість працівників.

8. **Що є основною метою навчання персоналу у сфері безпеки?**
   а) підвищення рівня плинності кадрів;
   б) формування корпоративної культури;
   в) зниження впливу людського фактора на ризики безпеки;
   г) зменшення витрат на технологічні засоби захисту.

9. **Який метод є найбільш ефективним для мінімізації поведінкових ризиків?**
   а) проведення тренінгів із кібербезпеки;
   б) запровадження багатофакторної аутентифікації;
   в) забезпечення справедливих умов праці;
   г) підписання NDA із кожним працівником.

10. **Що є головним завданням програм лідерського навчання?**
    а) зниження витрат на навчання персоналу;
    б) формування навичок управління кризовими ситуаціями;
    в) підвищення заробітної плати менеджерів;
    г) створення додаткових робочих місць.

11. **Що включає оцінка потреб підприємства в навчанні персоналу?**
    а) аналіз потреб співробітників у відпочинку;
    б) аналіз рівня знань співробітників у сфері безпеки;
    в) перевірка рівня задоволеності працівників;
    г) оцінка витрат на навчання.

12. **Що є основним компонентом політики конфіденційності?**
    а) зменшення обсягу інформації у звітах;
    б) забезпечення доступу до всіх даних для всіх співробітників;
    в) розподіл інформації за рівнями доступу;
    г) проведення тренінгів з використання обладнання.

13. **Як можна мінімізувати комунікаційні ризики на підприємстві?**
    а) заборонити співробітникам використовувати електронну пошту;
    б) запровадити відкритий діалог між керівництвом і співробітниками;
    в) збільшити кількість звітів;
    г) використовувати автоматизовані системи управління.

14. **Що є ключовим завданням навчальних програм із кібербезпеки?**
    а) формування навичок розпізнавання загроз і реагування на них;
    б) підвищення рівня довіри клієнтів;
    в) зниження витрат на технічне обладнання;
    г) оцінка фінансової стабільності компанії;

15. **Який із методів є найбільш ефективним для підвищення лояльності співробітників?**
    а) забезпечення регулярних тренінгів із кібербезпеки;
    б) формування справедливих умов праці;
    в) збільшення кількості звітів;
    г) введення системи моніторингу;

Практичні завдання:

Завдання 1. Аналіз людського фактора

Мета: Визначити позитивний і негативний вплив людського фактора на економічну безпеку.

1. Проаналізуйте наведені ситуації:
   - Співробітник випадково відправив конфіденційний звіт не тому адресатові.
   - Група працівників запропонувала нову ідею для оптимізації процесу.
2. Визначте:
   - Які ризики та можливості створює людський фактор у цих прикладах?
   - Як можна мінімізувати ризики?
3. Запропонуйте заходи для зниження негативного впливу людського фактора.

Завдання 2. Оцінка кадрових ризиків

Мета: Навчитися виявляти та оцінювати кадрові ризики на підприємстві.

1. Оцініть наведені кадрові ризики:
   - Висока плинність кадрів.
   - Недостатня кваліфікація співробітників.
   - Конфлікти між працівниками.
2. Заповніть таблицю оцінки ризиків:

Ризик	Ймовірність виникнення (висока/середня/низька)	Можливі наслідки	Рівень ризику
Висока плинність кадрів			
Недостатня кваліфікація			
Конфлікти між працівниками			

3. Запропонуйте стратегії для мінімізації кожного ризику.

Завдання 3. Розробка політики конфіденційності

Мета: Створити базову політику конфіденційності для захисту інформації на підприємстві.

1. Визначте:
   - Які дані на підприємстві слід вважати конфіденційними?
   - Як потрібно регулювати доступ до цієї інформації?
2. Напишіть основні положення політики конфіденційності, що включатимуть:

- Вимоги до співробітників.
- Механізми захисту інформації.
- Санкції за порушення.

3. Представте політику у вигляді структурованого документа.

Завдання 4. План підвищення лояльності персоналу

Мета: Розробити план заходів для підвищення лояльності співробітників.

1. Проаналізуйте поточний стан лояльності персоналу на підприємстві:
   - Що може знижувати мотивацію співробітників?
   - Які існують конфліктні моменти?
2. Розробіть план заходів, який включатиме:
   - Матеріальні стимули (премії, соціальні пільги).
   - Нематеріальні стимули (професійний розвиток, комфортні умови праці).
3. Опишіть очікувані результати впровадження цього плану.

Завдання 5. Проведення навчання у сфері безпеки

Мета: Сформувати програму навчання для підвищення обізнаності персоналу у сфері безпеки.

1. Розробіть навчальну програму, що включає такі теми:
   - Основи кібербезпеки.
   - Методи захисту конфіденційної інформації.
   - Правила роботи з критичною інформацією.
2. Вкажіть:
   - Формат навчання (тренінги, семінари, онлайн-курси).
   - Тривалість і періодичність навчання.
3. Запропонуйте методи оцінки ефективності програми (тестування, практичні завдання).

Завдання 6. Виявлення та управління конфліктами

Мета: Навчитися ідентифікувати конфлікти в команді та ефективно ними управляти.

1. Оцініть приклади конфліктних ситуацій:
   - Працівник відмовляється виконувати нові обов’язки.
   - Конфлікт між відділами через розподіл ресурсів.
2. Запропонуйте методи вирішення кожної ситуації, зокрема:
   - Посередництво керівника.
   - Тренінги з комунікації.
3. Опишіть, як запобігти подібним конфліктам у майбутньому.

ТЕМА 10. ВНУТРІШНІЙ КОНТРОЛЬ ТА АУДИТ У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

10.1 Роль внутрішнього контролю та аудиту.
10.2 Процедури аудиту економічної безпеки.
10.3 Виявлення та запобігання шахрайству.
10.4 Моніторинг ефективності заходів безпеки.

10.1 Роль внутрішнього контролю та аудиту

Сутність внутрішнього контролю та аудиту

Внутрішній контроль та аудит є ключовими елементами системи економічної безпеки підприємства (рис. 10.1), які забезпечують ефективність управління ризиками, захист активів, дотримання законодавчих вимог та досягнення стратегічних цілей компанії (табл. 10.1).

Рисунок 10.1 – Сутність внутрішнього контролю та аудиту

Таблиця 10.1 – Взаємозв'язок внутрішнього контролю та аудиту

Показник	Внутрішній контроль	Внутрішній аудит
Мета	Забезпечення дотримання політик і процедур	Оцінка ефективності системи контролю
Характер діяльності	Постійна діяльність	Періодична діяльність
Основні завдання	Запобігання порушенням	Виявлення недоліків і ризиків
Інструменти	Автоматизовані системи, звітність	Аудиторські звіти, рекомендації

Ключові функції внутрішнього контролю та аудиту

1. **Контроль ефективності бізнес-процесів**
   - Аналіз дотримання стандартів і політик.
   - Виявлення надлишкових або неефективних операцій.
2. **Захист активів**
   - Контроль за збереженням матеріальних і нематеріальних активів.
   - Виявлення та запобігання шахрайству.
3. **Забезпечення достовірності інформації**
   - Перевірка правильності бухгалтерських даних і фінансової звітності.
   - Оцінка адекватності звітів для ухвалення управлінських рішень.

Основні функції внутрішнього контролю та аудиту на підприємстві зазвичай мають такий вигляд (рис. 10.2):

Рисунок 10.2 – Основні функції внутрішнього контролю та аудиту

Роль внутрішнього контролю та аудиту у системі економічної безпеки важко переоцінити. Вони допомагають підприємствам:

- вчасно виявляти та усувати недоліки;
- забезпечувати відповідність бізнесу стратегічним цілям і нормативним вимогам;
- захищати активи від зовнішніх і внутрішніх загроз.

Таким чином внутрішній контроль та аудит є фундаментальними складовими економічної безпеки підприємства. Їх впровадження дозволяє досягти прозорості, ефективності та стабільності бізнес-процесів, мінімізуючи ризики та забезпечуючи сталість компанії у довгостроковій перспективі.

10.2 Процедури аудиту економічної безпеки

Сутність аудиту економічної безпеки

Аудит економічної безпеки – це системний процес перевірки та аналізу механізмів, процедур і заходів, спрямованих на забезпечення стабільності підприємства та запобігання внутрішнім і зовнішнім загрозам. Метою аудиту є оцінка поточного стану економічної безпеки, виявлення слабких місць та розробка рекомендацій для їх усунення.

Етапи проведення аудиту економічної безпеки:

1. **Планування аудиту**
   - **ціль –** визначити обсяги перевірки, ключові напрями аудиту та ресурси, необхідні для його проведення.
   - **дії:**
     - аналіз стратегічних цілей підприємства;
     - ідентифікація можливих ризиків;
     - розробка програми аудиту.
2. **Збір інформації**
   - **ціль –** отримати дані для оцінки стану економічної безпеки.
   - **джерела інформації:**
     - внутрішні документи (фінансова звітність, політики безпеки);
     - інтерв'ю з керівниками підрозділів;
     - спостереження за роботою співробітників.
3. **Аналіз даних**
   - **ціль –** визначити відповідність процедур і механізмів безпеки внутрішнім та зовнішнім стандартам.
   - **методи аналізу:**
     - порівняння з нормативними вимогами;
     - аналіз ризиків і вразливостей;
     - використання спеціалізованого програмного забезпечення для оцінки ефективності.
4. **Виявлення порушень**
   - **ціль –** ідентифікувати слабкі місця, що становлять загрозу економічній безпеці.
   - **приклади порушень:**
     - недотримання політик безпеки;
     - витоки конфіденційної інформації;
     - недоцільне використання фінансових ресурсів.
5. **Розробка рекомендацій**
   - **ціль –** надати пропозиції для усунення виявлених проблем і підвищення рівня безпеки.
   - **типові рекомендації:**
     - посилення контролю за доступом до інформації;
     - оптимізація бізнес-процесів;
     - організація тренінгів для персоналу.

6. **Складання звіту**
   - **ціль –** представити результати аудиту у зрозумілій та структурованій формі.
   - **компоненти звіту:**
     – загальна характеристика стану економічної безпеки;
     – перелік виявлених ризиків і порушень;
     – рекомендації для їх усунення.
7. **Моніторинг виконання рекомендацій**
   - **ціль –** перевірити, чи були впроваджені запропоновані заходи.
   - **методи:**
     – контроль виконання плану дій;
     – проведення повторних перевірок.

Таблиця 10.2 – Основні інструменти аудиту

Інструмент	Опис
SWOT-аналіз	Визначення сильних і слабких сторін, можливостей та загроз.
Ключові показники ефективності	Оцінка відповідності результатів діяльності стратегічним цілям.
Ризик-аналіз	Ідентифікація та оцінка можливих ризиків.
Програмне забезпечення	Використання автоматизованих систем для аналізу великих обсягів даних.

Приклади процедур аудиту економічної безпеки

1. **Аналіз фінансової безпеки:**
   – перевірка обґрунтованості витрат;
   – оцінка платоспроможності підприємства.
2. **Перевірка інформаційної безпеки:**
   – аудит систем доступу до конфіденційної інформації;
   – аналіз захисту електронних баз даних.
3. **Оцінка управління ризиками:**
   – перевірка дотримання процедур ризик-менеджменту;
   – аналіз ефективності системи внутрішнього контролю.

Проведення аудиту економічної безпеки забезпечує:

- своєчасне виявлення порушень і ризиків;
- підвищення ефективності використання ресурсів;
- зміцнення довіри з боку інвесторів і партнерів.

Процедури аудиту є невід’ємною частиною системи економічної безпеки підприємства. Їхнє впровадження дозволяє мінімізувати ризики, забезпечити дотримання законодавчих вимог і підтримувати стабільність у діяльності компанії.

10.3 Виявлення та запобігання шахрайству

Сутність шахрайства та його вплив на економічну безпеку

Шахрайство — це умисні дії, спрямовані на незаконне отримання вигоди, які завдають шкоди підприємству. Воно може бути як внутрішнім (здійснюваним працівниками компанії), так і зовнішнім (з боку партнерів, клієнтів або сторонніх осіб).

Шахрайство створює загрозу для фінансової стабільності, репутації та операційної діяльності підприємства, тому виявлення та запобігання цим діям є ключовим завданням системи економічної безпеки.

Таблиця 10.3 – Основні види шахрайства

Тип шахрайства	Приклади
Фінансове шахрайство	Підробка фінансових документів, махінації з активами.
Інформаційне шахрайство	Несанкціонований доступ до конфіденційних даних, фішинг.
Корпоративне шахрайство	Завищення витрат, фіктивні контракти.
Зовнішнє шахрайство	Махінації з боку клієнтів або постачальників.

Методи виявлення шахрайства

4. **Аналіз даних**
   - Використання спеціалізованого програмного забезпечення для аналізу великих обсягів даних.
   - Виявлення нетипових транзакцій або відхилень у фінансових документах.
5. **Аудит**
   - Проведення регулярних перевірок внутрішніх процесів і операцій.
   - Оцінка відповідності даних у звітах реальним показникам.
6. **Моніторинг поведінки співробітників**
   - Спостереження за нетиповими діями (зміна робочого графіка, доступ до конфіденційних даних без потреби).
   - Використання систем відеоспостереження або аналізу електронної пошти.
7. **Впровадження систем контролю доступу**
   - Розмежування рівнів доступу до інформації.
   - Використання багатофакторної аутентифікації.

Стратегії запобігання шахрайству

8. **Формування корпоративної культури**
   - Розробка кодексу етики, який визначає неприпустимість шахрайських дій.
   - Проведення регулярних тренінгів для персоналу.
9. **Запровадження жорстких політик контролю**
   - Використання чітких інструкцій щодо роботи з фінансами та інформацією.
   - Автоматизація процесів для зниження впливу людського фактора.
10. **Створення системи захисту інформації**
    - Використання шифрування та захисту баз даних.
    - Встановлення систем моніторингу дій співробітників.

11. **Залучення зовнішніх аудиторів**
    - Проведення незалежних перевірок фінансової діяльності та систем безпеки.

Рекомендації з протидії шахрайству

12. **Впровадження автоматизованих систем**
    - Використання програмного забезпечення для аналізу транзакцій та ідентифікації ризиків.
    - Регулярне оновлення систем захисту.
13. **Навчання персоналу**
    - Проведення тренінгів із виявлення шахрайства та фішингових атак.
    - Ознайомлення співробітників із прикладами шахрайських дій.
14. **Забезпечення прозорості**
    - Запровадження системи відкритої звітності.
    - Регулярне інформування керівництва про результати перевірок.

Ефективне виявлення та запобігання шахрайству:

- Захищає фінансову стабільність підприємства.
- Знижує репутаційні ризики.
- Підвищує довіру з боку інвесторів, клієнтів і партнерів.

Виявлення та запобігання шахрайству є ключовим елементом системи економічної безпеки. Впровадження комплексних заходів, що поєднують технічні, організаційні та освітні аспекти, дозволяє мінімізувати ризики шахрайських дій і забезпечити стабільність роботи підприємства.

10.4 Моніторинг ефективності заходів безпеки

Сутність моніторингу ефективності заходів безпеки

Моніторинг ефективності заходів безпеки — це процес регулярного спостереження, аналізу та оцінки ефективності впроваджених заходів, спрямованих на захист активів підприємства, мінімізацію ризиків та забезпечення економічної безпеки.

Головною метою є вчасне виявлення недоліків у системі безпеки та адаптація заходів до нових викликів і загроз.

Основні цілі моніторингу

1. **Оцінка відповідності заходів цілям безпеки**
    - Перевірка того, чи відповідають заходи стратегічним цілям підприємства.
    - Оцінка досягнення ключових показників ефективності (KPI).
2. **Виявлення вразливостей**
    - Аналіз слабких місць у системі безпеки.
    - Розробка планів усунення недоліків.
3. **Адаптація до змін у зовнішньому середовищі**
    - Врахування нових загроз (кіберзлочинність, економічна нестабільність).
    - Постійне оновлення технологій і процесів.

4. **Забезпечення ефективного використання ресурсів**
   - Аналіз витрат на заходи безпеки.
   - Визначення найбільш економічно ефективних рішень.

Етапи моніторингу заходів безпеки

1. **Встановлення цілей та критеріїв оцінки**
   - визначення ключових показників ефективності (наприклад, кількість інцидентів, витрати на захист, час реагування на загрози);
   - визначення очікуваних результатів від впроваджених заходів.
2. **Збір даних**
   - використання автоматизованих систем моніторингу для збору інформації;
   - проведення внутрішніх перевірок і аналітичних досліджень.
3. **Аналіз ефективності**
   - порівняння фактичних результатів із запланованими;
   - виявлення факторів, які знижують ефективність заходів.
4. **Розробка рекомендацій**
   - надання пропозицій щодо вдосконалення заходів безпеки;
   - визначення пріоритетів для розподілу ресурсів.
5. **Звітування**
   - підготовка звіту, який містить результати моніторингу, виявлені проблеми та рекомендації.
6. **Реалізація коригувальних дій**
   - впровадження заходів для усунення недоліків;
   - адаптація стратегії безпеки до нових викликів.

Таблиця 10.4 – Ключові показники ефективності заходів безпеки

Показник	Опис
Кількість інцидентів	Загальна кількість випадків порушення безпеки.
Час реагування на загрозу	Період від виявлення інциденту до його усунення.
Рівень витрат на безпеку	Співвідношення витрат на заходи безпеки до фінансового результату.
Кількість витоків інформації	Кількість випадків розголошення конфіденційних даних.

Методи моніторингу

7. **Використання автоматизованих систем**
   - програмні рішення для моніторингу IT-систем і бізнес-процесів;
   - аналітичні платформи для оцінки ризиків.
8. **Проведення аудитів**
   - регулярні перевірки виконання політик безпеки;
   - аналіз дотримання регуляторних вимог.
9. **Опитування персоналу**
   - оцінка обізнаності співробітників щодо політик безпеки;
   - виявлення слабких місць у корпоративній культурі.

10. **Аналіз статистичних даних**
    - вивчення динаміки інцидентів за певний період;
    - порівняння з середньогалузевими показниками.

Моніторинг ефективності заходів безпеки дозволяє:
- забезпечити прозорість і підзвітність;
- знизити ризики, пов’язані з людським і технічним факторами;
- оптимізувати витрати на безпеку.

Моніторинг ефективності заходів безпеки є невід'ємною частиною управління економічною безпекою. Системний підхід до аналізу результатів допомагає вчасно адаптувати політики, запобігти інцидентам і підвищити стабільність роботи підприємства.

Перелік питань:

1. Що таке внутрішній контроль, і яку роль він відіграє в системі економічної безпеки підприємства?
2. Які основні функції внутрішнього аудиту в контексті забезпечення економічної безпеки?
3. У чому полягає відмінність між внутрішнім контролем і внутрішнім аудитом?
4. Як взаємопов’язані внутрішній контроль та аудит у системі економічної безпеки?
5. Які етапи включає процес проведення аудиту економічної безпеки?
6. Які ключові показники ефективності внутрішнього контролю?
7. Які інструменти використовуються під час проведення аудиту економічної безпеки?
8. У чому полягає значення аналізу даних під час аудиту економічної безпеки?
9. Як моніторинг заходів безпеки допомагає виявляти вразливості системи?
10. Які методи можна використовувати для виявлення шахрайства на підприємстві?
11. У чому полягає важливість розробки рекомендацій після проведення аудиту?
12. Як оцінюється ефективність впроваджених заходів безпеки?
13. Які основні процедури аудиту застосовуються для оцінки фінансової безпеки підприємства?
14. Що таке системи моніторингу, і як вони допомагають у запобіганні шахрайству?
15. Як визначаються критерії оцінки ефективності заходів безпеки?
16. Які основні показники використовуються для моніторингу витрат на безпеку?
17. У чому полягає значення навчання співробітників для підвищення ефективності заходів безпеки?
18. Які основні типи шахрайства можна виділити в системі економічної безпеки?
19. Як впровадження автоматизованих систем впливає на ефективність моніторингу заходів безпеки?
20. У чому полягає роль звітності за результатами аудиту економічної безпеки?

Тести:

1. **Основна мета внутрішнього контролю:**
   а) зменшення витрат на управління підприємством;
   б) забезпечення відповідності діяльності підприємства стандартам і політикам;
   в) формування стратегічного плану розвитку;
   г) аналіз зовнішнього середовища.

2. **Що є ключовою функцією внутрішнього аудиту?**
   а) підготовка фінансової звітності;
   б) оцінка ефективності внутрішніх процедур і ризиків;
   в) управління персоналом;
   г) оптимізація виробничих процесів.

3. **Який із наведених інструментів використовується під час аудиту економічної безпеки?**
   а) аналіз PESTEL;
   б) SWOT-аналіз;
   в) розрахунок ROI;
   г) виробничі показники.

4. **Який із показників найкраще характеризує ефективність внутрішнього контролю?**
   а) час реагування на інциденти;
   б) кількість працівників у відділі контролю;
   в) сума витрат на контроль;
   г) кількість виробленої продукції.

5. **Що є основним етапом процесу аудиту?**
   а) аналіз зовнішнього ринку;
   б) збір та аналіз інформації;
   в) розробка нових політик управління;
   г) зменшення витрат на інфраструктуру.

6. **Який із методів найефективніший для виявлення шахрайства?**
   а) проведення SWOT-аналізу;
   б) застосування автоматизованих систем моніторингу;
   в) оцінка рівня задоволеності клієнтів;
   г) проведення зустрічей із персоналом.
7. **У чому полягає мета моніторингу заходів безпеки?**
   а) аналіз конкурентів;
   б) виявлення слабких місць і адаптація заходів;
   в) зменшення кількості співробітників;
   г) впровадження нових інформаційних систем.
8. **Який із показників є ключовим для моніторингу витрат на безпеку?**

а) загальна сума витрат;
б) співвідношення витрат на безпеку до доходів підприємства;
в) сума витрат на навчання персоналу;
г) кількість витоків інформації.

9. **Що таке ключовий показник ефективності (KPI)?**
а) система фінансової звітності;
б) інструмент вимірювання результативності заходів безпеки;
в) метод розподілу ресурсів підприємства;
г) аналіз конкурентного середовища.

10. **Що є обов'язковим компонентом звіту за результатами аудиту?**
а) інформація про виробничі потужності підприємства;
б) перелік виявлених ризиків і рекомендацій;
в) список нових клієнтів;
г) оцінка рівня задоволеності інвесторів.

11. **Який із підходів дозволяє оцінити рівень ризиків у системі безпеки?**
а) моніторинг поведінки клієнтів;
б) порівняння з галузевими стандартами;
в) аналіз рентабельності;
г) оцінка часу виконання завдань.

12. **Як можна зменшити ризик витоку інформації?**
а) впровадити автоматизовані системи контролю доступу;
б) скоротити кількість працівників;
в) збільшити витрати на маркетинг;
г) зменшити витрати на безпеку.

13. **Що таке система внутрішнього контролю?**
а) набір стандартів для виробництва продукції;
б) система заходів для забезпечення ефективності, достовірності звітності та відповідності законодавству;
в) програма автоматизації операцій;
г) метод аналізу витрат.

14. **Як визначити ефективність впроваджених заходів безпеки?**
а) провести опитування співробітників;
б) зменшити витрати на контроль;
в) виміряти зміну кількості інцидентів;
г) оцінити рівень прибутковості.

Практичні завдання:

Завдання 1. Аналіз системи внутрішнього контролю

Мета: Оцінити ефективність системи внутрішнього контролю на прикладі підприємства.

1. Описати основні елементи системи внутрішнього контролю обраного підприємства: політики та процедури, засоби контролю (технологічні, організаційні).
2. Проаналізувати ефективність внутрішнього контролю за такими критеріями:
   - Чи всі працівники дотримуються політик?
   - Як швидко виявляються недоліки в роботі?
3. Запропонувати три рекомендації для покращення системи внутрішнього контролю.

Завдання 2. Проведення аудиту економічної безпеки

Мета: Провести аудит економічної безпеки підприємства за наданими даними.

1. Використовуючи фінансову звітність підприємства, оцініть:
   - відповідність витрат нормативним показникам;
   - наявність незвичайних транзакцій або відхилень.
2. Складіть таблицю ризиків, яку можна виявити під час аудиту:

Тип ризику	Приклад	Можливий наслідок
Фінансовий		
Інформаційний		

3. Розробіть три рекомендації для усунення виявлених ризиків.

Завдання 3. Виявлення шахрайства

Мета: Ідентифікувати випадки можливого шахрайства та запропонувати заходи для їх запобігання.

1. На основі наведеної ситуації ідентифікуйте шахрайські дії:
   - співробітник завищив вартість придбаного обладнання;
   - здійснювалися транзакції у неробочий час без погодження.
2. Заповніть таблицю:

Вид шахрайства	Методи виявлення	Можливі заходи протидії

3. Розробіть план дій для запобігання подібним випадкам у майбутньому.

Завдання 4. Моніторинг ефективності заходів безпеки

Мета: Оцінити ефективність заходів безпеки на основі зібраних даних.

1. Вивчіть динаміку кількості інцидентів безпеки на підприємстві до і після впровадження нових заходів.
2. Побудуйте графік зміни інцидентів за період (місяць, рік).
3. Заповніть таблицю оцінки ефективності:

Показник	До впровадження заходів	Після впровадження заходів
Кількість інцидентів		
Час реагування (у годинах)		
Рівень витрат на безпеку		

4. На основі аналізу запропонуйте додаткові заходи для підвищення ефективності системи безпеки.

Завдання 5. Розробка політики внутрішнього аудиту

Мета: Розробити основні положення політики внутрішнього аудиту.

1. Опишіть структуру політики, що включатиме:
   - основні принципи (прозорість, об’єктивність, регулярність);
   - ключові процедури аудиту.
2. Розробіть алгоритм дій під час проведення аудиту:
   - підготовчий етап;
   - проведення перевірок;
   - узагальнення результатів.
3. Представте політику у вигляді схеми.

Завдання 6. Розробка ключових показників ефективності (KPI)

Мета: Розробити KPI для моніторингу заходів безпеки.

1. Визначте 5 показників, які можна використовувати для оцінки ефективності заходів безпеки, наприклад, кількість порушень політик безпеки, час реагування на інциденти.
2. Заповніть таблицю:

KPI	Метод розрахунку	Очікуваний результат

3. Поясніть, як обрані KPI впливають на економічну безпеку підприємства.

ТЕМА 11. КОРПОРАТИВНА КУЛЬТУРА ТА ЇЇ ВПЛИВ НА ЕКОНОМІЧНУ БЕЗПЕКУ

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

11.1 Вплив корпоративної культури на безпеку підприємства.
11.2 Формування культури безпеки в організації.
11.3 Етичні стандарти та їх роль у забезпеченні безпеки.
11.4 Приклади впровадження корпоративної культури безпеки.

11.1 Вплив корпоративної культури на безпеку підприємства

Сутність корпоративної культури

Корпоративна культура – це система спільних цінностей, норм, переконань і моделей поведінки, яка формує внутрішню атмосферу підприємства. Вона визначає, як співробітники виконують свої обов'язки, спілкуються та взаємодіють один із одним і з керівництвом. Корпоративна культура є фундаментом, який підтримує стійкість підприємства, зокрема в питаннях економічної безпеки.

Роль корпоративної культури у забезпеченні економічної безпеки

1. **Формування культури відповідальності**
   - Корпоративна культура сприяє розвитку відповідальності серед співробітників, коли кожен працівник розуміє свою роль у збереженні активів і дотриманні стандартів безпеки.
2. **Підвищення лояльності персоналу**
   - Стабільна та позитивна корпоративна культура мотивує співробітників залишатися у компанії, що знижує ризик витоку інформації через недобросовісних працівників.
3. **Протидія внутрішнім загрозам**
   - Ефективна культура мінімізує можливості для шахрайства, конфліктів і недбалості завдяки прозорим правилам та етичним стандартам.
4. **Зміцнення репутації компанії**
   - Підприємство з розвиненою корпоративною культурою викликає довіру серед партнерів, клієнтів і інвесторів, що забезпечує додатковий рівень захисту від зовнішніх ризиків.
5. **Адаптація до змін**
   - Команда, згуртована спільними цінностями, здатна швидше адаптуватися до змін у зовнішньому середовищі, зокрема до нових викликів у сфері економічної безпеки.

Таблиця 11.1 – Ключові аспекти впливу корпоративної культури

Аспект	Вплив на економічну безпеку
Етичні стандарти	Запобігають корупції, шахрайству та зловживанням.
Дотримання політик	Гарантують відповідність законодавству та внутрішнім правилам.
Лідерство та довіра	Мотивують співробітників дотримуватися заходів безпеки.
Комунікація	Забезпечує прозорість і своєчасність обміну інформацією.
Інноваційність	Сприяє впровадженню сучасних технологій для захисту активів.

Приклади впливу корпоративної культури

1. **Позитивний приклад:**
   - У компанії запроваджено регулярні тренінги з етики та безпеки. Це допомагає співробітникам краще розуміти, як уникати ризиків, та підвищує їхню обізнаність.
   - Результат: Зменшення випадків шахрайства на 25% протягом року.
2. **Негативний приклад:**
   - Відсутність чітких правил щодо використання конфіденційної інформації.
   - Результат: Витік даних до конкурентів, що спричинило фінансові втрати.

Ключові інструменти зміцнення корпоративної культури для безпеки (рис. 11.1) у розширеному вигляді містить:

1. **Кодекс корпоративної етики –** розробка документа, який визначає стандарти поведінки та відповідальності співробітників.

2. **Система навчання та тренінгів –** проведення регулярних тренінгів із захисту інформації, запобігання шахрайству та кризового управління.

3. **Програми мотивації –** заохочення співробітників за дотримання політик безпеки.

4. **Прозорість управління –** чітке визначення обов’язків і розподіл ролей у системі безпеки.

5. **Впровадження цифрових технологій –** використання автоматизованих систем для моніторингу дотримання політик.

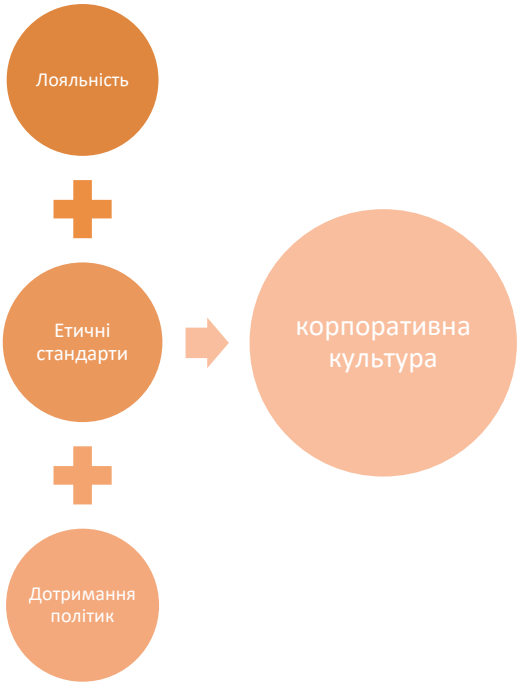

Рисунок 11.1 – Вплив корпоративної культури на економічну безпеку

Приклад розподілу аспектів корпоративної культури у контексті безпеки подано на рисунку 11.2.

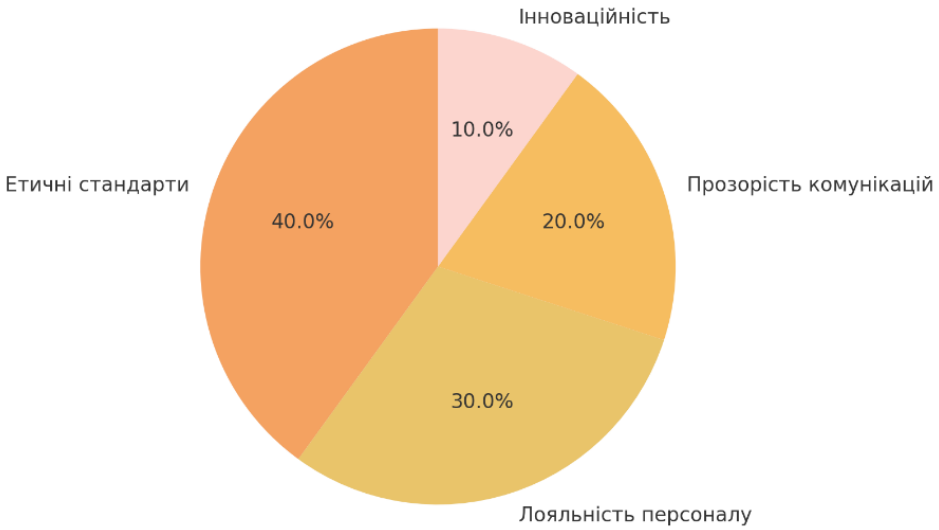

Рисунок 11.2 – Розподіл аспектів корпоративної культури у контексті безпеки

Розвинена корпоративна культура допомагає підприємству:

- Забезпечувати збереження активів.
- Мінімізувати внутрішні та зовнішні ризики.
- Підвищувати довіру співробітників, партнерів та клієнтів.

Корпоративна культура є невід'ємною частиною системи економічної безпеки. Її розвиток сприяє підвищенню ефективності заходів безпеки, формуванню лояльності персоналу та зміцненню репутації підприємства.

11.2 Формування культури безпеки в організації

Що таке культура безпеки?

Культура безпеки — це система цінностей, переконань і моделей поведінки, яка спрямована на захист активів підприємства, запобігання ризикам та забезпечення стабільності. Вона формує розуміння серед співробітників важливості дотримання заходів безпеки як на індивідуальному, так і на організаційному рівнях.

Культура безпеки є основою ефективної системи економічної безпеки, оскільки мінімізує внутрішні загрози та підвищує здатність протидіяти зовнішнім викликам.

Етапи формування культури безпеки

1. **Оцінка поточного стану**
   - проведення аудиту існуючих підходів до безпеки;
   - виявлення слабких місць і прогалин у знаннях співробітників.
2. **Розробка політики безпеки**
   - визначення принципів, цінностей і стандартів, яких повинні дотримуватися всі працівники;
   - підготовка кодексу корпоративної безпеки.
3. **Навчання персоналу**
   - проведення регулярних тренінгів і семінарів щодо ризик-менеджменту, кібербезпеки та етичної поведінки;
   - ознайомлення співробітників із реальними прикладами ризиків і наслідків їх недотримання.
4. **Впровадження системи мотивації**
   - заохочення співробітників, які демонструють відповідальне ставлення до безпеки;
   - запровадження системи премій за виявлення порушень або ініціативи щодо вдосконалення процесів.
5. **Комунікація та прозорість**
   - регулярне інформування працівників про нові політики, стандарти та виявлені ризики;
   - залучення персоналу до розробки заходів безпеки.
6. **Моніторинг і вдосконалення**
   - постійний аналіз ефективності впроваджених заходів;
   - внесення змін до політики безпеки відповідно до нових викликів.

Таблиця 11.2 – Елементи культури безпеки

Елемент	Опис
Освітні програми	Навчання співробітників щодо ризиків і правил безпеки.
Етичні стандарти	Розвиток культури прозорості та відповідальності.
Політики безпеки	Визначення правил та інструкцій щодо захисту активів.
Мотивація співробітників	Заохочення за ініціативність у питаннях безпеки.
Технічна інфраструктура	Використання сучасних технологій для захисту даних і активів.

Приклади успішного впровадження культури безпеки

1. **Компанія А:**
   - Провела аудит внутрішніх процесів і запровадила тренінги з кібербезпеки.
   - Результат: Зменшення витоків інформації на 30% за рік.
2. **Компанія В:**
   - Ввела систему премій за виявлення ризиків у бізнес-процесах.
   - Результат: Підвищення мотивації працівників і своєчасне виявлення загроз.

Роль керівництва у формуванні культури безпеки

1. **Лідерство прикладом**
   - Керівники повинні демонструвати важливість безпеки через власну поведінку.
2. **Забезпечення ресурсів**
   - Інвестиції у навчання, технології та систему моніторингу.
3. **Комунікація**
   - Постійна взаємодія з персоналом для пояснення важливості дотримання заходів безпеки.

Формування культури безпеки допомагає підприємству:

- знижувати рівень внутрішніх і зовнішніх загроз;
- підвищувати довіру співробітників до керівництва;
- забезпечувати стабільність і конкурентоспроможність у довгостроковій перспективі.

Формування культури безпеки – це системний підхід, що потребує залучення всього персоналу, регулярного навчання та впровадження інноваційних рішень. Це не лише підвищує рівень економічної безпеки, а й сприяє успішному розвитку підприємства.

11.3 Етичні стандарти та їх роль у забезпеченні безпеки

Сутність етичних стандартів

Етичні стандарти — це система моральних принципів, норм і правил, які визначають поведінку працівників у межах організації. Вони спрямовані на створення середовища довіри, прозорості та відповідальності, що є основою ефективної системи економічної безпеки.

У сучасному бізнесі етичні стандарти стали невід’ємною частиною корпоративної культури, оскільки вони формують репутацію підприємства, мінімізують ризики та сприяють сталому розвитку.

Роль етичних стандартів у забезпеченні безпеки

1. **Запобігання шахрайству та корупції**
   - чітко визначені етичні принципи створюють умови, за яких працівники уникають недобросовісної поведінки.
   - розробка антикорупційної політики знижує ймовірність внутрішніх загроз.

2. **Формування довіри**
   - етичні стандарти зміцнюють довіру серед співробітників, партнерів та клієнтів.
   - підтримка прозорості в бізнес-процесах сприяє зміцненню репутації.
3. **Поліпшення комунікації**
   - етичні норми забезпечують відкритість у внутрішній комунікації, що дозволяє оперативно виявляти ризики.
4. **Підвищення відповідальності персоналу**
   - співробітники розуміють важливість дотримання стандартів безпеки та відповідально ставляться до своїх обов'язків.
5. **Забезпечення відповідності законодавству**
   - етичні стандарти допомагають уникати юридичних ризиків, забезпечуючи дотримання законодавчих норм і регуляцій.

Таблиця 11.3 – Основні компоненти етичних стандартів

Компонент	Значення для безпеки
Кодекс корпоративної етики	Визначає правила поведінки співробітників у різних ситуаціях.
Прозорість	Сприяє відкритості у взаємодії між підрозділами та з партнерами.
Дотримання законів	Гарантує мінімізацію правових ризиків.
Запобігання конфлікту інтересів	Забезпечує прийняття рішень, які відповідають інтересам підприємства.
Система звітності	Дозволяє вчасно виявляти порушення етичних норм.

Етапи впровадження етичних стандартів

1. **Розробка кодексу етики**
   - визначення ключових цінностей та принципів організації.
   - розробка практичних прикладів застосування етичних норм у повсякденній діяльності.
2. **Навчання співробітників**
   - проведення тренінгів із впровадження етичних стандартів.
   - вивчення реальних кейсів порушення етики та їх наслідків.
3. **Створення механізмів контролю**
   - впровадження системи регулярного моніторингу дотримання етичних стандартів.
   - запуск «гарячої лінії» для повідомлень про порушення.
4. **Система заохочень і санкцій**
   - заохочення співробітників, які дотримуються етичних стандартів.
   - введення санкцій за порушення норм етики.

Вплив етичних стандартів на економічну безпеку

1. **Зниження фінансових втрат**
   - запобігання корупційним схемам і шахрайству зменшує витрати підприємства.

2. **Підвищення конкурентоспроможності**
   - підприємства, що демонструють етичну поведінку, приваблюють більше клієнтів і партнерів.
3. **Зміцнення репутації**
   - дотримання етичних норм створює позитивний імідж, що підвищує довіру серед інвесторів.

Впровадження етичних стандартів дозволяє підприємству:
- підвищити ефективність системи економічної безпеки;
- зміцнити корпоративну культуру та лояльність персоналу;
- забезпечити відповідність законодавчим нормам та зменшити репутаційні ризики.

Етичні стандарти – це важливий інструмент у забезпеченні економічної безпеки підприємства. Їх впровадження сприяє зміцненню довіри, зниженню ризиків і досягненню стабільності в діяльності компанії.

11.4 Приклади впровадження корпоративної культури безпеки

Реальні приклади впровадження корпоративної культури безпеки:

1. **Компанія Google: Створення культури прозорості та захисту інформації**
   - **Особливості:**
     Google активно впроваджує заходи, спрямовані на забезпечення інформаційної безпеки, такі як шифрування даних, багатофакторна аутентифікація та контроль доступу.
     У компанії діє програма «Bug Bounty», яка заохочує співробітників і зовнішніх експертів виявляти вразливості в системах.
   - **Результати:**
     - Значне зниження кількості випадків несанкціонованого доступу до даних.
     - Формування довіри серед клієнтів і партнерів.
   - **Елементи корпоративної культури безпеки:**
     - Чітка політика етики та конфіденційності.
     - Навчання персоналу основам інформаційної безпеки.

2. **Компанія Nestlé: Захист бренду через безпеку ланцюга постачання**
   - **Особливості:**
     Nestlé розробила політики безпеки у сфері постачання, включаючи контроль якості сировини, аудит постачальників і мінімізацію ризиків у ланцюгах поставок.
     Для співробітників проводяться регулярні тренінги з питань етики та прозорості.
   - **Результати:**
     - Зменшення ризику фінансових втрат через підроблену продукцію.
     - Поліпшення репутації компанії на ринку.

- **Елементи корпоративної культури безпеки:**
  - Строгі стандарти безпеки для постачальників.
  - Регулярний моніторинг і аудит.

3. **Компанія IBM: Формування культури кібербезпеки**

   Особливості:

   IBM інвестує значні ресурси у навчання персоналу з кібербезпеки, впроваджує системи моніторингу та реагування на інциденти в реальному часі. У компанії діє принцип «Zero Trust» (нульова довіра), який передбачає ретельну перевірку кожного користувача та пристрою.

- **Результати:**
  - Мінімізація ризику кібератак.
  - Підвищення обізнаності співробітників про сучасні загрози.
- **Елементи корпоративної культури безпеки:**
  - Програми навчання та сертифікації з кібербезпеки.
  - Використання інноваційних технологій для захисту даних.

Гіпотетичні приклади впровадження корпоративної культури безпеки:

1. **Промислове підприємство "Енергія": Захист фізичних активів**
   - **Ситуація:**

     Підприємство стикається з ризиком крадіжок обладнання через слабкі процедури фізичної безпеки.
   - **Рішення:**
     - Встановлення системи відеоспостереження.
     - Введення політики доступу до складів і цехів лише за персональними перепустками.
     - Проведення навчання співробітників щодо виявлення підозрілих дій.
   - **Очікувані результати:**
     - Зменшення випадків крадіжок на 50% протягом року.
     - Збільшення довіри серед працівників.

2. **ІТ-компанія "Діджитал Тех": Створення етичної культури серед працівників**
   - **Ситуація:**

     Через відсутність чітких етичних правил співробітники компанії іноді використовують конфіденційну інформацію в особистих цілях.
   - **Рішення:**
     - Розробка кодексу етики із забороною використання корпоративних даних у власних інтересах.
     - Проведення тренінгів про етичну поведінку на робочому місці.
     - Введення системи звітності про порушення етичних норм.
   - **Очікувані результати:**
     - Зменшення випадків порушень етики на 70%.
     - Зміцнення довіри між керівництвом і персоналом.

Етапи успішного впровадження корпоративної культури безпеки

1. **Аналіз поточної ситуації:**
   - Оцінка рівня обізнаності співробітників про безпеку.
   - Ідентифікація основних ризиків.
2. **Розробка програми культури безпеки:**
   - Створення кодексу етики та політик безпеки.
   - Визначення індикаторів ефективності (KPI).
3. **Навчання персоналу:**
   - Організація тренінгів і семінарів із безпеки.
   - Реальні приклади наслідків порушень безпеки.
4. **Моніторинг і вдосконалення:**
   - Постійний контроль за дотриманням політик.
   - Внесення коректив відповідно до нових викликів.

Приклади впровадження корпоративної культури безпеки демонструють, що правильний підхід може:

- Знизити ризики та фінансові втрати.
- Поліпшити внутрішній клімат в організації.
- Зміцнити позиції підприємства на ринку.

Впровадження корпоративної культури безпеки є стратегічно важливим для підприємств будь-якої галузі. Реальні та гіпотетичні приклади показують, що інвестиції у культуру безпеки завжди окупаються через підвищення стабільності та довіри до компанії.

Як підготувати тренінг для персоналу: покрокова інструкція

Тренінг для персоналу — це один із найефективніших способів підвищення кваліфікації співробітників, зміцнення корпоративної культури та вирішення конкретних бізнес-завдань, наприклад, у сфері економічної безпеки.

Крок 1: Визначення мети та завдань тренінгу

1. **Задайте ціль тренінгу:**
   Наприклад: навчити співробітників розпізнавати ризики шахрайства, підвищити обізнаність про правила безпеки чи ознайомити з новими внутрішніми політиками.
2. **Чітко сформулюйте завдання:**
   - Ознайомлення з політиками безпеки.
   - Формування навичок реагування на інциденти.
   - Розвиток культури прозорості.

Крок 2: Аналіз аудиторії

1. **Оцініть рівень знань:**
   - Проведіть анкетування або опитування для виявлення прогалин у знаннях.
2. **Врахуйте специфіку роботи співробітників:**

- Для ІТ-відділу варто акцентувати увагу на кібербезпеці.
- Для відділу продажів — на запобіганні витоку комерційної інформації.

Крок 3: Розробка програми тренінгу

1. **Структуруйте програму:**
   - **Вступ:** Ознайомлення з метою тренінгу, мотивація учасників.
   - **Теоретична частина:** Пояснення ключових понять, законів чи стандартів.
   - **Практична частина:** Розбір кейсів, інтерактивні вправи, симуляції.
   - **Заключна частина:** Питання, обговорення, зворотний зв'язок.
2. **Приклад структури тренінгу:**
   - **Вступ:** 10 хв.
   - **Теорія:** 30 хв.
   - **Практика** (розбір кейсів): 40 хв.
   - **Підбиття підсумків і тестування:** 20 хв.

Крок 4: Вибір методів навчання

1. **Теоретичні методи:**
   - Лекції з використанням мультимедійних презентацій.
   - Інтерактивні дискусії.
2. **Практичні методи:**
   - **Кейси:** Розгляд реальних чи гіпотетичних ситуацій.
   - **Рольові ігри:** Симуляція кризових ситуацій і рішень.
   - **Групові вправи:** Робота в команді над вирішенням завдань.

Крок 5: Підготовка матеріалів

1. **Презентації:**
   - Використовуйте графіки, схеми, інфографіку.
   - Дотримуйтесь чіткої структури: «Теза → Приклад → Висновок».
2. **Роздаткові матеріали:**
   - Короткий посібник із правилами або політиками.
   - Зразки документів (заяви про інциденти, звіти).
3. **Технічне забезпечення:**
   - Комп’ютери, проектори, доступ до програмного забезпечення, якщо це потрібно для практичної частини.

Крок 6: Проведення тренінгу

1. **Почніть із мотивації:**
   - Розкажіть, як тренінг допоможе учасникам у роботі.
2. **Використовуйте інтерактив:**
   - Задавайте питання, залучайте до обговорення.
3. **Забезпечте зворотний зв’язок:**
   - Учасники можуть ставити питання або пропонувати свої рішення.

Крок 7: Оцінка ефективності

1. **Тестування знань:**
   - Проведіть невелике тестування наприкінці тренінгу для оцінки засвоєного матеріалу.
2. **Анкетування учасників:**
   - Запитайте, що було зрозуміло, а що можна покращити.
3. **Моніторинг практичного впровадження:**
   - Оцініть, як співробітники застосовують знання на практиці через місяць після тренінгу.

Додаткові поради

- **Інклюзивність:** Враховуйте рівень знань і досвіду всіх учасників.
- **Інтерактивність:** Чим більше практичних завдань, тим ефективніший тренінг.
- **Візуалізація:** Використовуйте яскраві графіки, схеми, відео для зацікавлення аудиторії.
- **Реальні приклади:** Пояснюйте теорію через кейси, пов’язані з реальними подіями.

Приклад кейса для тренінгу: Запобігання шахрайству

- **Ситуація:**
  Співробітник фінансового відділу отримує електронного листа від імені директора з проханням терміново переказати кошти на зовнішній рахунок.
- **Завдання для учасників:**
  1. Проаналізуйте ситуацію та визначте потенційні ризики.
  2. Вкажіть, які дії потрібно виконати, щоб уникнути шахрайства.
  3. Розробіть протокол для подібних випадків.

Підготовка тренінгу для персоналу — це важливий процес, який потребує чіткого планування, інтерактивності та відповідності реальним викликам. Ефективний тренінг сприяє формуванню культури безпеки, знижує ризики та підвищує рівень залученості співробітників до вирішення завдань безпеки.

Перелік питань:

1. Що таке корпоративна культура, і як вона впливає на економічну безпеку підприємства?
2. Які основні елементи корпоративної культури можна виділити?
3. У чому полягає зв'язок між корпоративною культурою та безпекою інформації?
4. Як корпоративна культура сприяє запобіганню внутрішнім загрозам на підприємстві?
5. Які особливості формування культури безпеки в організації?
6. Як впровадження політики прозорості впливає на зміцнення корпоративної культури?
7. Які етапи необхідно пройти для формування культури безпеки в компанії?
8. У чому полягає роль керівництва у створенні культури безпеки?
9. Які програми навчання допомагають зміцнити культуру безпеки в організації?
10. Як система мотивації працівників впливає на підвищення рівня економічної безпеки?
11. У чому полягає значення етичних стандартів для збереження репутації підприємства?
12. Які основні компоненти етичних стандартів можна виділити?
13. Як система звітності сприяє зміцненню корпоративної культури безпеки?
14. Які ризики можуть виникати у компанії за відсутності етичних стандартів?
15. Які приклади успішного впровадження культури безпеки відомі у світовій практиці?
16. Як запобігання конфлікту інтересів може зміцнити корпоративну культуру?
17. Які технологічні інструменти можна використовувати для моніторингу дотримання етичних стандартів?
18. Які показники ефективності (KPI) можна використовувати для оцінки впровадження корпоративної культури безпеки?
19. У чому відмінність між гіпотетичними та реальними прикладами впровадження культури безпеки?
20. Як корпоративна культура впливає на довіру серед партнерів і клієнтів?

Тести:

1. **Основна функція корпоративної культури в контексті економічної безпеки:**
   а) управління фінансовими потоками;
   б) забезпечення довіри між працівниками;
   в) аналіз ринкових тенденцій;
   г) оптимізація виробничих процесів.

2. **Що таке культура безпеки?**
   а) політики щодо конфіденційної інформації;
   б) система заходів із мінімізації ризиків;
   в) моральні принципи співробітників;
   г) система цінностей, норм і правил, спрямована на захист активів організації.

3. **Який компонент є основою корпоративної культури?**
   а) технології;
   б) політика прозорості;
   в) етичні стандарти;
   г) лояльність клієнтів.

4. **У чому полягає роль керівництва у формуванні культури безпеки?**
   а) у фінансуванні заходів безпеки;
   б) у забезпеченні прикладу дотримання стандартів;
   в) у наймі співробітників;
   г) у моніторингу ринкових показників.
5. **Який із наведених елементів сприяє запобіганню внутрішнім загрозам?**
   а) навчання персоналу;
   б) запровадження штучного інтелекту;
   в) аналіз конкурентів;
   г) використання аутсорсингових послуг.

6. **Що передбачає прозорість у корпоративній культурі?**
   а) відкритий доступ до всіх документів компанії;
   б) регулярне інформування працівників про правила та заходи безпеки;
   в) публікацію фінансових звітів у медіа;
   г) виключення відповідальності працівників.

7. **Який із методів найкраще підходить для впровадження етичних стандартів?**
   а) підвищення зарплати;
   б) проведення тренінгів та семінарів;
   в) запровадження штрафів за порушення правил;
   г) моніторинг фінансової звітності.

8. **Який елемент є важливим для успішного впровадження культури безпеки?**
   а) використання аутсорсингових послуг;
   б) впровадження цифрових технологій;
   в) залучення працівників до розробки політик безпеки;
   г) зниження витрат на навчання персоналу.

9. **Що таке етичні стандарти?**
   а) правила, які регулюють поведінку лише керівництва;
   б) система моральних принципів, які регулюють поведінку всіх співробітників;
   в) положення про звітність компанії;
   г) інструкції щодо використання конфіденційної інформації.

10. **Який із компонентів етичних стандартів сприяє мінімізації конфлікту інтересів?**
    а) система звітності;

б) антикорупційна політика;
в) навчання персоналу;
г) використання автоматизованих систем.

11. **Як корпоративна культура впливає на економічну безпеку?**
    а) збільшує витрати на навчання персоналу;
    б) підвищує стабільність роботи компанії;
    в) знижує продуктивність праці;
    г) обмежує інноваційні процеси.

12. **Який із етапів впровадження культури безпеки є першим?**
    а) розробка системи мотивації;
    б) моніторинг ефективності заходів;
    в) аналіз поточного стану;
    г) створення технічної інфраструктури.

13. **Що передбачає система мотивації у культурі безпеки?**
    а) тільки фінансові винагороди;
    б) заохочення працівників за дотримання правил безпеки;
    в) покарання за недотримання політик;
    г) перевірку знань персоналу.

14. **Як можна оцінити ефективність етичних стандартів?**
    а) через кількість конфліктів у команді;
    б) аналізуючи кількість інцидентів, пов’язаних із порушеннями правил;
    в) збільшуючи кількість тренінгів;
    г) використовуючи анкетування клієнтів.

15. **Що забезпечує корпоративна культура прозорості?**
    а) підвищення витрат на безпеку;
    б) зменшення репутаційних ризиків;
    в) скорочення кількості співробітників;
    г) зниження рівня комунікації у команді.

Практичні завдання:

Завдання 1: Аналіз корпоративної культури в організації
Мета: Оцінити поточний стан корпоративної культури в організації та визначити її вплив на економічну безпеку.

1. Оцініть за допомогою опитувальника основні аспекти корпоративної культури у вашій організації:
   - чіткість етичних стандартів;
   - рівень довіри між працівниками та керівництвом;

– наявність політик безпеки.Заповніть таблицю оцінки:

Аспект	Рівень (високий, середній, низький)	Рекомендації для покращення
Етичні стандарти		
Лояльність співробітників		
Прозорість комунікацій		

2. Запропонуйте три ініціативи для зміцнення корпоративної культури безпеки.

Завдання 2: Розробка політики корпоративної етики

Мета: Сформулювати основні положення кодексу етики для підвищення рівня економічної безпеки.

1. Визначте три ключові цінності, які повинні бути основою корпоративної культури.
2. Напишіть короткий розділ кодексу етики, який охоплює:
   – правила роботи з конфіденційною інформацією;
   – принципи запобігання конфліктів інтересів;
   – вимоги до прозорості у звітуванні.
3. Розробіть план впровадження цього кодексу в організації.

Завдання 3: Впровадження етичних стандартів

Мета: Оцінити етапи впровадження етичних стандартів у компанії.

1. На основі запропонованого кейсу заповніть таблицю:

Етап впровадження	Дії	Очікувані результати
Аналіз поточного стану		
Розробка етичних стандартів		
Навчання персоналу		
Моніторинг і вдосконалення		

2. Запропонуйте ініціативи, які дозволять ефективно донести стандарти до персоналу.

Завдання 4: Виявлення внутрішніх ризиків

Мета: Визначити потенційні внутрішні загрози через недотримання корпоративної культури.

1. Розгляньте наступну ситуацію:
   У відділі закупівель були зафіксовані випадки ухилення співробітників від дотримання політик прозорості.
2. Визначте:
   – можливі ризики для організації;
   – наслідки для економічної безпеки.
3. Запропонуйте три заходи для усунення ризиків і запобігання подібним випадкам у майбутньому.

Завдання 5: Створення програми навчання з етики

Мета: Розробити тренінг для персоналу, спрямований на підвищення обізнаності про етичні стандарти та безпеку.

1. Сформулюйте ключові теми тренінгу:
   - роль корпоративної культури у безпеці;
   - запобігання конфліктів інтересів;
   - робота з конфіденційною інформацією.
2. Визначте структуру тренінгу:
   - теоретична частина;
   - практичні кейси;
   - запитання та відповіді.
3. Створіть короткий сценарій одного із кейсів, наприклад:

   Ситуація: Співробітник випадково розголосив конфіденційну інформацію під час телефонної розмови.

   Завдання: Оцініть ризики для компанії та запропонуйте рішення.

Завдання 6: Оцінка ефективності корпоративної культури

Мета: Визначити, як корпоративна культура впливає на економічну безпеку підприємства.

1. Використовуючи дані підприємства (реального або гіпотетичного), оцініть рівень економічної безпеки до та після впровадження етичних стандартів.
2. Заповніть таблицю:

Показник	До впровадження	Після впровадження
Кількість внутрішніх інцидентів		
Рівень лояльності співробітників		
Фінансові втрати через порушення		

3. Підготуйте короткий звіт із рекомендаціями для подальшого вдосконалення корпоративної культури.

РОЗДІЛ 4. ІННОВАЦІЙНІ ПІДХОДИ ТА СТРАТЕГІЧНЕ ПЛАНУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

ТЕМА 12. СТРАТЕГІЧНЕ ПЛАНУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

12.1 Підходи до стратегічного планування безпеки.
12.2 Розробка та впровадження стратегії безпеки.
12.3 Оцінка ефективності стратегічних заходів.
12.4 Приклади успішних практик.

12.1 Підходи до стратегічного планування безпеки

Сутність стратегічного планування економічної безпеки

Стратегічне планування економічної безпеки – це процес розробки довгострокових заходів і рішень, спрямованих на запобігання ризикам, захист активів підприємства та забезпечення його стабільності. Такий підхід дозволяє організації не тільки реагувати на виклики, але й проактивно створювати умови для мінімізації загроз.

Основна мета – досягнення балансу між ефективністю бізнес-процесів і мінімізацією ризиків.

Ключові підходи до стратегічного планування безпеки

1. **Прогнозно-аналітичний підхід**
   - **Сутність:** Використання прогнозування для оцінки можливих ризиків і сценаріїв їх розвитку.
   - **Інструменти:** PEST-аналіз, SWOT-аналіз, моделі сценарного планування.
   - **Переваги:**
     - Можливість передбачити загрози на ранніх етапах.
     - Ефективне планування ресурсів для їх мінімізації.
   - **Приклад:**
     Компанія оцінює вплив економічної кризи на фінансову стабільність і заздалегідь розробляє план скорочення витрат.

2. **Ризик-орієнтований підхід**
   - **Сутність:** Виявлення ключових ризиків і формування стратегій їх управління.
   - **Інструменти:** Матриця оцінки ризиків, «теплова карта» ризиків, система раннього попередження.
   - **Переваги:**
     - Концентрація на найбільш критичних загрозах.
     - Ефективний розподіл ресурсів.

- **Приклад:**
  Промислове підприємство впроваджує систему моніторингу виробничих ризиків для запобігання зупинкам виробництва.

3. **Інноваційний підхід**
   - **Сутність:** Впровадження сучасних технологій для підвищення безпеки.
   - **Інструменти:** Автоматизація процесів, кібербезпека, використання штучного інтелекту.
   - **Переваги:**
     – Підвищення швидкості та точності реагування на загрози.
     – Оптимізація витрат на безпеку.
   - **Приклад:**
     Використання аналітичних платформ для виявлення аномалій у фінансових транзакціях.

4. **Інтеграційний підхід**
   - **Сутність:** Поєднання економічної безпеки з іншими аспектами стратегічного управління.
   - **Інструменти:** Залучення відділів фінансів, маркетингу та HR до розробки стратегії безпеки.
   - **Переваги:**
     - Синергія різних функцій у компанії.
     - Підвищення загальної стійкості організації.
   - **Приклад:**
     Інтеграція заходів із захисту даних у стратегію цифрової трансформації компанії.

Основні етапи стратегічного планування

1. **Аналіз зовнішнього та внутрішнього середовища:**
   – Використання інструментів аналізу для оцінки загроз (SWOT, PESTEL).
2. **Визначення ключових цілей:**
   – Формування цілей, які забезпечать стійкість і розвиток підприємства.
1. **Розробка стратегій управління ризиками:**
   – Вибір найбільш ефективних заходів для мінімізації загроз.
3. **Впровадження заходів:**
   – Розробка чіткого плану дій для реалізації стратегії.
4. **Моніторинг і коригування:**
   – Постійний контроль за реалізацією заходів і внесення змін у разі потреби.

Таблиця12.1 – Порівняння підходів до стратегічного планування

Підхід	Сильні сторони	Слабкі сторони
Прогнозно-аналітичний	Довгострокове бачення	Може бути складним у реалізації
Ризик-орієнтований	Фокус на ключових загрозах	Високі витрати на моніторинг
Інноваційний	Використання сучасних технологій	Залежність від рівня технічного забезпечення
Інтеграційний	Синергія між функціональними відділами	Вимагає узгодження між різними відділами

У постіндустріальній економіці на сучасному етапі розвитку спостерігається виразна тенденція органічного інтегрування суб'єктів господарювання в інформаційно-інноваційний простір, яка характеризується пожвавленням, гнучкістю та оперативним пристосуванням підприємства в нових реаліях. Відповідно особливості економічної захищеності визначаються варіативністю комплексу та типів чинників, що її формують, такими критеріями, як «стратегічна потужність» та напрямом впливу «потенціалу агресивності». Суттєве посилення значення кожної зі складових потенціалу: фінансової, економічної, інформаційної, наукової, технічної спричиняє адекватну відповідь у формі «неагресивного мислення» у безпеці економічного поступу та об'єднання можливостей у протидії виникаючим загрозам.

У стрімко змінюваних сучасних умовах вкрай важливого значення набули питання забезпечення належного рівня економічної захищеності. Вітчизняні товаровиробники відчули на собі збитки від донедавна рідкісного явища – промислового шпигунства, поширенням і продажем комерційної таємниці, переманюванням цінних співробітників, застосуванням методів недобросовісної конкуренції, а також низкою інших негативних процесів, спричинених діяльністю зовнішніх конкурентів та й самими працівниками суб'єкта господарювання.

Ефективність системи економічної захищеності суб'єкта господарювання значною мірою зумовлюється врівноваженістю власних інтересів з відповідними інтересами контрагентів зовнішнього оточення, які в силу різних обставин змушені співпрацювати з промисловим підприємством, як правило, опираючись на дію певного механізму. Процес формування економічної захищеності суб'єкта господарювання може сприйматись як комплекс організаційно-управлінських, економіко-правових і мотиваційних засобів узгодження інтересів промислового підприємства з відповідними інтересами різноманітних зовнішніх суб'єктів, в результаті чого з урахуванням специфіки виробничої діяльності підприємства створюються необхідні умови для отримання очікуваного прибутку величиною, яка здатна забезпечити економічну захищеність та стабільність положення суб'єкта господарювання.

Економічна захищеність промислового підприємства відзначається амбівалентною природою, а її особливості зумовлені масштабом загроз фінансовому та економічному становищу, а також головним фінансовим показникам діяльності суб'єкта господарювання.

Економічна захищеність являє собою особливу економічну категорію, для якої не існує загроза впливу зовнішніх та внутрішніх факторів дестабілізуючого характеру на

економічний розвиток, що властивий усім структурним і функціональним компонентам певної економічної системи, які задіяні у виробничій та фінансово-економічній діяльності.

Зважаючи на певний досвід і наукові розробки провідних вчених, можна виокремити характерні особливості економічної захищеності суб'єкта господарювання, серед яких: загальний рівень менеджменту; ґенеза ймовірних загроз (внутрішні та зовнішні відносно до системи чинників); галузь виробничої діяльності виробника; повторюваність та системність вияву; часовий лаг; керованість; значимість кризових явищ.

Комплексне вивчення системи критеріїв економічної захищеності та їх граничних показників дає змогу виокремити:

– економічні критерії, які доцільно застосовувати для оцінювання економічної захищеності;

– оптимальну систему критеріїв відповідно до мети дослідження;

– граничні показники проявів економічної захищеності з урахуванням особливостей та специфіки промислового підприємства, для якого вони призначені [216].

Виходячи з економічних показників, варто аналізувати такі індикатори економічної захищеності суб'єкта господарювання, насамперед, пропорційність чистого операційного прибутку на промисловому підприємстві та загальної сукупних операційних витрат, що дозволяє розмежувати пені зони: економічної незахищеності, перехідну, розділені точкою рівноваги, та зону економічної захищеності, порогом якої є виступає рівень економічної захищеності. Перехідна зона створює своєрідний «запас стійкості», беззбитковість операційної діяльності, суб'єкта господарювання, іншими словами – тобто здатність протидіяти зовнішнім і внутрішнім загрозам. Вона складається з певних етапів і фаз: фази активізації, перший перехідний етап, фази нестабільності, другий перехідний етап і фази стабільності.

Остаточною метою надійності сучасної системи економічної захищеності промислового підприємства є встановлення такого показника, як матеріальні збитки чи моральна шкода, які мають місце або відсутні взагалі. Такий показник включає в себе:

– захист наявного майна та належної підприємству інтелектуальної власності;

– унеможливлення розголошення конфіденційної інформації, яка є комерційною таємницею;

– профілактика та зупинення протизаконних дій працівників, клієнтів або відвідувачів;

– запобігання та усунення негативних наслідків надзвичайних ситуацій;

– захист персоналу, по відношенню до яких чиниться насильство;

– оперативне встановлення та припинення намагань недозволеного проникнення на важливі охоронювані об'єкти суб'єкта господарювання.

Створення системи ефективної економічної захищеності на вітчизняних підприємствах вимагає розробки та впровадження відповідних організаційних заходів, їх поєднання з дотриманням певної послідовності:

– задоволення потреб у достатній для продуктивної діяльності підприємства кількості виробничих ресурсів;

– планування та прогнозування економічної захищеності відповідно до реалізації ключових функцій;

– стратегічне планування виробничо-господарської діяльності суб'єкта господарювання;

– створення дієвих механізмів менеджменту господарською діяльністю суб'єкта господарювання;

– дослідження економічних явищ і процесів, пов'язаних з господарською діяльністю промислового підприємства;

– належний облік наявних ресурсів і виробничих витрат;

– оцінювання стану економічної захищеності.

Реалізація окреслених заходів щодо забезпечення економічної захищеності за своїм функціональним потенціалом зумовлює здатність до комбінування інтеграційних та інноваційних стимулів, а також належного мотивування процесу формування «особливих» можливостей, зокрема стратегічних, інституціональних, просторових, системних, ринкових, процесних, проектних та організаційних, які, відповідно, спонукають до переходу на якісно новий етап взаємопроникнення, який, у свою чергу, дає поштовх до створення ефективної інтерактивної моделі сучасного інноваційного розвитку, яка спирається на комунікацію, координацію та об'єднання низки суб'єктів міжнародного ринкового простору, що визначає подальший розвиток та рівень взаємодії інноваційних потоків різного типу: вертикальних, горизонтальних і зворотних. Відповідно, горизонтальна площина інноваційного розвитку статична за своєю природою репродукування та популяризації одиничних інновацій до повного задоволення ринкових потреб: вертикальна – має тісний зв'язок з економічною повторюваністю, чергуванням певних технологічних засад, поняттям життєвого циклу нововведень, розвитком у напрямі від базових новацій до псевдоінновацій; зворотна площина демонструє відповідь на управлінський вплив і загальний рівень продуктивності втілення інноваційного процесу. Результатом реалізації зазначених заходів стає формування стабільного середовища економічної захищеності інноваційного партнерства в різних галузях (науково-технологічній, фінансово-економічній, інвестиційній, комунікаційно-інформаційній, екологічній тощо).

Таким чином, тільки застосування інноваційних методів створення системи економічної захищеності суб'єкта господарювання дозволить продуктивно та повною мірою використовувати різні форми та способи економічного захисту промислового підприємства в нових конкурентних умовах. Через це для забезпечення своєчасної ефективної роботи системи економічної захищеності суб'єкта господарювання доцільно використовувати комплексний інноваційний підхід для:

– інноваційного аналізу фінансового компоненту економічної захищеності суб'єкта господарювання;

– інноваційної системи керування можливими ризиками у виробничі діяльності суб'єкта господарювання;

– втілення інноваційних заходів з реалізації антикризової політики суб'єкта господарювання.

Застосування стратегічного планування економічної безпеки дозволяє:

- знизити ризики фінансових втрат.
- підвищити конкурентоспроможність підприємства.
- забезпечити стабільний розвиток навіть у кризових умовах.

Стратегічне планування економічної безпеки — це багатогранний процес, який вимагає врахування різних підходів і методик. Завдяки комбінуванню прогнозування, управління ризиками, інновацій і інтеграції, підприємства можуть забезпечити стійкість і ефективність своєї діяльності.

12.2 Розробка та впровадження стратегії безпеки

Сутність розробки стратегії економічної безпеки

Стратегія економічної безпеки — це довгостроковий план дій, спрямований на захист активів підприємства, мінімізацію ризиків і забезпечення його стабільного розвитку. Розробка та впровадження такої стратегії є ключовим елементом управління підприємством у сучасному бізнес-середовищі, де загрози стають все більш комплексними.

Етапи розробки стратегії економічної безпеки

1. **Аналіз поточного стану**
   - Оцінка зовнішнього та внутрішнього середовища підприємства за допомогою PESTEL-аналізу, SWOT-аналізу або GAP-аналізу.
   - Визначення вразливих місць у фінансовій, інформаційній, кадровій та виробничій сферах.

Приклад: підприємство ідентифікує ризик втрати комерційної інформації через недостатній рівень захисту інформаційних систем.

2. **Визначення цілей стратегії**
   - **Глобальна мета:** Забезпечення довгострокової стійкості бізнесу.
   - **Оперативні цілі:**
     - Зниження ймовірності ризиків на 50%.
     - Захист ключових активів (інтелектуальної власності, фінансів, персоналу).

Приклад цілі: впровадити систему кіберзахисту, яка мінімізує ризики несанкціонованого доступу.

3. **Розробка стратегії**

Вибір відповідного підходу до управління безпекою:

- Ризик-орієнтованого (фокус на найбільш критичних загрозах).
- Інноваційного (використання новітніх технологій).
- Інтеграційного (об'єднання функцій різних підрозділів).

Приклад: для забезпечення фінансової безпеки підприємство розробляє політику управління ліквідністю.

4. **Впровадження заходів**
   - Розподіл відповідальності між відділами.
   - Визначення KPI для оцінки ефективності стратегії.
   - Встановлення системи моніторингу для відстеження змін у бізнес-середовищі.

Приклад заходів:

- Навчання співробітників правилам інформаційної безпеки.

- Встановлення багаторівневої системи аутентифікації в IT-системах.

5. **Моніторинг та вдосконалення**
   - Постійний контроль реалізації стратегії за допомогою аудиту.
   - Внесення коректив на основі змін у бізнес-середовищі.

Приклад: через нові законодавчі вимоги підприємство оновлює політику конфіденційності.

Таблиця 12.2 – Ключові аспекти впровадження стратегії

Аспект	Опис
Фінансування заходів	Виділення достатнього бюджету для реалізації стратегії.
Технічна інфраструктура	Використання сучасних технологій для забезпечення безпеки.
Кадрове забезпечення	Навчання співробітників і залучення фахівців у сфері безпеки.
Контроль виконання	Регулярний моніторинг реалізації заходів і досягнення поставлених цілей.

Типові помилки при розробці та впровадженні стратегії

1. Відсутність чітких цілей і критеріїв ефективності.
2. Недооцінка ризиків або зосередження тільки на одному аспекті безпеки.
3. Відсутність навчання персоналу.
4. Недостатнє фінансування або неправильний розподіл ресурсів.

Таблиця 12.3 – Порівняння підходів до впровадження стратегії

Підхід	Сильні сторони	Слабкі сторони
Ризик-орієнтований	Зосередженість на ключових загрозах	Може ігнорувати менш значні ризики
Інноваційний	Використання сучасних рішень	Потребує великих інвестицій
Інтеграційний	Синергія між функціями компанії	Складність узгодження між підрозділами

Розробка та впровадження стратегії економічної безпеки дозволяє:

- Знижувати ризики втрат активів.
- Забезпечувати стабільність підприємства в умовах кризи.
- Підвищувати довіру клієнтів і партнерів.

Розробка стратегії економічної безпеки є багатогранним процесом, що вимагає комплексного підходу, врахування всіх можливих ризиків і залучення ресурсів. Її ефективне впровадження сприяє зміцненню конкурентоспроможності підприємства та забезпечує стабільний розвиток у довгостроковій перспективі.

12.3 Оцінка ефективності стратегічних заходів

Сутність оцінки ефективності стратегічних заходів

Ефективність стратегічних заходів у сфері економічної безпеки визначається здатністю цих заходів знижувати рівень ризиків, захищати активи підприємства та сприяти його стабільності й розвитку. Оцінка ефективності дозволяє виявити сильні й слабкі сторони реалізованої стратегії, коригувати дії та визначити, наскільки досягнуто поставлених цілей.

Ключові етапи оцінки ефективності

1. **Визначення критеріїв оцінки**

Критерії оцінки залежать від цілей стратегії, характеру діяльності підприємства та специфіки ризиків.

Основні критерії:

- **Економічні показники:** рівень прибутковості, рентабельність, витрати на безпеку.
- **Інформаційні показники:** кількість інцидентів, пов'язаних із витоком даних.
- **Організаційні показники:** швидкість реагування на загрози, виконання планів безпеки.

2. **Аналіз результатів заходів**

Оцінка здійснюється на основі зібраних даних, що відображають фактичний стан безпеки на підприємстві.

Інструменти аналізу:

- KPI (ключові показники ефективності).
- SWOT-аналіз.
- Динаміка змін у показниках безпеки.

Приклад:

Якщо стратегія передбачала впровадження системи кіберзахисту, аналізується кількість кібератак до та після впровадження.

3. **Порівняння результатів із цілями**

Зіставлення фактичних результатів із запланованими дозволяє оцінити, чи були досягнуті поставлені цілі.

Приклад:

- Мета: зменшення випадків шахрайства на 30%.
- Фактичний результат: зменшення на 25%.
- Оцінка: необхідність додаткових заходів.

4. **Моніторинг ефективності у динаміці**

Регулярний моніторинг дозволяє оцінити тривалість і стабільність досягнутих результатів.

Приклад:

Показник стабільності фінансової безпеки оцінюється протягом кількох кварталів.

Таблиця 12.4 – Методи оцінки ефективності

Метод	Опис	Приклад використання
Фінансовий аналіз	Оцінка витрат і вигод від реалізації стратегічних заходів.	Визначення рентабельності інвестицій у безпеку (ROI).
Аудит безпеки	Аналіз відповідності впроваджених заходів внутрішнім політикам і зовнішнім регуляціям.	Перевірка дотримання стандартів ISO 27001.
SWOT-аналіз	Визначення сильних і слабких сторін стратегії.	Виявлення недоліків у підході до управління ризиками.
Порівняльний аналіз	Порівняння результатів із галузевими стандартами чи іншими підприємствами.	Аналіз кількості інцидентів на підприємстві порівняно з іншими.
Соціологічне опитування	Вивчення думки співробітників щодо ефективності заходів.	Оцінка рівня задоволеності персоналу заходами безпеки.

Таблиця 12.5 – Основні показники для оцінки ефективності

Показник	Значення для оцінки
Кількість інцидентів	Зменшення кількості ризикових ситуацій.
Фінансові втрати через ризики	Зниження обсягів збитків.
Рівень обізнаності співробітників	Відсоток персоналу, що пройшов навчання.
Час реагування на загрози	Швидкість виявлення та усунення загроз.
Витрати на безпеку	Співвідношення витрат на заходи та отриманих вигод.

Практичні приклади оцінки ефективності

1. **Компанія А:**
   - **Мета:** Зменшити ризики витоку даних.
   - **Заходи:** Встановлення системи багаторівневої аутентифікації.
   - **Результат:** Кількість інцидентів зменшилася на 40% за перший рік.
2. **Компанія В:**
   - **Мета:** Знизити фінансові втрати через шахрайство.
   - **Заходи:** Проведення тренінгів для фінансового відділу.
   - **Результат:** Зменшення втрат на 25%, підвищення обізнаності персоналу.

Оцінка ефективності стратегічних заходів дозволяє:

- Оптимізувати витрати на безпеку.
- Швидко реагувати на зміни у внутрішньому та зовнішньому середовищі.
- Забезпечити досягнення бізнес-цілей навіть у складних умовах.

Оцінка ефективності є обов’язковим етапом управління економічною безпекою. Вона дозволяє не лише перевірити доцільність уже впроваджених заходів, але й адаптувати стратегію відповідно до нових викликів, забезпечуючи довгострокову стійкість підприємства.

12.4 Приклади успішних практик

Успішне стратегічне планування економічної безпеки дозволяє підприємствам не лише запобігати ризикам, а й зміцнювати свої позиції на ринку. Реальні кейси компаній свідчать, що впровадження комплексних заходів безпеки може значно знизити фінансові втрати, покращити репутацію та підвищити ефективність операційної діяльності.

Приклад 1: Інноваційний підхід компанії IBM

- **Контекст:**
  IBM, як світовий лідер у сфері IT-рішень, зіткнулася зі зростанням кібератак через великий обсяг конфіденційних даних клієнтів.
- **Заходи:**
  1. Розробка платформи Security QRadar для аналізу кібератак у реальному часі.
  2. Впровадження принципу «Zero Trust» — кожен запит доступу до ресурсів перевіряється незалежно від джерела.
  3. Проведення навчальних програм для співробітників.
- **Результати:**
  - Зниження кількості успішних атак на 60%.
  - Підвищення довіри клієнтів до систем кіберзахисту компанії.
- **Елемент для натхнення:**
  Інтеграція інноваційних рішень у стратегію економічної безпеки може значно мінімізувати ризики.

Приклад 2: Захист виробничих потужностей Nestlé

- **Контекст:**
  Nestlé, найбільший виробник харчових продуктів, зіткнувся з ризиками підробки продукції та логістичних збоїв.
- **Заходи:**
  1. Впровадження системи відстеження продукції у реальному часі (Track & Trace).
  2. Проведення регулярного аудиту постачальників і партнерів.
  3. Розробка політик реагування на кризи у сфері безпеки постачання.
- **Результати:**
  - Зменшення кількості підробленої продукції на ринку на 30%.
  - Підвищення ефективності ланцюгів постачання на 20%.
- **Елемент для натхнення:**
  Використання цифрових рішень для захисту фізичних активів і зміцнення безпеки постачання.

Приклад 3: Банківська сфера — ПриватБанк

- **Контекст:**
  ПриватБанк, один із найбільших банків України, стикався із значними загрозами кіберзлочинів.

- **Заходи:**
  1. Впровадження багаторівневої системи аутентифікації для клієнтів.
  2. Використання технологій штучного інтелекту для моніторингу підозрілих транзакцій.
  3. Розробка програми навчання клієнтів правилам кібербезпеки.
- **Результати:**
  - Зниження випадків шахрайства з картковими операціями на 50%.
  - Підвищення довіри клієнтів до онлайн-банкінгу.
- **Елемент для натхнення:**
  Розвиток інноваційних інструментів кіберзахисту є критично важливим для забезпечення економічної безпеки.

Гіпотетичний приклад: Сталевий кластер «МеталІнвест»

- **Контекст:**
  Підприємство стикається з ризиками втрати конкурентоспроможності через нестабільну економічну ситуацію та збої у виробничому процесі.
- **Заходи:**
  1. Формування стратегічного запасу сировини.
  2. Розробка програми автоматизації ключових процесів виробництва.
  3. Навчання персоналу правилам роботи з технологіями Industry 4.0.
- **Очікувані результати:**
  - Зниження залежності від коливань цін на сировину.
  - Підвищення ефективності роботи на 25%.
- **Елемент для натхнення:**
  Комбінування фінансових, технологічних і кадрових заходів підвищує стабільність у кризових умовах.

Етапи успішного впровадження стратегій

1. Аналіз ризиків та потенціалу компанії.
2. Розробка чітких цілей і пріоритетів.
3. Планування ресурсів.
4. Моніторинг та внесення коригувань.

Реальні та гіпотетичні кейси демонструють, що впровадження інноваційних рішень, ефективного управління ризиками та навчання персоналу є ключовими факторами успіху в забезпеченні економічної безпеки.

Успішні практики стратегічного планування безпеки підтверджують, що системний підхід і врахування індивідуальних особливостей бізнесу сприяють досягненню стабільності та конкурентоспроможності. Ці кейси можуть надихнути підприємства на впровадження власних ефективних стратегій.

Перелік питань:

4. Що таке стратегічне планування економічної безпеки, і яку роль воно відіграє в діяльності підприємства?
5. Які основні цілі стратегічного планування економічної безпеки?
6. Назвіть основні підходи до стратегічного планування безпеки підприємства.
7. У чому полягає сутність прогнозно-аналітичного підходу до планування економічної безпеки?
8. Як ризик-орієнтований підхід сприяє підвищенню економічної безпеки підприємства?
9. У чому переваги інноваційного підходу до стратегічного планування?
10. Які основні етапи розробки стратегії безпеки підприємства?
11. Як проводиться аналіз зовнішнього та внутрішнього середовища під час розробки стратегії безпеки?
12. Які інструменти використовуються для оцінки ризиків у рамках стратегічного планування?
13. У чому полягає значення моніторингу та контролю під час впровадження стратегії безпеки?
14. Які методи можна застосовувати для оцінки ефективності стратегічних заходів безпеки?
15. Назвіть ключові показники ефективності (KPI) для оцінки впровадження стратегії безпеки.
16. Як фінансовий аналіз використовується для оцінки ефективності стратегічних заходів?
17. Які можливі помилки можуть виникнути під час впровадження стратегії безпеки?
18. У чому полягає важливість аудиту у процесі реалізації заходів безпеки?
19. Як соціологічні опитування допомагають оцінити ефективність стратегічних заходів?
20. Наведіть приклади успішного впровадження стратегій безпеки в реальних компаніях.
21. Як можна використовувати інноваційні технології для забезпечення економічної безпеки?
22. Який вплив мають тренінги для персоналу на успішність стратегічного планування безпеки?
23. У чому полягає значення адаптації стратегії до змін у зовнішньому середовищі?

Тести:

1. **Основна мета стратегічного планування економічної безпеки:**
   а) зниження витрат на безпеку;
   б) забезпечення довгострокової стабільності та мінімізації ризиків;
   в) підвищення рівня інновацій;
   г) контроль за діяльністю постачальників.

2. **Що є першим етапом розробки стратегії безпеки?**
   а) моніторинг результатів;
   б) визначення ключових ризиків;
   в) аналіз поточного стану середовища;
   г) формування фінансового плану.

3. **Який із підходів фокусується на виявленні та управлінні найбільш критичними загрозами?**
   а) інноваційний підхід;
   б) ризик-орієнтований підхід;
   в) інтеграційний підхід;
   г) прогнозно-аналітичний підхід.

4. **У чому полягає сутність інноваційного підходу до стратегічного планування?**
   а) у використанні сучасних технологій для підвищення безпеки;
   б) у контролі за фінансовими показниками;
   в) у залученні сторонніх аудиторів;
   г) у створенні окремого відділу безпеки.

5. **Який інструмент найбільш ефективний для аналізу зовнішнього середовища?**
   а) SWOT-аналіз;
   б) матриця ризиків;
   в) PESTEL-аналіз;
   г) соціологічне опитування.

6. **Який метод оцінює витрати на заходи безпеки відносно отриманих вигод?**
   а) аудит ризиків;
   б) ROI (рентабельність інвестицій);
   в) SWOT-аналіз;
   г) метод порівняльного аналізу.

7. **Що є основним критерієм оцінки ефективності стратегічних заходів?**
   а) збільшення кількості персоналу;
   б) зниження рівня ризиків;
   в) підвищення витрат на безпеку;
   г) скорочення звітності.

8. **Що передбачає інтеграційний підхід до планування безпеки?**
   а) консолідацію функцій різних відділів компанії;
   б) використання автоматизованих систем моніторингу;
   в) регулярне оновлення політик безпеки;
   г) залучення сторонніх консультантів.

9. **Як можна визначити успіх впровадженої стратегії безпеки?**
   а) за кількістю навчань співробітників;
   б) за кількістю реалізованих заходів;
   в) за досягненням запланованих KPI;
   г) за збільшенням кількості клієнтів.

10. **Що є основою ризик-орієнтованого підходу?**
   а) аналіз фінансових звітів;
   б) ідентифікація та управління ризиками;
   в) формування бюджетів на безпеку;
   г) використання сучасних технологій.

11. **Який інструмент дозволяє візуалізувати ризики для підприємства?**
   а) SWOT-аналіз;
   б) «Теплова карта» ризиків;
   в) PESTEL-аналіз;
   г) система KPI.

12. **Що є основною перевагою прогнозно-аналітичного підходу?**
   а) довгострокове бачення ризиків;
   б) можливість інтеграції функцій;
   в) економія ресурсів;
   г) автоматизація процесів.

13. **Який підхід передбачає адаптацію стратегії до змін у зовнішньому середовищі?**
   а) ризик-орієнтований підхід;
   б) інноваційний підхід;
   в) інтеграційний підхід;
   г) прогнозно-аналітичний підхід.

14. **Яка основна мета моніторингу ефективності стратегічних заходів?**
   а) виявлення нових бізнес-можливостей;
   б) контроль за виконанням плану безпеки;
   в) аналіз конкурентоспроможності;
   г) розробка нових продуктів.

15. **Що є прикладом кількісного показника для оцінки ефективності безпеки?**
   а) кількість проведених тренінгів;
   б) скорочення фінансових втрат через шахрайство;
   в) впровадження нових технологій;
   г) участь у зовнішніх аудиторських перевірках.

Практичні завдання:

Завдання 1: Аналіз ризиків у процесі стратегічного планування

1. Виберіть підприємство (реальне або гіпотетичне) та визначте основні загрози для його економічної безпеки.
2. Використовуючи SWOT-аналіз, заповніть таблицю:

Сильні сторони	**Слабкі сторони**
Можливості	**Загрози**

3. На основі результатів запропонуйте три рекомендації для стратегічного планування.

Завдання 2: Формування стратегії економічної безпеки

1. Виберіть один із підходів до стратегічного планування (ризик-орієнтований, прогнозно-аналітичний або інноваційний).
2. Для обраного підходу розробіть план впровадження, що включає:
   - Визначення ключових ризиків.
   - Формування короткострокових і довгострокових цілей.
   - Визначення ресурсів, необхідних для реалізації стратегії.
3. Представте план у вигляді таблиці:

Етап	**Дія**	**Очікуваний результат**
Аналіз ризиків		
Визначення цілей		
Реалізація		
Моніторинг		

Завдання 3: Оцінка ефективності заходів безпеки

1. Визначте три показники ефективності (KPI) для оцінки реалізації стратегії безпеки (наприклад, кількість інцидентів, витрати на безпеку, фінансові втрати).
2. Наведіть гіпотетичні дані до впровадження заходів і після.
3. Заповніть таблицю для порівняння результатів:

Показник	**До впровадження**	**Після впровадження**	**Зміна (%)**
Кількість інцидентів			
Фінансові втрати			
Витрати на безпеку			

4. На основі отриманих даних сформулюйте висновки про ефективність заходів.

Завдання 4: Моніторинг реалізації стратегії

1. Визначте можливі показники моніторингу реалізації стратегії економічної безпеки.
2. Заповніть таблицю:

Показник	**Частота моніторингу**	**Відповідальний відділ**

3. Розробіть план дій на випадок, якщо результати моніторингу виявляться незадовільними.

Завдання 5: Розробка антикризового сценарію

4. Сформулюйте антикризовий сценарій для підприємства, яке стикається з такими проблемами:
   - Підвищення витрат на сировину.
   - Зменшення обсягу продажів через економічну кризу.
5. Розробіть дії для кожного етапу антикризового сценарію:
   - Аналіз ситуації.
   - Планування заходів.
   - Впровадження.
   - Моніторинг.

Завдання 6: Розробка матриці ризиків

1. Визначте п’ять основних ризиків для підприємства.
2. Використовуючи методику побудови матриці ризиків, оцініть ймовірність виникнення та рівень їх впливу.
3. Заповніть таблицю:

Ризик	**Ймовірність (низька/середня/висока)**	**Рівень впливу (низький/середній/високий)**	**Пріоритет**

4. На основі таблиці визначте, які ризики потребують негайних заходів.

Завдання 7: Вивчення успішних практик

5. Оберіть одну з компаній (реальної чи гіпотетичної), яка успішно реалізувала стратегію економічної безпеки.
6. Проаналізуйте:
   - Які підходи були використані?
   - Які результати вдалося досягти?
7. Сформулюйте рекомендації, які можна застосувати для вашого підприємства.

ТЕМА 13. МІЖНАРОДНА ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

13.1 Вплив глобалізації на економічну безпеку підприємства.
13.2 Міжнародні загрози та ризики для економічної безпеки підприємств.
13.3 Оцінка та управління міжнародними ризиками.
13.4 Приклади успішного забезпечення міжнародної економічної безпеки.

13.1 Вплив глобалізації на економічну безпеку підприємства

Сутність глобалізації та її вплив на економічну безпеку

Глобалізація – це процес інтеграції світової економіки, що включає взаємодію країн, підприємств і споживачів через транснаціональні потоки капіталу, товарів, послуг, інформації та технологій. Вона створює нові можливості для бізнесу, але водночас супроводжується ризиками, які значно впливають на економічну безпеку підприємств.

Позитивний вплив глобалізації:

1. **Доступ до нових ринків.**
   Підприємства можуть розширювати географію своєї діяльності, залучаючи нових клієнтів та інвесторів.
2. **Технологічний розвиток.**
   Завдяки глобальному доступу до інновацій підприємства мають змогу підвищувати ефективність своїх процесів.
3. **Зниження витрат.**
   Можливість використовувати дешевші ресурси, виробничі потужності та послуги за кордоном.

Негативний вплив глобалізації:

1. **Збільшення конкуренції.**
   Локальні підприємства можуть втрачати ринкову частку через активність транснаціональних корпорацій.
2. **Фінансові ризики.**
   Валютні коливання, глобальні економічні кризи та торговельні санкції можуть негативно впливати на фінансову стабільність.
3. **Залежність від глобальних ланцюгів постачання.**
   Перебої в логістиці через воєнні дії, пандемії чи політичну нестабільність можуть зупинити виробництво.

Ключові аспекти впливу глобалізації на безпеку підприємства

1. **Глобальні ризики для підприємств**
   - **Економічні ризики:**
     - Коливання валютних курсів.
     - Міжнародні торговельні бар’єри.

- **Політичні ризики:**
  - Санкції та обмеження доступу до ринків.
  - Нестабільність у країнах-партнерах.
- **Соціальні ризики:**
  - Відмінності у правових та культурних стандартах, які можуть впливати на взаємодію з партнерами.

2. **Можливості глобалізації**
   - **Залучення іноземних інвестицій.**
     Вихід на міжнародні ринки дозволяє підприємствам отримувати доступ до капіталу.
   - **Диверсифікація ризиків.**
     Глобалізація дає змогу підприємствам знижувати ризики, пов'язані з одним ринком.
   - **Інноваційний потенціал.**
     Взаємодія з міжнародними партнерами сприяє обміну технологіями та підвищенню конкурентоспроможності.

Стратегії управління ризиками у глобалізованому середовищі

1. **Оцінка зовнішніх ризиків.**
   Постійний аналіз міжнародного середовища, використання інструментів, таких як PESTEL-аналіз.
2. **Диверсифікація ринків.**
   Розподіл діяльності між різними країнами для зниження ризику залежності від одного ринку.
3. **Хеджування фінансових ризиків.**
   Використання інструментів, таких як форвардні та ф'ючерсні контракти, для захисту від валютних коливань.
4. **Забезпечення гнучкості ланцюгів постачання.**
   Розробка альтернативних маршрутів і постачальників.

Приклади впливу глобалізації на економічну безпеку

5. **Позитивний приклад:**
   Apple Inc.
   Завдяки глобальному доступу до дешевих виробничих потужностей у Китаї компанія знизила витрати на виробництво. Водночас Apple створила диверсифіковану мережу постачальників, що зменшує ризик залежності від одного регіону.
6. **Негативний приклад:**
   Автомобільна промисловість під час пандемії COVID-19.
   Перебої у глобальних ланцюгах постачання мікрочипів призвели до зупинки виробництва на багатьох підприємствах. Це підкреслило важливість резервування запасів і диверсифікації постачальників.

13.2 Міжнародні загрози та ризики для економічної безпеки підприємств

У сучасному глобалізованому світі підприємства стикаються з безпрецедентною кількістю міжнародних загроз, які можуть значно вплинути на їхню економічну безпеку. Ці загрози варіюються від економічних і політичних до технологічних і соціальних факторів. Усвідомлення та управління цими ризиками є ключовими для забезпечення стійкості бізнесу.

Класифікація міжнародних загроз для підприємств

1. **Економічні загрози**
   - **Валютні коливання:**
     Різкі зміни обмінного курсу можуть впливати на вартість імпорту, експорту та міжнародних угод.
     Приклад: Коливання курсу гривні щодо долара США змінюють собівартість товарів для експортерів.
   - **Глобальні економічні кризи:**
     Зниження платоспроможності партнерів і клієнтів під час економічних спадів.
   - **Порушення міжнародної торгівлі:**
     Митні тарифи, квоти та санкції можуть обмежувати доступ до ринків.
2. **Політичні загрози**
   - **Геополітична нестабільність:**
     Воєнні конфлікти, зміна урядів або політичні санкції.
     Приклад: Воєнний стан в Україні створив ризики для підприємств, що співпрацюють із закордонними партнерами.
   - **Санкції:**
     Заборона торгівлі з певними країнами або компаніями може ускладнити бізнес.
3. **Технологічні загрози**
   - **Кібератаки:**
     Порушення роботи інформаційних систем через атаки хакерів.
     Приклад: Атака на компанію Maersk призвела до збитків у розмірі $300 млн.
   - **Витік даних:**
     Недостатній захист інформації може призвести до втрати комерційних таємниць.
4. **Логістичні загрози**
   - **Перебої у постачанні:**
     Збої в роботі міжнародних транспортних маршрутів через воєнні дії, пандемії чи природні катаклізми.
   - **Залежність від окремих постачальників:**
     Втрата ключового постачальника може паралізувати виробничі процеси.
5. **Соціальні та культурні загрози**
   - **Культурні бар'єри:**
     Неправильна інтерпретація національних особливостей може призвести до непорозумінь із партнерами.
   - **Репутаційні ризики:**
     Порушення етичних або правових стандартів у країнах-партнерах може знизити довіру клієнтів.

Таблиця 13.1 – Приклади міжнародних ризиків

Загроза	Приклад	Наслідок
Санкції	Торговельні обмеження з боку США щодо Huawei	Зменшення ринкової частки компанії.
Валютні коливання	Падіння курсу гривні під час воєнного стану	Збільшення собівартості імпортованих товарів.
Кібератаки	Атака вірусу NotPetya на глобальні компанії	Втрата даних, фінансові збитки.
Перебої у логістиці	Затримки постачання через закриття портів	Зупинка виробничих процесів.
Репутаційні ризики	Скандали навколо використання праці у несприятливих умовах	Втрата клієнтів і партнерів.

Стратегії мінімізації міжнародних ризиків

1. **Диверсифікація ринків:**
   Зменшення залежності від одного регіону або країни.
2. **Хеджування валютних ризиків:**
   Використання фінансових інструментів для страхування від коливань курсів валют.
3. **Кіберзахист:**
   Впровадження сучасних систем безпеки для захисту даних і IT-інфраструктури.
4. **Розробка плану В для логістики:**
   Пошук альтернативних постачальників і маршрутів транспортування.
5. **Культурна адаптація:**
   Навчання персоналу національним особливостям країн-партнерів.

Розуміння міжнародних загроз та ризиків дає можливість підприємствам:

- розробляти ефективні стратегії управління ризиками.
- підвищувати стійкість бізнесу до зовнішніх впливів.
- забезпечувати стабільний розвиток навіть у складних умовах.

Міжнародні загрози є невід'ємною частиною сучасного бізнес-середовища. Підприємства, які розуміють їхню природу та мають стратегії для їхнього мінімізації, отримують конкурентну перевагу на глобальному ринку.

13.3 Оцінка та управління міжнародними ризиками

Міжнародні ризики стають ключовими викликами для підприємств, що працюють на глобальному ринку. Ефективна оцінка та управління цими ризиками дозволяють мінімізувати негативні наслідки, забезпечити стабільність бізнесу та зберегти конкурентні переваги. Цей процес вимагає застосування сучасних інструментів аналізу та впровадження стратегій адаптації до змінного міжнародного середовища.

Етапи оцінки міжнародних ризиків

1. **Ідентифікація ризиків**
   На цьому етапі підприємство визначає загрози, що можуть вплинути на його діяльність. Основні джерела ризиків:
   - Економічні (валютні коливання, інфляція, економічні кризи).
   - Політичні (санкції, зміна урядів, військові конфлікти).
   - Технологічні (кібератаки, швидке моральне старіння технологій).
   - Соціальні (зміна поведінки споживачів, репутаційні ризики).
2. **Оцінка ймовірності та впливу ризиків**
   Використовується матриця ризиків, яка дозволяє оцінити ймовірність виникнення загроз та рівень їх впливу.

Таблиця 13.2 – Оцінка ймовірності впливу ризиків

Ризик	Ймовірність (низька/середня/висока)	Рівень впливу (низький/середній/високий)	Пріоритет
Валютні коливання	Висока	Високий	Високий
Санкції	Середня	Високий	Високий
Кібератаки	Середня	Середній	Середній
Перебої у постачанні	Низька	Високий	Середній

3. **Визначення ключових показників ризиків (KRI)**
   - Кількість інцидентів, пов’язаних із зовнішніми ризиками.
   - Рівень фінансових втрат від міжнародних загроз.
   - Тривалість простоїв у роботі через зовнішні фактори.
4. **Розробка плану реагування**
   Для кожного ризику розробляється набір заходів, спрямованих на його мінімізацію або усунення.

Методи управління міжнародними ризиками

1. **Диверсифікація**
   - **Ринки збуту:** Розподіл бізнесу між різними регіонами.
   - **Ланцюги постачання:** Пошук альтернативних постачальників.

   Приклад: Nestlé, яка працює в багатьох країнах, мінімізує залежність від одного ринку.
2. **Хеджування фінансових ризиків**
   - Використання фінансових інструментів (форварди, ф’ючерси, опціони) для захисту від валютних коливань.

   Приклад: Авіакомпанії часто хеджують ціни на паливо.
3. **Використання інформаційних технологій**
   - Системи моніторингу ризиків у реальному часі (ERP-системи).
   - Захист інформаційних систем від кібератак.
4. **Розробка кризового плану**
   - Створення резервних запасів.
   - Формування кризових команд для швидкого реагування.

5. **Залучення зовнішніх експертів**
   - Проведення незалежного аудиту ризиків.
   - Консультації з міжнародного права та регуляторної політики.

Таблиця 13.3 – Інструменти оцінки та управління ризиками

Інструмент	Опис	Приклад використання
Матриця ризиків	Візуалізація ймовірності та впливу ризиків	Визначення пріоритетних загроз для підприємства.
SWOT-аналіз	Аналіз сильних, слабких сторін, можливостей та загроз	Визначення стратегії реагування на глобальні виклики.
PESTEL-аналіз	Аналіз політичних, економічних, соціальних, технологічних факторів	Виявлення факторів зовнішнього впливу.
KPI та KRI	Показники ефективності управління ризиками	Контроль досягнення запланованих цілей безпеки.

Реальні приклади управління ризиками

1. **Amazon**
   - **Ризик:** Перебої в роботі складів через пандемію.
   - **Заходи:** Автоматизація процесів на складах, збільшення кількості постачальників.
2. **Coca-Cola**
   - **Ризик:** Зростання цін на сировину.
   - **Заходи:** Довгострокові контракти з постачальниками та диверсифікація джерел сировини.
3. **Maersk**
   - **Ризик:** Кібератака на інформаційну систему.
   - **Заходи:** Впровадження системи резервного копіювання та посилення IT-безпеки.

13.4 Приклади успішного забезпечення міжнародної економічної безпеки

Успішне забезпечення міжнародної економічної безпеки залежить від здатності підприємств і держав адаптуватися до глобальних ризиків, використовувати інноваційні підходи та співпрацювати на міжнародному рівні. Цей розділ аналізує реальні приклади компаній та країн, які ефективно управляють міжнародними ризиками та створюють стійкі системи безпеки.

Приклади компаній, що успішно забезпечують міжнародну економічну безпеку

1. **Nestlé: Глобальна диверсифікація та стійкість**
   - **Контекст:** Nestlé є одним із лідерів харчової промисловості, працює в більш ніж 190 країнах.
   - **Виклики:** Геополітичні ризики, валютні коливання, залежність від локальних постачальників.

- **Рішення:**
  1. **Диверсифікація:** Nestlé розподіляє виробничі потужності по всьому світу, знижуючи ризик зупинки виробництва в одному регіоні.
  2. **Локалізація:** Частина продукції виробляється з місцевої сировини, що мінімізує логістичні ризики.
  3. **Інновації:** Використання системи прогнозування ризиків на базі штучного інтелекту для оптимізації поставок.
- **Результати:** Nestlé зберегла стабільність доходів навіть під час пандемії COVID-19.

2. **Microsoft: Захист даних у глобальному середовищі**
   - **Контекст:** Microsoft обслуговує мільйони клієнтів по всьому світу, що робить компанію вразливою до кібератак.
   - **Виклики:** Постійні спроби зламу систем, витік даних, регуляторні обмеження в різних країнах.
   - **Рішення:**
     1. **Інвестиції в кіберзахист:** Розробка Azure Security Center для моніторингу загроз у реальному часі.
     2. **Комплаєнс:** Дотримання законодавства щодо захисту даних, зокрема GDPR у ЄС.
     3. **Навчання клієнтів:** Кампанії з підвищення обізнаності про кіберзагрози.
   - **Результати:** Зниження кібератак на клієнтів на 40%.
3. **Toyota: Управління ризиками постачання**
   - **Контекст:** Toyota є однією з провідних автомобільних компаній, яка використовує глобальні ланцюги постачання.
   - **Виклики:** Перебої в постачанні через природні катаклізми, торговельні обмеження.
   - **Рішення:**
     1. **Модель Just-in-Time:** Оптимізація запасів для зниження витрат і уникнення залежності від одного постачальника.
     2. **Створення резервних ланцюгів постачання:** Розширення мережі постачальників у різних країнах.
     3. **Технології:** Впровадження цифрових інструментів для моніторингу постачань у реальному часі.
   - **Результати:** Компанія зберегла стабільність виробництва навіть під час пандемії.

Державні приклади успішного забезпечення міжнародної економічної безпеки

1. **Сингапур: Центр економічної стабільності**
   - **Контекст:** Невелика країна, яка залежить від міжнародної торгівлі та інвестицій.
   - Рішення:
     1. **Економічна політика:** Створення сприятливого середовища для іноземних інвестицій.
     2. **Логістична інфраструктура:** Розвиток одного з найбільших портів у світі.
     3. **IT-безпека:** Інвестиції в кіберзахист на рівні держави.

- **Результати:** Сингапур є лідером у світових рейтингах економічної стабільності.

2. **Німеччина: Індустріальний лідер Європи**
   - **Контекст:** Найбільша економіка Європи, яка значною мірою залежить від експорту.
   - **Рішення:**
     1. **Диверсифікація ринків:** Експорт продукції в понад 100 країн світу.
     2. **Енергетична незалежність:** Розвиток відновлюваних джерел енергії.
     3. **Стандарти якості:** Високі вимоги до продукції, що зміцнює довіру до німецьких товарів.
   - **Результати:** Економіка Німеччини залишається стійкою навіть під час глобальних криз.

Висновки з успішних прикладів

Ключові фактори успіху:

1. **Диверсифікація:** Розподіл ризиків між ринками, постачальниками та напрямами діяльності.
2. **Інновації:** Використання сучасних технологій для прогнозування ризиків і оптимізації процесів.
3. **Комплаєнс:** Дотримання міжнародних норм і стандартів.
4. **Резерви:** Створення запасів для подолання кризових ситуацій.

Таблиця13.4 – Порівняння підходів до забезпечення міжнародної економічної безпеки

Компанія/Країна	Основні ризики	Заходи	Результати
1	2	3	4
Nestlé	Логістичні, валютні	Диверсифікація, прогнозування	Стабільність під час криз.
Microsoft	Кібератаки, витік даних	Інвестиції в кіберзахист, навчання клієнтів	Зниження кількості інцидентів на 40%.

Продовження таблиці 13.4

1	2	3	4
Toyota	Ланцюги постачання	Резервні постачальники, цифрові інструменти	Стійкість виробництва під час пандемії.
Сингапур	Логістичні, інвестиційні	Розвиток портів, IT-безпека	Лідер економічної стабільності.
Німеччина	Експорт, енергетика	Диверсифікація ринків, стандарти якості	Економічна стійкість у глобальних кризах.

Досвід компаній і країн доводить, що успішне забезпечення міжнародної економічної безпеки вимагає стратегічного планування, використання інновацій і співпраці на глобальному рівні. Ці приклади можуть бути джерелом натхнення для підприємств, які прагнуть зміцнити свою стійкість у міжнародному середовищі.

Перелік питань:

1. Що таке міжнародна економічна безпека підприємства?
2. Який вплив глобалізації на економічну безпеку підприємства?
3. Які основні позитивні наслідки глобалізації для бізнесу?
4. Назвіть основні ризики, які виникають через глобалізацію.
5. Як валютні коливання впливають на міжнародну економічну безпеку підприємства?
6. У чому полягає загроза геополітичної нестабільності для підприємств?
7. Які кібератаки найбільш поширені серед міжнародних компаній?
8. Як порушення ланцюгів постачання впливають на роботу підприємства?
9. Назвіть основні соціальні загрози в міжнародній діяльності.
10. У чому полягає суть репутаційних ризиків для компаній у глобальному середовищі?
11. Які методи використовуються для оцінки міжнародних ризиків?
12. Як PESTEL-аналіз допомагає оцінити зовнішні ризики?
13. У чому полягає суть матриці ризиків у міжнародній економічній безпеці?
14. Як диверсифікація бізнесу допомагає знижувати міжнародні ризики?
15. Які фінансові інструменти використовуються для хеджування валютних ризиків?
16. У чому перевага використання інформаційних систем для управління ризиками?
17. Наведіть приклад компанії, яка успішно адаптувалася до міжнародних ризиків.
18. Які кроки слід зробити підприємству для забезпечення кіберзахисту?
19. Як міжнародна співпраця між державами сприяє забезпеченню економічної безпеки бізнесу?
20. Які стратегії можна використовувати для успішного забезпечення міжнародної економічної безпеки?

Тести:

1. **Що є основною метою забезпечення міжнародної економічної безпеки підприємства?**
   а) збільшення прибутку на внутрішньому ринку
   б) мінімізація ризиків у глобальному середовищі
   в) залучення іноземного капіталу
   г) створення нових ринків збуту

2. **Який із наведених факторів є прикладом економічної загрози?**
   а) зміна політичного режиму
   б) валютні коливання
   в) кібератака на інформаційну систему
   г) репутаційні ризики

3. **Що таке PEST-аналіз?**
   а) метод оцінки внутрішніх ризиків
   б) інструмент аналізу політичних, економічних, соціальних, технологічних,

екологічних і правових факторів
в) процес розробки стратегії безпеки
г) оцінка фінансової стійкості підприємства

4. **Який метод найкраще підходить для управління валютними ризиками?**
   а) диверсифікація ринків
   б) хеджування фінансових ризиків
   в) використання інформаційних систем
   г) резервування коштів

5. **Що є основною перевагою диверсифікації бізнесу?**
   а) зниження витрат на логістику
   б) зменшення залежності від одного ринку або постачальника
   в) підвищення доходів від продажу
   г) удосконалення виробничих потужностей

6. **Як визначаються пріоритети в матриці ризиків?**
   а) за кількістю працівників у компанії
   б) за ймовірністю виникнення та рівнем впливу ризиків
   в) за тривалістю дії ризику
   г) за фінансовими втратами компанії

7. **Що є основним завданням кіберзахисту в міжнародній економічній безпеці?**
   а) розширення бази клієнтів
   б) захист інформаційних систем від несанкціонованого доступу
   в) впровадження цифрових технологій
   г) контроль валютних операцій

8. **Який із наведених ризиків є прикладом політичної загрози?**
   а) перебої в логістиці
   б) санкції проти компанії
   в) культурні відмінності
   г) зниження купівельної спроможності

9. **Що є головною метою використання інформаційних систем у міжнародному бізнесі?**
   а) збільшення кількості угод
   б) моніторинг ризиків у реальному часі
   в) зменшення вартості виробництва
   г) аналіз конкурентів

10. **Що включає в себе стратегія мінімізації репутаційних ризиків?**
    а) створення резервних запасів
    б) впровадження етичних стандартів та прозорої політики

в) контроль за валютними операціями
г) оптимізацію логістичних процесів

Практичні завдання:

Завдання 1: Ідентифікація міжнародних ризиків

1. Розгляньте підприємство, яке експортує свою продукцію до трьох різних країн. Наведіть можливі ризики для кожної країни у таких категоріях:
   - Політичні ризики.
   - Економічні ризики.
   - Технологічні ризики.
   - Логістичні ризики.
2. Заповніть таблицю:

Країна	Ризик	Категорія	Ймовірність (низька/середня/висока)	Вплив (низький/середній/високий)
Країна 1				
Країна 2				
Країна 3				

Завдання 2: Оцінка ризиків за допомогою матриці

1. Для кожного з визначених у попередньому завданні ризиків оцініть його за допомогою матриці ймовірності та впливу.
2. Визначте пріоритетність реагування на ризики.
3. Відобразіть матрицю у вигляді таблиці або графічної схеми.

Завдання 3: Розробка антикризових заходів

1. Розробіть антикризовий план для підприємства, яке стикається із такими ризиками:
   - Санкції на ключовий продукт експорту.
   - Перебої у ланцюгах постачання через геополітичну нестабільність.
   - Валютні коливання, що призводять до збитків.
2. Заповніть таблицю антикризових заходів:

Ризик	Можливі заходи	Очікуваний результат
Санкції		
Перебої у ланцюгах постачання		
Валютні коливання		

Завдання 4: Аналіз успішних практик

1. Дослідіть приклад однієї міжнародної компанії, яка ефективно впоралася з міжнародними ризиками (наприклад, Nestlé, Toyota, Microsoft).
2. Охарактеризуйте:

- З якими ризиками зіткнулося підприємство?
- Які методи використовувалися для їх подолання?
- Які результати були досягнуті?

3. Сформулюйте три уроки, які можуть бути застосовані до іншого бізнесу.

Завдання 5: Оцінка впливу глобалізації на підприємство

1. Розгляньте вплив глобалізації на підприємство, яке веде діяльність у таких галузях:
   - Харчова промисловість.
   - Технологічний сектор.
   - Логістика.
2. Для кожної галузі визначте:
   - Основні переваги.
   - Основні загрози.
3. Заповніть таблицю:

Галузь	Переваги глобалізації	Загрози глобалізації
Харчова промисловість		
Технологічний сектор		
Логістика		

Завдання 6: Стратегія мінімізації міжнародних ризиків

1. Розробіть стратегічний план для підприємства, що працює у глобальному середовищі, для мінімізації таких ризиків:
   - Кібератаки.
   - Репутаційні ризики.
   - Політична нестабільність.
2. Заповніть таблицю:

Категорія ризику	Стратегічний підхід	Очікуваний результат
Кібератаки		
Репутаційні ризики		
Політична нестабільність		

Завдання 7: Міжнародне співробітництво

1. Опишіть, як міжнародне співробітництво може сприяти зміцненню економічної безпеки підприємств.
2. Розробіть план взаємодії між підприємствами та урядами для подолання таких викликів:
   - Торговельні санкції.
   - Недобросовісна конкуренція на глобальному ринку.
   - Витік інтелектуальної власності.

ТЕМА 14. ІННОВАЦІЇ ТА ТЕХНОЛОГІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

14.1 Роль інновацій у забезпеченні економічної безпеки.
14.2 Управління технологічними ризиками.
14.3 Захист інноваційних розробок.
14.4 Інноваційні підходи до економічної безпеки.

14.1 Роль інновацій у забезпеченні економічної безпеки

Інновації стають ключовим фактором забезпечення економічної безпеки сучасних підприємств. У світі швидких змін технологічного середовища компанії, які інтегрують інновації у свої бізнес-процеси, отримують значну конкурентну перевагу, мінімізуючи ризики, підвищуючи ефективність і захищаючи свою економічну стабільність.

Значення інновацій для економічної безпеки

1. **1. Забезпечення конкурентоспроможності**

Інновації дозволяють підприємствам залишатися актуальними на ринку:

- Впровадження нових продуктів та послуг для залучення клієнтів.
- Автоматизація виробництва для підвищення продуктивності.
- Використання передових методів маркетингу для збільшення продажів.

Приклад: Tesla, завдяки інноваціям у виробництві електромобілів, утримує лідерство у своєму сегменті.

2. **2. Підвищення стійкості до зовнішніх загроз**

Інноваційні рішення знижують вплив ризиків, таких як економічні кризи, зміни в законодавстві або конкурентний тиск.

- Використання штучного інтелекту для прогнозування кризових ситуацій.
- Інтеграція цифрових інструментів для швидкої адаптації до змін на ринку.

3. **3. Ефективне управління ресурсами**

Інноваційні технології допомагають знизити витрати та оптимізувати використання ресурсів:

- Використання відновлюваних джерел енергії.
- Впровадження програмного забезпечення для управління ресурсами.

Приклад: Nestlé скоротила витрати на логістику завдяки впровадженню автоматизованих систем управління поставками.

4. **4. Захист інформаційних активів**

Сучасні підприємства використовують інноваційні технології для забезпечення інформаційної безпеки:

- Хмарні платформи для резервного копіювання даних.
- Кібербезпека на основі машинного навчання для моніторингу та запобігання загрозам.

Інноваційні підходи до економічної безпеки

1. **Технології штучного інтелекту (AI)**
   - Прогнозування фінансових ризиків.
   - Автоматичний аналіз великих обсягів даних для виявлення аномалій.

   Приклад: PayPal використовує AI для виявлення шахрайства в реальному часі.
2. **Блокчейн**
   - Забезпечення прозорості в операціях.
   - Захист даних у фінансових та логістичних процесах.

   Приклад: IBM Food Trust використовує блокчейн для відстеження постачання продуктів харчування.
3. **Інтернет речей (IoT)**
   - Моніторинг стану обладнання в реальному часі.
   - Попередження аварій завдяки аналітиці даних.
4. **Відновлювальні джерела енергії**
   - Зниження залежності від викопного палива.
   - Підвищення екологічної відповідальності.

   Приклад: Amazon інвестує у вітрові та сонячні ферми для забезпечення енергонезалежності.

Таблиця 14.1 – Переваги використання інновацій для безпеки

Переваги	Опис
Зниження операційних витрат	Автоматизація процесів скорочує витрати на персонал і ресурси.
Збільшення швидкості адаптації	Інноваційні рішення дозволяють швидше реагувати на виклики.
Захист інформації	Використання передових рішень кібербезпеки знижує ризики втрат.
Розширення ринкових можливостей	Інновації відкривають доступ до нових ринків і клієнтів.

Практичне значення

1. Використання інновацій сприяє захисту підприємств від економічних, політичних і технологічних ризиків.
2. Компанії, що інтегрують інноваційні технології, підвищують свою конкурентоспроможність і забезпечують довгострокову стабільність.
3. Інновації дозволяють оптимізувати бізнес-процеси, скорочуючи витрати й підвищуючи ефективність.

Роль інновацій у забезпеченні економічної безпеки неможливо переоцінити. Вони допомагають компаніям адаптуватися до глобальних викликів, захищати свої ресурси та створювати нові можливості для розвитку. Інноваційний підхід є ключем до успіху в сучасному бізнес-середовищі.

14.2 Управління технологічними ризиками

Технологічні ризики є невід'ємною частиною діяльності сучасних підприємств, адже інтеграція новітніх технологій приносить не тільки переваги, але й виклики. Управління технологічними ризиками дозволяє підприємствам мінімізувати загрози, забезпечити безперервність бізнес-процесів і зберегти конкурентоспроможність.

Ключові аспекти технологічних ризиків

Типи технологічних ризиків

1. **Технічні збої:**
   - Неполадки обладнання, програмного забезпечення або IT-систем.

   Приклад: Перебої у роботі серверів компанії Amazon призвели до втрати доступу до онлайн-платформи на кілька годин.
2. **Кібератаки:**
   - Хакерські атаки, витоки даних, блокування систем.

   Приклад: Атака вірусу NotPetya завдала збитків міжнародним компаніям, включаючи Maersk.
3. **Моральне старіння технологій:**
   - Втрата актуальності технологій через швидкий розвиток інновацій.

   Приклад: Застарілі системи кіберзахисту стають вразливими для нових видів атак.
4. **Людський фактор:**
   - Помилки персоналу, відсутність належної кваліфікації чи недотримання процедур.

Процес управління технологічними ризиками

1. **Ідентифікація ризиків**
   - Визначення основних технологічних загроз.
   - Використання аудиту IT-систем, обладнання та процесів.
2. **Оцінка ймовірності та впливу ризиків**
   - Використання матриці ризиків для класифікації загроз за рівнем їх важливості.
   - Оцінка потенційних фінансових збитків, пов'язаних із технологічними ризиками.
3. **Розробка заходів реагування**
   - Зниження ймовірності ризику:
   - Регулярне оновлення обладнання та програмного забезпечення.
     - Впровадження автоматизованих систем моніторингу.
   - Мінімізація впливу ризику:
     - Створення резервних копій даних (backup).
     - Розробка планів аварійного відновлення (disaster recovery plans).
4. **Контроль і моніторинг**
   - Постійний моніторинг систем у реальному часі.
   - Регулярні перевірки відповідності процедур стандартам безпеки (ISO 27001).

Інструменти управління технологічними ризиками

1. **Системи кіберзахисту:**
   - Антивірусні програми, міжмережеві екрани (firewalls), системи виявлення загроз.
2. **Автоматизація управління ризиками:**
   - Програмне забезпечення для моніторингу ризиків у реальному часі.

   Приклад: SAP GRC для управління комплаєнсом і ризиками.
3. **Навчання персоналу:**
   - Регулярні тренінги для підвищення кваліфікації працівників.
4. **Технологічний аудит:**
   - Оцінка стану обладнання та програмного забезпечення.

Приклади управління технологічними ризиками

1. **Microsoft**
   - **Ризик:** Часті атаки на хмарні сервіси.
   - **Рішення:** Розробка Azure Security Center для моніторингу загроз.
   - **Результат:** Зниження ризику втрати даних клієнтів.
2. **Toyota**
   - **Ризик:** Збої у постачанні компонентів через залежність від постачальників.
   - **Рішення:** Використання Інтернету речей (IoT) для відстеження стану постачання.
   - **Результат:** Оптимізація ланцюгів постачання.
3. **Google**
   - **Ризик:** Витік конфіденційної інформації.
   - **Рішення:** Впровадження багаторівневої системи автентифікації та шифрування даних.
   - **Результат:** Підвищення довіри користувачів до сервісів Google.

Ефективне управління технологічними ризиками є ключовим елементом забезпечення економічної безпеки. Використання інноваційних підходів, навчання персоналу та регулярний моніторинг дозволяють підприємствам мінімізувати вплив ризиків і залишатися конкурентоспроможними у швидко змінюваному світі.

14.3 Захист інноваційних розробок

Інноваційні розробки є важливим активом підприємства, який забезпечує його конкурентоспроможність і стійкість на ринку. Захист цих розробок дозволяє зберегти інтелектуальну власність, запобігти копіюванню і втраті ноу-хау, а також забезпечити довгострокову економічну безпеку.

Основні аспекти захисту інноваційних розробок

Види інноваційних активів, що потребують захисту

1. **Патенти:**
   - Технологічні рішення, винаходи, промислові зразки.
   - **Приклад:** Патент на електромобільні технології компанії Tesla.
2. **Торгові марки:**
   - Логотипи, бренди, слогани.

   Приклад: Фірмовий стиль Apple.
3. **Комерційна таємниця:**
   - Ноу-хау, алгоритми, рецепти, бізнес-моделі.
   - **Приклад:** Рецепт Coca-Cola.
4. **Авторські права:**
   - Програмне забезпечення, дизайнерські рішення, художні твори.

Юридичні механізми захисту інновацій

1. **Реєстрація інтелектуальної власності**
   - **Патенти:** Захист винаходів на національному та міжнародному рівнях.

   Приклад: Всесвітня організація інтелектуальної власності (WIPO) забезпечує реєстрацію патентів у кількох країнах.
   - **Торгові марки:** Забезпечення унікальності бренду через офіційну реєстрацію.
   - **Авторські права:** Захист програмного забезпечення, дизайнів, музичних творів.
2. **Використання ліцензій**
   - Надання прав на використання інноваційних рішень іншим підприємствам у межах визначених умов.

   Приклад: Microsoft ліцензує своє програмне забезпечення іншим компаніям.
3. **Захист комерційної таємниці**
   - Впровадження політики конфіденційності:
     - Обмеження доступу до ключових документів.
     - Використання угод про нерозголошення (NDA).

   Приклад: NDA у стартапах для збереження ноу-хау.
4. **Дотримання міжнародних стандартів**
   - **TRIPS Agreement:** Міжнародна угода про торговельні аспекти інтелектуальної власності.
   - **ISO 27001:** Стандарти інформаційної безпеки.

Технологічні інструменти захисту інновацій

1. **Кібербезпека**
   - Захист цифрових даних від несанкціонованого доступу.

   Інструменти: Антивіруси, системи багаторівневої автентифікації, шифрування даних.

2. **Блокчейн**
   - Реєстрація прав інтелектуальної власності та транзакцій у децентралізованій базі даних.

   Приклад: Використання блокчейн-технологій для відстеження авторства в музичній індустрії.
3. **Хмарні технології**
   - Резервне копіювання даних у хмарі для запобігання втраті інформації.
4. **Інтелектуальні системи моніторингу**
   - Автоматизований пошук порушень інтелектуальної власності в мережі.

   Приклад: Програмні платформи для пошуку контрафактної продукції.

Приклади успішного захисту інновацій

1. **Tesla**
   - **Ризик:** Копіювання технологій електромобілів.
   - **Рішення:** Реєстрація патентів і публічний доступ до них, що дозволяє стимулювати ринок без загрози власній конкурентоспроможності.
2. **Microsoft**
   - **Ризик:** Незаконне використання програмного забезпечення.
   - **Рішення:** Впровадження унікальних ключів активації програм і постійне оновлення системи ліцензування.
3. **Coca-Cola**
   - **Ризик:** Викрадення рецепту напою.
   - **Рішення:** Збереження формули як комерційної таємниці, доступної лише для кількох осіб.

Захист інноваційних розробок є невід'ємною складовою економічної безпеки підприємств. Відсутність належних заходів захисту може призвести до фінансових втрат, втрати конкурентних переваг і репутаційних ризиків.

Ефективний захист інноваційних розробок є ключовим для довгострокового успіху бізнесу. Використання юридичних, технологічних та організаційних механізмів дозволяє мінімізувати ризики втрати інтелектуальних активів і зміцнити конкурентну позицію на ринку.

14.4 Інноваційні підходи до економічної безпеки

Інноваційні підходи до економічної безпеки забезпечують підприємствам ефективні засоби протидії сучасним загрозам та викликам. Використання передових технологій, адаптивних моделей управління і новаторських стратегій дозволяє мінімізувати ризики, оптимізувати ресурси і підвищувати конкурентоспроможність.

Сучасні інноваційні підходи

1. **Використання штучного інтелекту (AI)**
    1. **Аналіз великих обсягів даних (Big Data):**
        - Виявлення ризиків у реальному часі.
        - Прогнозування змін у зовнішньому середовищі.

        Приклад: Компанія JPMorgan використовує AI для аналізу фінансових ризиків і виявлення шахрайства.
    2. **Автоматизація рутинних процесів:**
        - Зниження витрат на адміністративні операції.
        - Покращення швидкості прийняття рішень.
2. **Технології блокчейну**
    1. **Прозорість операцій:**
        - Забезпечення прозорості у фінансових транзакціях.
        - Захист від підробок документів.
    2. **Контроль ланцюгів постачання:**
        - Відстеження товарів на кожному етапі постачання.

        Приклад: Walmart використовує блокчейн для моніторингу якості продуктів харчування.
3. **Інтернет речей (IoT)**
    1. **Моніторинг стану обладнання:**
        - Виявлення несправностей у реальному часі.
        - Профілактичне обслуговування.
    2. **Оптимізація виробничих процесів:**
        - Зниження енергетичних витрат.

        Приклад: General Electric впровадила IoT для контролю стану своїх авіаційних двигунів.
4. **Кібербезпека нового покоління**
    1. **Машинне навчання для моніторингу загроз:**
        - Виявлення підозрілої активності в мережі.
        - Автоматична адаптація до нових видів атак.
    2. **Багаторівневі системи аутентифікації:**
        - Використання біометрії, токенів і паролів.

        Приклад: Google застосовує багаторівневий доступ для захисту своїх даних.
5. **Автоматизація управління ризиками**
    - Використання спеціалізованих програм для моніторингу, оцінки та управління ризиками.

    Приклад: SAP GRC, що забезпечує інтеграцію управління ризиками з бізнес-процесами.

Впровадження інноваційних стратегій

1. **Моделі управління ризиками**
    - **Проактивний підхід:** Постійний моніторинг загроз та швидке реагування на зміни.

- **Адаптивний підхід:** Швидка перебудова бізнес-процесів під впливом зовнішніх факторів.

2. **Впровадження комплаєнс-програм**
   - Забезпечення відповідності міжнародним стандартам (GDPR, ISO).
3. **Створення інноваційних центрів**
   - Розробка нових технологій всередині компанії.
   - Підтримка стартапів та інноваційних проектів.

   Приклад: Bosch відкрила інноваційний центр для розробки IoT-рішень.

Приклади впровадження інновацій

1. **Amazon:**
   - Використання робототехніки для автоматизації складів.
   - Прогнозування поведінки покупців за допомогою AI.
2. **Tesla:**
   - Інноваційні батареї для електромобілів.
   - Використання IoT для оновлення програмного забезпечення автомобілів у режимі реального часу.
3. **IBM:**
   - Впровадження блокчейн-рішень для захисту конфіденційних даних.

Практичне значення

1. Інноваційні підходи дозволяють підприємствам:
   - Реагувати на ризики у реальному часі.
   - Захищати інтелектуальну власність і ресурси.
   - Підвищувати ефективність і знижувати витрати.
2. Вони забезпечують конкурентні переваги на глобальному ринку та довгострокову стабільність.

Інноваційні підходи до економічної безпеки відкривають нові можливості для розвитку бізнесу та забезпечення його стійкості до сучасних викликів. Впровадження новітніх технологій, автоматизації процесів і адаптивних стратегій стає обов’язковим кроком для кожного підприємства, яке прагне досягти успіху в умовах глобальної економіки.

Перелік питань:

1. Що таке інновації в контексті економічної безпеки підприємства?
2. Які основні види інновацій впливають на економічну безпеку підприємства?
3. Чому інновації є ключовим елементом забезпечення конкурентоспроможності?
4. Як автоматизація бізнес-процесів підвищує рівень економічної безпеки?
5. Яку роль відіграють технології штучного інтелекту у забезпеченні безпеки підприємства?
6. Що таке блокчейн, і як його використовують для забезпечення економічної безпеки?
7. Як Інтернет речей (IoT) допомагає підприємствам моніторити виробничі процеси?
8. Які типи ризиків виникають при використанні новітніх технологій у бізнесі?
9. У чому полягає роль кібербезпеки нового покоління у захисті інновацій?
10. Як впровадження систем моніторингу в реальному часі знижує рівень ризиків?
11. Які переваги дає підприємствам автоматизація управління ризиками?
12. Що таке адаптивний підхід до управління ризиками, і як його застосовують?
13. Як використання Big Data дозволяє передбачати ризики в економічній безпеці?
14. Чому міжнародні стандарти, такі як ISO 27001, є важливими для технологічної безпеки?
15. Як хмарні технології забезпечують захист даних підприємства?
16. У чому переваги впровадження інноваційних центрів на підприємствах?
17. Як технології допомагають боротися з моральним старінням обладнання?
18. Які інструменти використовуються для захисту інноваційних розробок?
19. Чому інтеграція інноваційних підходів є ключовою для довгострокової стратегії підприємства?
20. Як реальні приклади впровадження інновацій, наприклад, у Tesla або Amazon, можуть бути адаптовані до українських підприємств?

Тести:

1. **Яка основна мета впровадження інновацій у забезпеченні економічної безпеки підприємства?**
   а) Підвищення рівня прибутковості
   б) Мінімізація ризиків і підвищення стійкості бізнесу
   в) Зниження витрат на виробництво
   г) Оптимізація кадрової політики

2. **Що таке блокчейн у контексті економічної безпеки?**
   а) Система моніторингу ризиків у реальному часі
   б) Технологія децентралізованого збереження даних
   в) Система управління ризиками
   г) Програмне забезпечення для автоматизації фінансів

3. **Який інструмент використовується для прогнозування ризиків у економічній безпеці?**
   а) PESTEL-аналіз
   б) Матриця SWOT
   в) Штучний інтелект (AI)
   г) Контроль за дотриманням стандартів

4. **Як Інтернет речей (IoT) сприяє забезпеченню економічної безпеки?**
   а) Забезпечує хмарне зберігання даних
   б) Дозволяє відстежувати стан обладнання у реальному часі
   в) Використовується для управління фінансовими потоками
   г) Сприяє аналізу маркетингових стратегій

5. **Який з наведених стандартів стосується кібербезпеки?**
   а) ISO 9001
   б) ISO 27001
   в) TRIPS Agreement
   г) GDPR

6. **Що таке автоматизація управління ризиками?**
   а) Використання штучного інтелекту для створення нових продуктів
   б) Впровадження програмного забезпечення для моніторингу та аналізу ризиків
   в) Створення резервних копій даних
   г) Використання матриці SWOT для оцінки ринкових можливостей

7. **Як хмарні технології забезпечують безпеку даних підприємства?**
   а) Дозволяють створювати резервні копії даних у реальному часі
   б) Знижують витрати на виробництво
   в) Збільшують швидкість передачі даних
   г) Забезпечують автоматизацію виробничих процесів

8. **Що є головним завданням штучного інтелекту у сфері економічної безпеки?**
   а) Прогнозування ризиків та аналіз великих обсягів даних
   б) Автоматизація кадрового обліку
   в) Управління витратами підприємства
   г) Розробка маркетингових стратегій

9. **Яке програмне забезпечення використовується для інтеграції управління ризиками?**
   а) SAP GRC
   б) Google Docs
   в) Microsoft Teams
   г) Slack

10. **Яка з наведених компаній успішно використовує блокчейн для забезпечення економічної безпеки?**
    а) Tesla
    б) Walmart
    в) Amazon
    г) Microsoft

Практичні завдання:

Завдання 1: Аналіз інноваційних ризиків

1. Оцініть основні ризики, пов'язані з впровадженням нових технологій у підприємстві:
   - Технічні ризики.
   - Ризики конфіденційності.
   - Ризики фінансових втрат.
2. Заповніть таблицю ризиків:

Ризик	Ймовірність (низька / середня / висока)	Вплив (низький / середній / високий)	Заходи мінімізації
Технічний ризик			
Ризик конфіденційності			
Фінансовий ризик			

Завдання 2: Розробка інноваційної стратегії

1. Розробіть інноваційну стратегію для підприємства у сфері:
   - Харчова промисловість.
   - Логістика.
   - IT-технології.
2. Для кожної галузі визначте:
   - Які технології доцільно впровадити?
   - Які ризики можуть виникнути?
   - Які заходи потрібні для їх мінімізації?
3. Заповніть таблицю:

Галузь	Інновація	Ризики	Заходи мінімізації
Харчова промисловість			
Логістика			
IT-технології			

Завдання 3: Моделювання управління ризиками

1. Використовуючи метод матриці ризиків, оцініть загрози від упровадження таких технологій, як:
   - Блокчейн.
   - Штучний інтелект.

- Інтернет речей (IoT).

2. Побудуйте матрицю ризиків, класифікуючи їх за рівнями ймовірності та впливу.

Завдання 4: Аналіз реального кейсу

1. Ознайомтеся з діяльністю таких компаній, як Tesla, Walmart або IBM, які успішно впроваджують інновації.
2. Проаналізуйте:
   - Які технології були впроваджені?
   - Які ризики виникали під час впровадження?
   - Які заходи були застосовані для їх мінімізації?
3. Сформулюйте три ключові уроки, які можуть бути застосовані до українських підприємств.

Завдання 5: Створення інноваційної моделі

1. Розробіть модель використання інновацій для забезпечення економічної безпеки підприємства.
2. Вкажіть основні елементи:
   - Впровадження інновацій.
   - Управління технологічними ризиками.
   - Захист інноваційних розробок.
3. Представте модель у вигляді схеми або інфографіки.

Завдання 6: Використання технологій для захисту

1. Запропонуйте інноваційні підходи до захисту інтелектуальної власності для таких видів активів:
   - Патенти.
   - Авторські права.
   - Комерційна таємниця.
2. Наведіть конкретні приклади інструментів для забезпечення захисту.

Завдання 7: Розробка плану автоматизації

3. Створіть план автоматизації управління ризиками для підприємства, яке працює в енергетичній сфері.
4. Укажіть етапи автоматизації:
   - Ідентифікація ризиків.
   - Оцінка ризиків.
   - Контроль ризиків за допомогою програмного забезпечення.

ТЕМА 15. ЕКОЛОГІЧНА БЕЗПЕКА ПРОМИСЛОВОГО ПІДПРИЄМСТВА

ПИТАННЯ, ЩО ВИВЧАЮТЬСЯ:

15.1 Взаємозв'язок між екологічною та економічною безпекою.
15.2 Управління екологічними ризиками.
15.3 Стратегії зниження екологічного впливу на безпеку підприємства.
15.4 Вимоги до екологічної відповідальності підприємства.

15.1 Взаємозв'язок між екологічною та економічною безпекою

Екологічна та економічна безпека промислового підприємства є взаємопов'язаними поняттями, що впливають на стійкий розвиток бізнесу. Екологічна безпека забезпечує збереження природних ресурсів та мінімізацію негативного впливу на довкілля, що у свою чергу створює передумови для зниження ризиків, підвищення ефективності і конкурентоспроможності підприємства.

Значення екологічної безпеки для економічної стабільності

1. **Зниження витрат**
    1. **Економія ресурсів:**
        - Зменшення споживання енергії та води.
        - Оптимізація використання сировини.

        Приклад: Впровадження енергоефективних технологій дозволяє зменшити витрати на енергопостачання.
    2. **Зменшення екологічних платежів:**
        - Виконання вимог екологічного законодавства знижує штрафи та екологічні податки.

        Приклад: Металургійні компанії зменшують викиди CO_2, впроваджуючи сучасні фільтри.
2. **Покращення репутації**
    1. **Довіра споживачів:**
        - Екологічно відповідальний бізнес привертає увагу клієнтів, які віддають перевагу «зеленим» продуктам.
    2. **Залучення інвесторів:**
        - Підприємства, які дотримуються принципів ESG (екологічне, соціальне та корпоративне управління), частіше отримують підтримку від міжнародних інвесторів.

        Приклад: Компанії Unilever та Nestlé активно працюють над екологічними ініціативами, що зміцнює їхній бренд.
3. **Зменшення ризиків**
    1. **Правові ризики:**
        - Дотримання екологічних стандартів запобігає штрафам та судовим позовам.
    2. **Ризики соціальної відповідальності:**
        - Зменшення негативного впливу на громади навколо підприємства.

Приклад: Запобігання забрудненню водних ресурсів захищає місцеве населення від екологічних катастроф.

Вплив економічної безпеки на екологічну стабільність

1. **Інвестиції в екологічні проєкти**
   - Підприємства, які мають стабільну фінансову основу, інвестують у:
     - Енергоефективні технології.
     - Відновлювальні джерела енергії.

     Приклад: Tesla інвестує у розробку сонячних панелей для зарядних станцій.
2. **Оптимізація процесів**
   - Раціональне використання ресурсів знижує екологічний вплив. **Приклад:** Заміна традиційних технологій виробництва на менш енергоємні.
3. **Розвиток циклічної економіки**
   - Перехід до моделі «reduce-reuse-recycle» дозволяє зменшити кількість відходів.

Синергетичний ефект екологічної та економічної безпеки

1. **Підвищення ефективності:** скорочення витрат за рахунок раціонального використання ресурсів.
2. **Зменшення впливу на довкілля:** зниження викидів шкідливих речовин.
3. **Довгострокова стабільність:** підприємства, які інвестують у екологічну безпеку, залишаються конкурентоспроможними навіть у періоди змін законодавства.

Практичне значення

1. **Дотримання стандартів:** впровадження екологічних технологій допомагає підприємствам виконувати вимоги міжнародних стандартів.
2. **Оптимізація витрат:** скорочення споживання енергоресурсів сприяє фінансовій стабільності.
3. **Соціальна відповідальність:** підприємства формують позитивний імідж серед споживачів і партнерів.

Екологічна та економічна безпека є взаємозалежними складовими, що забезпечують довгострокову стабільність підприємства. Інтеграція екологічних практик у бізнес-процеси дозволяє мінімізувати ризики, підвищити ефективність і створити стійку основу для подальшого розвитку.

15.2 Управління екологічними ризиками

Екологічні ризики становлять серйозну загрозу для стійкого функціонування підприємств, оскільки вони можуть призвести до фінансових втрат, погіршення репутації та санкцій. Ефективне управління екологічними ризиками допомагає мінімізувати вплив на довкілля, забезпечити відповідність законодавчим нормам та підвищити конкурентоспроможність підприємства.

Етапи управління екологічними ризиками

1. **Ідентифікація екологічних ризиків**
   - Виявлення потенційних джерел ризиків:
     - Викиди шкідливих речовин у повітря.
     - Забруднення водних ресурсів.
     - Генерація твердих відходів.

   Приклад: Нафтопереробні підприємства аналізують можливі ризики розливу нафти та її вплив на екосистему.
2. **Оцінка ймовірності та впливу**
   - Оцінка масштабу впливу ризику на довкілля:
     - Використання методів екологічного аудиту.
     - Визначення рівня ймовірності виникнення кожного ризику.

Таблиця 15.1 – Приклад розрахунку обсягів потенційних викидів парникових газів у разі аварії на підприємстві.

Ризик	Ймовірність (низька / середня / висока)	Вплив (низький / середній / високий)
Забруднення водних ресурсів	Середня	Високий
Викиди в атмосферу	Висока	Високий
Генерація небезпечних відходів	Низька	Середній

3. **Розробка стратегії реагування**
   - Уникнення ризиків:
     - Модернізація обладнання для зменшення викидів.
     - Використання екологічно безпечних матеріалів.
   - Зниження ризиків:
     - Встановлення очисних споруд.
     - Реалізація програм з управління відходами.
   - Передача ризиків:
     - Страхування екологічних ризиків для покриття витрат на ліквідацію наслідків.
   - Прийняття ризиків:
     - Виконання оцінки витрат і прибутків для обґрунтування прийняття ризику.
4. **Моніторинг і контроль**
   - Постійне відстеження рівня впливу діяльності підприємства на довкілля.
   - Використання інструментів моніторингу, таких як сенсори для контролю якості повітря та води.

Інструменти управління екологічними ризиками

1. **Екологічний аудит**
   - Регулярний аналіз стану довкілля навколо підприємства.
   - Оцінка відповідності екологічним стандартам.
2. **Впровадження екологічних стандартів**
   - Сертифікація за стандартами ISO 14001.

- Використання міжнародних норм для зниження впливу на довкілля.

3. **Використання технологій**
   - Системи моніторингу екологічних показників у реальному часі.
   - Автоматизовані очисні споруди для зменшення шкідливих викидів.
4. **Залучення громади**
   - Програми соціальної відповідальності для підвищення довіри місцевих громад.
   - Прозоре інформування про екологічні заходи підприємства.

Приклади успішного управління екологічними ризиками

1. **Nestlé:**
   - Використання відновлювальної енергії у виробничих процесах.
   - Реалізація програм із зменшення використання води.
2. **Siemens:**
   - Впровадження технологій Smart Grid для зниження енергетичних втрат.
3. **Shell:**
   - Інвестиції у технології з утилізації вуглекислого газу.

Практичне значення

1. Управління екологічними ризиками забезпечує стабільну діяльність підприємства в умовах зростаючих вимог екологічного законодавства.
2. Підприємства, які активно працюють над екологічною безпекою, отримують довіру інвесторів і споживачів.
3. Інтеграція інноваційних рішень дозволяє зменшити вплив на довкілля та уникнути значних штрафів.

Ефективне управління екологічними ризиками сприяє довгостроковій стабільності та конкурентоспроможності підприємства. Використання інноваційних інструментів і стратегій дозволяє мінімізувати негативний вплив на довкілля, одночасно покращуючи економічні показники компанії.

15.3 Стратегії зниження екологічного впливу на безпеку підприємства

Екологічний вплив діяльності підприємства прямо впливає на його економічну безпеку. Високі витрати на природоохоронні заходи, штрафи за порушення екологічних норм та негативний вплив на репутацію можуть стати серйозними викликами. Стратегії зниження екологічного впливу не лише дозволяють мінімізувати ризики, а й створюють умови для стійкого розвитку бізнесу.

Основні стратегії зниження екологічного впливу

1. **Енергоефективність**
   1. **Оптимізація споживання енергії:**
      - Встановлення енергоефективного обладнання.
      - Використання датчиків для контролю освітлення та енергоспоживання.

Приклад: Компанія Apple повністю перейшла на використання відновлювальної енергії у своїх офісах і дата-центрах.

2. **Впровадження відновлюваних джерел енергії:**
   - Використання сонячних батарей, вітрових турбін, біогазових установок.

   Приклад: Google інвестує у будівництво сонячних електростанцій.

2. **Зменшення відходів**
   1. **Перехід на циклічну економіку:**
      - Впровадження моделі «reduce-reuse-recycle».

      Приклад: Unilever працює над тим, щоб до 2030 року всі їхні пакування були повністю перероблюваними.
   2. **Утилізація та переробка:**
      - Роздільний збір відходів, впровадження програм компостування.
      - Переробка промислових відходів у нові матеріали.
3. **Управління водними ресурсами**
   1. **Зменшення споживання води:**
      - Встановлення систем для повторного використання води у виробничих процесах.

      Приклад: Nestlé використовує інноваційні технології для зменшення споживання води у виробництві на 30%.
   2. **Очищення стічних вод:**
      - Встановлення сучасних очисних споруд для мінімізації забруднення.
4. **Контроль викидів**
   1. **Зменшення викидів парникових газів:**
      - Використання електротранспорту на підприємстві.
      - Впровадження технологій уловлювання та зберігання вуглецю (CCS).
   2. **Фільтрація забруднюючих речовин:**
      - Встановлення сучасних фільтрів на заводах і виробничих лініях.

      Приклад: Компанія ArcelorMittal інвестує у технології зменшення викидів CO_2 у сталеливарній промисловості.

Економічна вигода від впровадження екологічних стратегій

1. **Зниження витрат:**
   - Скорочення витрат на енергоресурси та природоохоронні заходи.
2. **Підвищення ефективності:**
   - Оптимізація виробничих процесів через використання сучасних технологій.
3. **Покращення репутації:**
   - Привернення уваги екологічно свідомих клієнтів та інвесторів.

Реальні приклади успішних стратегій

1. **Tesla:**
   - Використання відновлюваних джерел енергії та повний перехід на електромобілі для зменшення вуглецевого сліду.

2. **IKEA:**
   - Програма з переходу на 100% відновлюваної енергії та зменшення використання пластику у пакуванні.
3. **Procter & Gamble:**
   - Впровадження енергоефективних технологій на всіх виробничих майданчиках та програми утилізації продукції.

Практичне значення

1. Екологічні стратегії сприяють зменшенню витрат і покращенню фінансових результатів підприємства.
2. Інтеграція екологічних практик допомагає зменшити ризики штрафів та санкцій.
3. Створення позитивного іміджу сприяє довгостроковому успіху бізнесу.

Впровадження стратегій зниження екологічного впливу дозволяє підприємствам забезпечити баланс між стійким розвитком і збереженням довкілля. Інноваційні підходи, ефективне управління ресурсами та залучення екологічних технологій стають обов'язковою складовою сучасного бізнесу.

15.4 Вимоги до екологічної відповідальності підприємства

Екологічна відповідальність підприємства стає одним із ключових факторів стійкого розвитку в умовах сучасної економіки. Зростаючі вимоги міжнародного та національного законодавства, а також зміни в очікуваннях суспільства змушують підприємства враховувати екологічні аспекти у своїй діяльності. Дотримання екологічних стандартів дозволяє знизити ризики, уникнути санкцій і покращити репутацію підприємства.

Ключові вимоги до екологічної відповідальності

1. **Дотримання законодавчих норм**
   - **Міжнародне законодавство:**
     - Директиви ЄС щодо скорочення викидів CO_2.
     - Паризька угода про клімат, яка встановлює рамки скорочення глобального потепління.
   - **Національні вимоги:**
     - Виконання екологічних законів, наприклад, законодавства України про охорону навколишнього середовища (ЗУ «Про охорону навколишнього природного середовища»).
2. **Впровадження стандартів екологічного менеджменту**
   - **Сертифікація за стандартами:**
     - **ISO 14001**: міжнародний стандарт екологічного менеджменту.
     - **EMAS (Eco-Management and Audit Scheme)**: європейська система управління довкіллям.

     Приклад: Заводи BMW отримали сертифікацію ISO 14001 для зниження впливу на навколишнє середовище.

3. **Прозорість та звітність**
   - **Екологічна звітність:**
     - Публікація інформації про екологічні ініціативи та досягнення.
     - Підготовка нефінансової звітності відповідно до стандартів GRI (Global Reporting Initiative).

     Приклад: Coca-Cola звітує про досягнення у зменшенні споживання води на глобальному рівні.
4. **Скорочення негативного впливу**
   - **Зниження викидів:**
     - Контроль за викидами парникових газів.
     - Встановлення очисних споруд.
   - **Економія ресурсів:**
     - Оптимізація використання води, енергії та сировини.
5. **Соціальна відповідальність**
   - **Взаємодія з місцевими громадами:**
     - Участь у екологічних ініціативах, таких як висадка дерев чи очищення територій.
   - **Освітні програми:**
     - Проведення тренінгів для працівників щодо зменшення впливу на довкілля.
6. **Інноваційний підхід**
   - Впровадження технологій для зменшення екологічного сліду:
     - Використання електротранспорту.
     - Розробка біорозкладного пакування.

     Приклад: IKEA активно використовує інноваційні матеріали для скорочення пластику.

Практичне значення екологічної відповідальності

1. **Економічна вигода:**
   - Зменшення витрат на штрафи та природоохоронні платежі.
2. **Конкурентоспроможність:**
   - Підвищення довіри інвесторів та споживачів.
3. **Довгострокова стійкість:**
   - Запобігання екологічним катастрофам та забезпечення стабільності бізнесу.

Реальні приклади екологічної відповідальності

1. **Nestlé:**
   - Зменшення використання пластикового пакування.
   - Створення програм повторного використання води.
2. **Tesla:**
   - Виробництво електромобілів для зменшення залежності від викопного палива.
3. **Unilever:**
   - Скорочення викидів парникових газів на виробництві.

Практичне значення

Дотримання вимог до екологічної відповідальності сприяє зниженню ризиків, зміцненню репутації та покращенню економічних результатів підприємства. Інтеграція екологічних практик є невід'ємною складовою стратегії сталого розвитку сучасного бізнесу.

Екологічна відповідальність підприємства – це не лише зобов’язання перед законодавством, а й стратегічна потреба для довгострокового успіху. Впровадження міжнародних стандартів, прозора звітність та інноваційні підходи дозволяють зменшити екологічний вплив і забезпечити стійкість бізнесу.

Перелік питань:

1. Що таке екологічна безпека промислового підприємства?
2. Як пов’язані між собою екологічна та економічна безпека підприємства?
3. Які основні ризики можуть виникати у сфері екологічної безпеки підприємства?
4. Чому дотримання екологічних стандартів важливе для забезпечення економічної безпеки підприємства?
5. Які міжнародні екологічні стандарти найчастіше застосовуються у промисловості?
6. Що таке ISO 14001, і як цей стандарт впливає на діяльність підприємств?
7. Як впровадження екологічних стратегій впливає на репутацію підприємства?
8. Які етапи включає процес управління екологічними ризиками?
9. Які методи ідентифікації екологічних ризиків застосовуються у промисловості?
10. Як оцінити вплив екологічних ризиків на діяльність підприємства?
11. Які основні заходи можна впровадити для зменшення викидів парникових газів?
12. Що таке циклічна економіка, і як вона сприяє екологічній безпеці підприємств?
13. Які інноваційні технології можуть бути застосовані для зменшення екологічного впливу?
14. Чому прозорість та екологічна звітність є важливими для сучасного бізнесу?
15. Як впровадження енергоефективних технологій допомагає підприємствам скоротити витрати?
16. Які вимоги висуваються до екологічної відповідальності підприємств згідно з українським законодавством?
17. Як взаємодія з місцевими громадами може сприяти екологічній безпеці підприємства?
18. Які реальні приклади впровадження екологічних стратегій демонструють міжнародні компанії?
19. Як оцінювати ефективність заходів зі зменшення екологічного впливу?
20. Чому екологічна безпека є невід’ємною складовою сталого розвитку підприємства?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Алькема В.Г., Літвін Н.М., Кириченко О.С. (2015). Економічна безпека інноваційного підприємства: навчальний посібник. Київ: Університет економіки та права "КРОК". Доступно за посиланням: https://library.krok.edu.ua/media/library/category/navchalni-posibniki/alkema_0012.pdf
2. Андріїв Н.М. Економічна безпека підприємства в умовах цифровізації ринку праці: теоретичні та практичні аспекти : монографія. Львів: Растр-7, 2023. 320 с. Доступно за посиланням: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7359/1/%D0%90%D0%9D%D0%94%D0%A0%D0%86%D0%87%D0%92_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf
3. Артеменко О. В. (2020). Управління економічною безпекою підприємства в умовах нестабільності середовища. Доступно за посиланням: https://ela.kpi.ua/bitstream/123456789/30481/1/Artemenko_magistr.pdf
4. Богдан С. (2024). ЕКОНОМІЧНА БЕЗПЕКА АГРОБІЗНЕСУ В УМОВАХ ЗЕЛЕНОГО КУРСУ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ. Цифрова економіка та економічна безпека, (1 (10), 129-136. Доступно за посиланням: https://doi.org/10.32782/dees.10-23 http://www.dees.iei.od.ua/index.php/journal/article/view/315
5. Бондаренко-Берегович В.В. Управління економічною безпекою підприємств хлібопекарської галузі: дис. ... д-ра філософії за спец. економіка. Вінниця, 2021. 298 с. Доступно за посиланням: https://vsau.org/assets/images/content/nauka/specradi-n/dusert-Bondarenko-Beregovuch.pdf
6. Булатова О.В., Захарова О.В., Карпенко О.І., Федоров Е.В. Економічна безпека країн в умовах сучасних глобальних трансформації: виклики, загрози, ризики/за загальною редакцією д.е.н., проф. О.В. Булатової. – Місто: Київ: МДУ, 2024. – 290 с. Доступно за посиланням: https://repository.mu.edu.ua/jspui/bitstream/123456789/7365/1/bul_zah_ekon_bez_mon_2024.pdf
7. Вовченко О.В. Вплив інноваційної діяльності у промисловості України на економічну безпеку держави: дис. ... канд. екон. наук. Київ, 2019. 205 с. Доступно за посиланням: https://library.krok.edu.ua/ua/kategoriji/disertatsiji-avtoreferati-vidguki/vplyv-innovatsiinoi-diialnosti-u-promyslovosti-ukrainy-na-ekonomichnu-bezpeku-derzhavy
8. Воловельська Н.І. (2020). Економічна безпека підприємства: сучасні підходи та методи. Доступно за посиланням: https://lib.kart.edu.ua/bitstream/123456789/21357/1/Volovelska.pdf Живко З.Б., Черевко О.В., Зачосова Н.В. (2019). Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник. Черкаси: Видавець Чабаненко Ю.А. Доступно за посиланням:

[dspace.lvduvs.edu.ua](https://dspace.lvduvs.edu.ua/bitstream/1234567890/3465/1/%D0%9D%D0%9C%D0%9F_%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0

9. Вороніна В.Л. (2019). Економічна безпека підприємств: сутність, фактори впливу та методи забезпечення. Доступно за посиланням: https://chmnu.edu.ua/wp-content/uploads/2019/07/Voronina-V.-L.-1.pdf
10. Гринкевич С. (2021). Еволюція теоретичних концепцій економічної безпеки підприємства. Економіка та суспільство, вип. 26. Доступно за посиланням: https://www.academia.edu/106923491/%D0%95%D0%92%D0%9E%D0%9B%D0%AE%D0%A6%D0%86%D0%AF_%D0%A2%D0%95%D0%9E%D0%A0%D0%95%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%A5_%D0%9A%D0%9E%D0%9D%D0%A6%D0%95%D0%9F%D0%A6%D0%86%D0%99_%D0%95%D0%9A%D0%9E%D0%9D%D0%9E%D0%9C%D0%86%D0%A7%D0%9D%D0%9E%D0%87_%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%98_%D0%9F%D0%86%D0%94%D0%9F%D0%A0%D0%98%D0%84%D0%9C%D0%A1%D0%A2%D0%92%D0%90
11. Живко З.Б., Черевко О.В., Зачосова Н.В. (2019). Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник. Черкаси: видавець Чабаненко Ю.А. Доступно за посиланням: https://library.snu.edu.ua/ekonomichna-bezpeka-pidpryyemstva/
12. Зайченко В.В., Коваленко С.В. (2013). Економічна безпека підприємства: сутність та основні складові. Доступно за посиланням: https://dspace.kntu.kr.ua/server/api/core/bitstreams/954dd1a2-c6ec-42e1-88ad-532c2c2fab75/content
13. Іванова Н.С. Економічна безпека : навч. посібник. / уклад. Н.С. Іванова; Донец. нац. ун-т економіки і торгівлі ім. М. Туган-Барановського, каф. маркетингу, менеджменту та публ. адміністрування. – Кривий Ріг: ДонНУЕТ, 2020. – 139 с. DOI: https://doi.org/10.5281/zenodo.10022448 . Доступно за посиланням: http://elibrary.donnuet.edu.ua/2312/1/2020_NP_Ivanova_Ekonom_bezpeka.pdf
14. Інноваційна економіка: теоретичні та практичні аспекти: монографія / Л.О. Волощук, Є.І. Масленніков, Е.А. Кузнєцов, Ю.М. Сафонов, С.В. Філиппова та ін.; за ред. д.е.н., доц. Л.О. Волощук, д.е.н., проф. Є.І. Масленнікова. Херсон: ОЛДІ-ПЛЮС, 2019. Випуск 4. 524 с. Доступно за посиланням: https://economics.net.ua/files/scientific-base/monogr/mono_innov_econom_4_2019.pdf
15. Калинюк В.Є. (2022). Сучасні наукові підходи до визначення сутності поняття «економічна безпека підприємства». Бізнес Інформ, №12, с. 221-228. Доступно за посиланням: https://www.business-inform.net/export_pdf/business-inform-2022-12_0-pages-221_228.pdf
16. Кузенко Т.Б., Сабліна Н.В. (2020). Фінансова безпека підприємства: навчальний посібник. Харків: ХНЕУ ім. С. Кузнеця. Доступно за посиланням: https://library.snu.edu.ua/ekonomichna-bezpeka-pidpryyemstva/
17. Левковець Н.П. Ідентифікація стану економічної безпеки та базові засади і заходи її забезпечення для підприємств автомобільного транспорту : автореф : дис. ... канд. екон. наук. Київ, 2020. 22 с. Доступно за посиланням: http://diser.ntu.edu.ua/Levkovets_aref.pdf

18. Максимюк М.М. Економічна безпека сільськогосподарських підприємств на пореформеному розвитку: автореф. дис. ... канд. екон. наук.Львів, 2019. 20 с.9. Ковальчук А.М. Мотиваційне управління економічною безпекою підприємств : автореф. дис. ... канд. екон. наук. Харків, 2020. 25 с Доступно за посиланням: https://uacademic.info/ua/document/0419U002517
19. Марченко О.С. (2022). Економічна безпека підприємства: навчальний посібник. Харків: Право. Доступно за посиланням: https://pravo-izdat.com.ua/novinki/ekonomichna-bezpeka-pidpriyemstva
20. Марчук Л.Л. Науково-методичні засади регулювання економічної безпеки аграрного виробництва в Україні: дис. ... канд. екон. наук. Чернігів, 2019. 295 с. Доступно за посиланням: https://ir.stu.cn.ua/handle/123456789/17599
21. Міщук Є.В. (2020). Формування економічної безпеки підприємства у динамічних умовах бізнес-середовища. Доступно за посиланням: https://uacademic.info/ua/document/0523U100231
22. Неустроєв Ю.Г. Роль інновацій у забезпечені економічної безпеки. Агросвіт No 7-8, 2021. С. 103-108. Доступно за посиланням: http://www.agrosvit.info/?op=1&z=3425&i=14
23. Ортинський В.Л., Керницький І.С., Живко З.Б. (2019). Економічна безпека підприємств: підручник. Київ: Алерта. Доступно за посиланням: https://library.snu.edu.ua/ekonomichna-bezpeka-pidpryyemstva/
24. Остапюк Б.Б. Управління економічною безпекою підприємств залізничного транспорту в умовах лібералізації ринку залізничних перевезень : автореф. дис. ... канд. екон. наук.Харків, 2019. 24 с. Доступно за посиланням: https://kart.edu.ua/dissertation/upravlinnja-ekonomichnoju-bezpekoju-pidpriiemstv-zaliznichnogo-transportu-v-umovah-liberalizacii-rinku-zaliznichnih-perevezen
25. Покришка Д.С. Технологічна конкурентоспроможність національної економіки як чинник економічної безпеки України: дис. ... канд. екон. наук.Київ, 2021. 303 с. Доступно за посиланням: https://niss.gov.ua/sites/default/files/2021-04/pokryshka_dissertation.pdf
26. Потябін М.Ю. (2018). Економічна безпека підприємства: сутність та основні складові. Доступно за посиланням: https://repository.hneu.edu.ua/bitstream/123456789/19817/1/%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D1%8B_%D0%9F%D0%BE%D1%82%D1%8F%D0%B1%D0%B8%D0%BD%20%D0%9C.%D0%AE..pdf
27. Рибальченко Л.В., Косиченко О.О. (2022). Основи забезпечення економічної безпеки підприємництва. Дніпро: ДДУВС. Доступно за посиланням: https://er.dduvs.in.ua/xmlui/handle/123456789/1693/browse?type=subject&value=%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%B0+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0&
28. Сафонік Н.П., Дудік А.О. Особливості формування системи економічної безпеки авіапідприємств в умовах трансформаційних перетворень. Економіка та суспільство. Випуск 45/2022. Доступно за посиланням: https://economyandsociety.in.ua/index.php/journal/article/view/1904

29. Сисоліна Н.П. (2014). Економічна безпека підприємства: навчальний посібник. Кіровоград: КНТУ. Доступно за посиланням: https://dspace.kntu.kr.ua/bitstream/123456789/3583/1/Ekonomichna%20bezpeka%20pidpryyemstva.pdf
30. Сосновська О.О. Система економічної безпеки підприємств зв'язку: монографія. Київ: «Центр учбової літератури», 2019. 440 с. Доступно за посиланням: https://core.ac.uk/download/pdf/241043898.pdf
31. Ситник Г.В., Блакита Г.В., Гуляєва Н.М. (2020). Економічна безпека підприємництва в Україні: монографія. Київ: КНТЕУ. Доступно за посиланням: https://library.snu.edu.ua/ekonomichna-bezpeka-pidpryyemstva/?utm_source=chatgpt.com
32. Срібна Є.В. Логістичні засади державного регулювання енергетичної безпеки країни: дис. ... канд. екон. наук. Рівне, 2018. 320 с. Доступно за посиланням: https://library.wunu.edu.ua/libsearch/DocDescription?doc_id=394123
33. Тульчинська С.О., Солосіч О.С., Чорній В.В. Вплив діджиталізації управлінських процесів на систему забезпечення економічної безпеки підприємства. Інвестиції: практика та досвід No 9/2021. С. 54-58. Доступно за посиланням: http://www.investplan.com.ua/?op=1&z=7439&i=7
34. Шашина М.П., Тульчинська С.О. (2021). Економічна безпека підприємства: навчальний посібник до виконання практичних завдань. Доступно за посиланням: https://www.ela.kpi.ua/bitstream/123456789/55883/1/Shashyna_TulchynsKa_np_ebp.pdf
35. Шира Т. Б. (2020). Корпоративна безпека підприємств: теоретичні та прикладні аспекти. Львів: Українська академія друкарства. Доступно за посиланням: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3539/1/shira_d.pdf
36. Яровенко Г.М. Інформаційна безпека як драйверрозвитку національної економіки: автореф. дис. ... д-ра екон. наук. Суми, 2021. 37 с.7. Любохинець Л.С. Гнучке управління у забезпеченні економічної безпеки промислових підприємств: автореф. дис. ... д-ра екон. наук. Хмельницький, 2022. 40 с. Доступно за посиланням: https://essuir.sumdu.edu.ua/handle/123456789/83320
37. https://elartu.tntu.edu.ua/bitstream/lib/42922/2/MNPK_2023_Levytskyi_V-Economic_and_legal_enterprise_71-74.pdf
38. https://hozpravoreposit.kyiv.ua/bitstream/handle/765432198/218/2018%20%E2%80%A2%20%E2%84%96%205.pdf?sequence=1
39. https://pdf.lib.vntu.edu.ua/books/2024/Nebava_2017_73.pdf
40. https://dspace.kntu.kr.ua/server/api/core/bitstreams/5be8e910-6806-43a5-9428-17e72c8a6f0e/content
41. ISO 31000:2018 – Risk management – Guidelines
42. ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements
43. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements
44. ISO 28000:2007 – Specification for security management systems for the supply chain
45. ISO 22316:2017 – Security and resilience – Organizational resilience – Principles and attributes

46. https://www.researchgate.net/publication/369219239_Risk_Management_in_the_Enterprise_The_Essence_Approaches_and_Methods
47. https://www.psae-jrnl.nau.in.ua/journal/2_82_2021_ukr/17.pdf
48. Пожуєва Т.О. Роль кластерів у посиленні економічної безпеки та стійкості металургійних підприємств // Економічний аналіз. 2024. Том 34. № 4. С. 473-483 https://www.econa.org.ua/index.php/econa/article/view/6242
49. Pozhuieva T.O., Bobko N.A. Economic security of metallurgical enterprises in the context of sustainable development: challenges and opportunities // Економічний вісник ДВНЗ «Український державний хіміко-технологічний університет». 2024. № 2. С. 97-104 http://ek-visnik.dp.ua/wp-content/uploads/pdf/2024-2/Pozhuieva.pdf
50. Pozhuieva T.O., Buhrim O.Y. Prospects and risks of using cryptocurrency in the modern economic space // Економічний вісник ДВНЗ «Український державний хіміко-технологічний університет». 2023. № 2. С. 126-131 http://ek-visnik.dp.ua/wp-content/uploads/pdf/2023-2/Pozhuieva.pdf
51. Pozhuieva T.O., Buhrim O.Y. The role of economic security in forecasting probable threats // Економічний вісник ДВНЗ "Український державний хіміко-технологічний університет" : загальнодерж. наук. вид. з питань економіки і бізнесу: зб. наук. пр. / ДВНЗ "Укр. держ. хіміко-технолог. ун-т". – Дніпропетровськ: ДВНЗ УДХТУ, 2022. – №2. – С. 58-64 http://ek-visnik.dp.ua/wp-content/uploads/pdf/2022-2/Pozhuiva.pdf

ВІДПОВІДІ НА ТЕСТИ

Тема 1
1. б; **2.** б; **3.** в; **4.** в; **5.** б; **6.** б; **7.** в; **8.** а; **9.** б; **10.** б;
11. б; **12.** б; **13.** в; **14.** б; **15.** б; **16.** а; **17.** а; **18.** б; **19.** б; **20.** б.

Тема 2
1. б; 2**.** б; 3**.** в; 4**.** в; 5**.** б; 6**.** а; 7**.** б; 8**.** б; 9**.** а; **10.** б;
11. а; **12.** б; **13.** б; **14.** б; **15.** б; **16.** б; **17.** б; **18.** а.

Тема 3
1. в; **2.** в; **3.** б; **4.** б; **5.** б; **6.** а; **7.** б; **8.** б; **9.** б; **10.** б.

Тема 4
1. б; **2.** в; **3.** а; **4.** в; **5.** в; **6.** а; **7.** а; **8.** б; **9.** б; **10.** б;
11. б; **12.** б; **13.** б; **14.** а; **15.** б; **16.** а; **17.** б; **18.** б; **19.** б; **20.** б.

Тема 5
1. б); **2.** в); **3.** б); **4.** б); **5.** б); **6.** а); **7.** б); **8.** в); **9.** б); **10.** а);
11. б); **12.** в); **13.** б); **14.** б); **15.** б); **16.** в); **17.** а); **18.** а); **19.** б); **20.** в)

Тема 6
1. б); **2.** б); **3.** б); **4.** б); **5.** б); **6.** б); **7.** а); **8.** б); **9.** а); **10.** б);
11. г); **12.** б); **13.** г); **14.** б); **15.** б); **16.** б); **17.** а); **18.** б); **19.** б); **20.** б)

Тема 7
1. б); **2.** б); **3.** в); **4.** б); **5.** б); **6.** в); **7.** б); **8.** а); **9.** в); **10.** а);
11. б); **12.** б); **13.** б); **14.** б); **15.** а); **16.** б); **17.** б); **18.** б); **19.** а); **20.** б)

Тема 8
1. в); **2.** б); **3.** а); **4.** б); **5.** б); **6.** б); **7.** г); **8.** в); **9.** б); **10.** а);
11. в); **12.** а); **13.** б); **14.** б); **15.** б); **16.** б); **17.** б); **18.** б); **19.** б); **20.** б)

Тема 9
1. в); **2.** б); **3.** а); **4.** б); **5.** б); **6.** в); **7.** б); **8.** в); **9.** а); **10.** б);
11. б); **12.** в); **13.** б); **14.** а); **15.** б)

Тема 10
1. б); **2.** б); **3.** б); **4.** а); **5.** б); **6.** б); **7.** б); **8.** б); **9.** б); **10.** б);
11. б); **12.** а); **13.** б); **14.** в)

Тема 11
1. б); **2.** г); **3.** в); **4.** б); **5.** а); **6.** б); **7.** б); **8.** в); **9.** б); **10.** б);
11. б); **12.** в); **13.** б); **14.** б); **15.** б)

Тема 12

1. б); **2.** в); **3.** б); **4.** а); **5.** в); **6.** б); **7.** б); **8.** а); **9.** в); **10.** б); **11.** б); **12.** а); **13.** г); **14.** б); **15.** б)

Тема 13

1. б); **2.** б); **3.** б); **4.** б); **5.** б); **6.** б); **7.** б); **8.** б); **9.** б); **10.** б)

Тема 14

1. б); **2.** б); **3.** в); **4.** б); **5.** б); **6.** б); **7.** а); **8.** а); **9.** а); **10.** б)

Науково-методичне видання

ПОЖУЄВА Тетяна Олександрівна

«Економічна безпека»

для здобувачів вищої освіти спеціальності 073 «Менеджмент» та 076 «Підприємництво та торгівля» усіх форм навчання

Комп’ютерний набір та верстка: Пожуєва Т.О.

Підписано до друку 19.12.2025. Формат 60×84/16. Ум. Друк. Арк. 17,32
Тираж 100 прим. Зам. №1117.

Національний університет «Запорізька політехніка»
Україна, 69063, м. Запоріжжя, вул. Університетська, 64
Тел.: (061) 769-82-96, 220-12-14

Свідоцтво суб’єкта видавничої справи ДК №6952 від 22.10.2019.